Configuration Guide for Cisco Unified ICM Enterprise-Release 12.6(1)

First Published: 2021-05-14

CONTENTS

Preface

- Change History, on page xv
- About This Guide, on page xv
- Audience, on page xv
- Communications, Services, and Additional Information, on page xvi
- Field Notice, on page xvi
- Documentation Feedback, on page xvi
- Conventions, on page xvii

Change History

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

Change	See	Date
Initial Release of Document for Release 12.6(1)		14-May-2021
New option **Manage Security** is available in Agent tab	Manage Security	

About This Guide

This guide describes how to use configuration tools to configure and maintain the system database. For instructions on how to create and manage scripts, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*. For specific information on an automatic call distribution (ACD) or network interface card (NIC), refer to the appropriate Cisco Unified ICM/Contact Center Enterprise ACD or NIC supplement documentation or ask your customer representative for that documentation.

Audience

This guide is intended for Unified ICM/Contact Center Enterprise system administrators. A system administrator must have a general understanding of call center operations and management and specific information about the call centers and carrier networks connected to Unified ICM/Contact Center Enterprise software.

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.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Configuration Overview

Software Overview

Cisco Unified Intelligent Contact Management Overview

Unified Intelligent Contact Management provides enterprise-wide distribution of multichannel contacts across geographically separated contact centers. Such multichannel contacts are inbound or outbound telephone calls, web collaboration requests, e-mail messages, and chat requests. Unified ICM is an open standards-based solution whose capabilities include routing, queuing, monitoring, and fault tolerance. Unified ICM forms the basis for the Cisco Unified Communications family of products.

The system software functions across environments and across channels.

The system software functions in the older environment of telephone calls delivered over Time-division multiplexing (TDM) lines, of hardware automatic call distributions (ACDs) and interactive voice responses (IVRs), and of call centers centralized around the hardware. The system software can route calls for a single 800 number or for several different numbers. The system software reads information about each incoming call from the public network. The system software also determines the best destination for that call, and returns information to the public network instructing it where to route the call. This process is known as *call-by-call routing*.

The system software makes routing decisions by executing scripts that can easily be modified. These scripts can use real-time information about activity at the contact centers to find the destination best able to handle the call. You can monitor how the system is handling calls. You can also observe how the system modifies scripts when needed.

The system software functions in the newer environment of multichannel contact delivered through IP connections. These IP connections are of software ACDs and IVRs. The connections are also of contact centers that can be as decentralized as the Internet or as centralized as business practices requirements, not hardware necessities requirements.

The system software functions in the mixed transition environment that involves all of the above.

For detailed information about Unified ICM, refer to the *Pre-installation Planning Guide for Cisco Unified ICM* and the *Administration Guide for Cisco Unified Contact Center Enterprise*.

Cisco Unified Contact Center Enterprise Overview

Cisco Unified Contact Center Enterprise (Unified CCE) delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. It combines multichannel ACD functionality with IP telephony in a unified solution, enabling your company to rapidly deploy a distributed contact center infrastructure.

Unified CCE provides:

- Segmentation of customers and monitoring of resource availability

- Delivery of each contact to the most appropriate resource anywhere in the enterprise

- Comprehensive customer profiles using contact-related data, such as dialed number (DN), and calling line ID

- Routing to the most appropriate resource to meet customer needs based on real-time conditions (such as agent skills, availability, and queue lengths)

- Presence integration to increase caller satisfaction through improved agent performance and knowledge-worker expertise

Unified CCE allows you to smoothly integrate inbound and outbound voice applications with Internet applications such as real-time chat, web collaboration, and email. This integration enables a single agent to support multiple interactions simultaneously regardless of which communications channel the customer has chosen. Because each interaction is unique and may require individualized service, Cisco provides contact center solutions to manage customer interactions based on almost any contact attribute.

For detailed information about Unified CCE, refer to the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* and the *Administration Guide for Cisco Unified Contact Center Enterprise*.

Configuration Management

Unified ICM configuration information is permanently stored in the Central Controller database. The system software configuration consists of hardware entities, call targets, announcements, routes, dialed numbers, and regions. Use the tools of the Unified ICM/CCE Configuration Manager (referred to as "Configuration Manager" in this guide) to create and modify configuration data. When you apply a change in Configuration Manager, it is immediately applied to the central database.

Note You cannot open more than 60 configuration windows simultaneously. If more than 60 configuration windows are required, you must add another distributor.

To get started setting up and maintaining your configuration, see **Access Configuration Manager**.

Script Management

After you have set up your configuration, you can write routing scripts and administrative scripts:

- *A routing script* processes a call routing request from a routing client and determines the best destination for that call. The system software then passes a label associated with the destination back to the routing client.

- *An administrative script* runs periodically to perform a task, such as setting variables.

Use the Script Editor to create, maintain, and monitor scripts.

You can set up different routing scripts to run for different types of tasks. You can define call types in terms of the telephone number the caller dialed, the number the caller is calling from, and additional digits entered by the caller. For each call type, you can schedule different routing scripts to run on different days or at different times of the day. The figure below shows a sample ICM routing script, including longest available agent (LAA), and minimum expected delay (MED).

Figure 1: Sample Routing Script
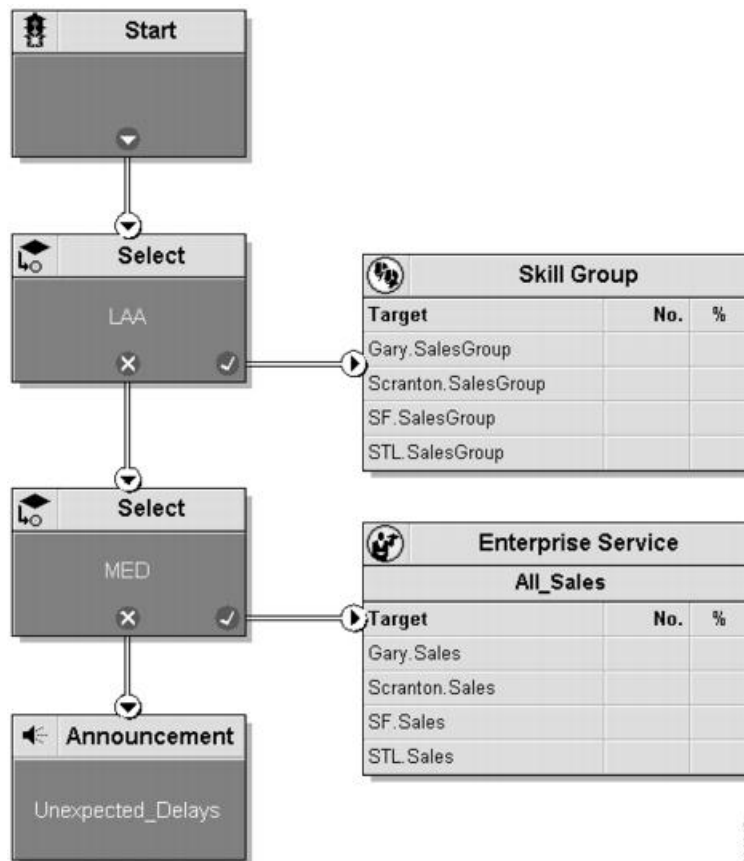
A routing script typically examines several targets and applies selection rules to find an available qualified agent or a target with the shortest expected delay. You can use any of several predefined selection rules or you can set up your own selection criteria.

Within the Script Editor, you can open a script for browsing, monitoring, or editing. When you open a script for editing, the Script Editor automatically obtains the lock for that script.

To get started using the Script Editor to create or maintain scripts, refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.

Routing a Call

Properly Route Calls

To properly route calls, three independent systems must work together:

- The routing client

- The system software

- The peripheral that ultimately receives the call

The *routing client* requests a route from the system software, receives a response, and delivers the call to the specified destination.

The *system software* receives a routing request and determines the appropriate destination for the call. The destination is an announcement (which is played by the routing client), a scheduled target, or a specific target at a peripheral (represented by a trunk group and dialed number identification service [DNIS]).

A *peripheral* is a switch at a call center, such as an ACD, a PBX, or Unified Communications Manager (Unified CM). The peripheral completes the routing by dispatching the call to the specific target determined by the system software.

Route a Call

The process of routing a call consists of the following steps:

1. A routing client requests a route from the system software.

2. The system software, using information supplied by the routing client, categorizes the request as a specific call type.

3. The system software runs a routing script scheduled for the call type to find a destination for the call. The destination can be a routing label, an announcement, or a skill target: a service, skill group, or agent. (If the script fails to find a destination, the system software uses a default destination based on the dialed number.)

   A *routing label* is a character string value that the routing client maps to a destination trunk group and, optionally, a DNIS value for the call.

4. The system software passes the routing label back to the routing client.

5. The routing client interprets the label to find the destination.

6. The routing client dispatches the call to the destination (with the appropriate DNIS value, if any).

7. The call is sent to a peripheral; the peripheral must determine the specific target for which the call is intended.

   The peripheral typically makes this determination based on the trunk group on which the call arrived and, optionally, the DNIS value sent with the call. The peripheral then completes the routing by dispatching the call appropriately.

The following sections describe the process in detail.

Related Topics

Routing a Call

Understanding the call-routing process helps you set up the configuration of your system software and create effective scripts.

Routing Requests

The system software receives routing requests from routing clients, where the type is either the specific IXC (for example, AT&T or MCI) or the specific type of the peripheral (for example, voice response unit (VRU) or a specific type of ACD).

Routing clients send messages to the system software. One type of message is a *route request*. In this case, given a call, the routing client asks the system software for a destination, or route, for that call. If the routing client is an IXC, this is the only type of message that it sends.

Routing requests are of two types: *pre-routing* and *post-routing*. A Pre-Routing request is sent by an IXC to determine the initial destination for a call. A Post-Routing request is sent by the peripheral that receives the call to either refine the original route or redirect the call.

A routing request includes the following information about the call to be routed:

- **Dialed Number (DN)**. The number the caller dialed.

- **Calling Line ID (CLID)**. The billing telephone number for the caller. This value is also referred to as Automatic Number Identification (ANI).

- **Caller-Entered Digits (CED)**. Digits the caller entered on a touch-tone phone in response to prompts.

Post-Routing messages vary depending on the type of the peripheral.

Targets

A target is the destination for a call. The target can be a label, an announcement defined by the routing client, or a target at a peripheral.

A target at the peripheral is a service, skill group, or individual agent that the system software selects to handle the call. This is called the *skill target*. Regardless of the specific skill target, every call routed by the system software must also be associated with a service. The combination of a skill target and a service is a *route*.

A target represents a network trunk group at the peripheral and, optionally, a DNIS value. The routing client uses this type of target, called a *peripheral target*, to route the call. Each peripheral target or announcement maps to a routing label.

The following figure shows the relationships among skill targets, routes, peripheral targets, announcements, and labels.

Figure 2: Targets, Routes, and Labels
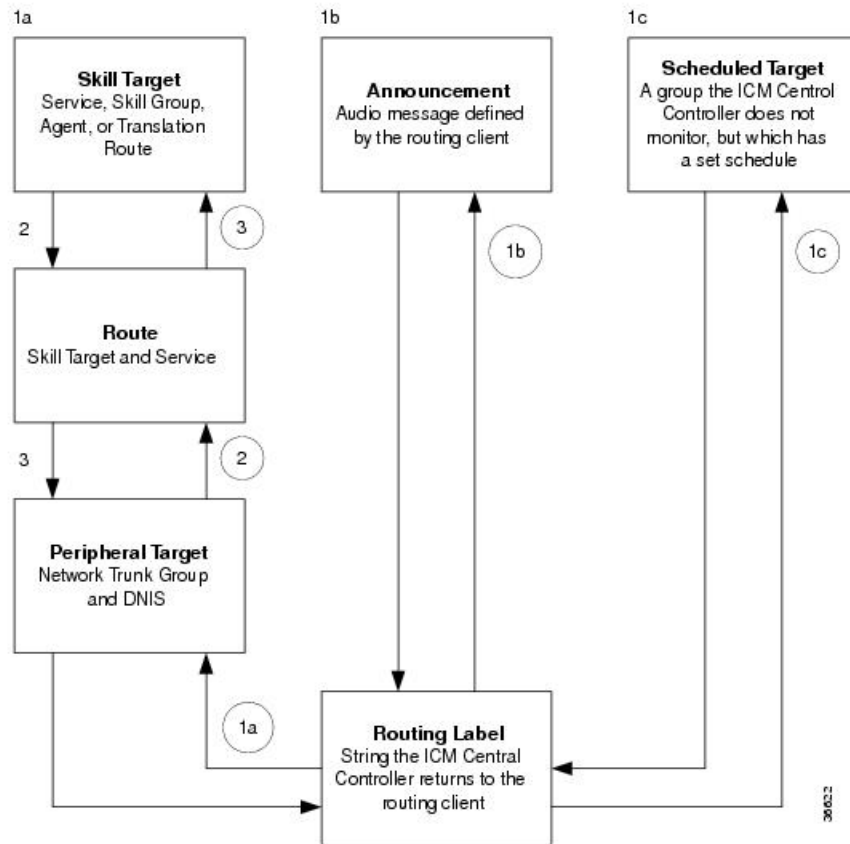
The system software works from top to bottom in the preceding figure:

1. A routing script determines a destination for the call.

   The destination is a routing label that the system software can return directly to the routing client.

   Otherwise, the destination is one of the following:

   - A skill target to receive the call

   - An announcement to be played

   - A scheduled target to receive the call

   If the destination is a skill target, that skill target has an associated route.

2. The system software uses the route to find an associated peripheral target supported by the routing client.

3. The peripheral target is associated with a label. The system software returns that label to the routing client. If the destination is an announcement, the system software needs only to find the label associated with that announcement and return the label to the routing client.

   The routing client processing depends on the type of the label. Some labels instruct the routing client to take a special action: playing a busy signal for the caller, playing an unanswered ring for the caller, or making a special query.

   For normal labels, the routing client converts the label to an announcement, scheduled target, or peripheral target by working up from the bottom of the above figure.

4. The routing client receives a label from the system software in response to its route request. It translates that label into one of the following:

   - A peripheral target

   - An announcement

   - A scheduled target

   - An unrouted task that gets routed to a local agent

   The result is an announcement, which plays the announcement for the caller. The result is a scheduled target, which delivers the call to that target.

5. The routing client delivers the call to the specified *network trunk group* at the peripheral and sends the specified DNIS value, if any, with it.

6. The peripheral itself must then recognize the network trunk group and DNIS for the call as it arrives and determine the associated service and skill target. The peripheral then completes the process by locating the appropriate agent to handle the call.

System Processing

The following figure summarizes how the system software processes a route request.

Figure 3: Unified ICM Route Request Processing
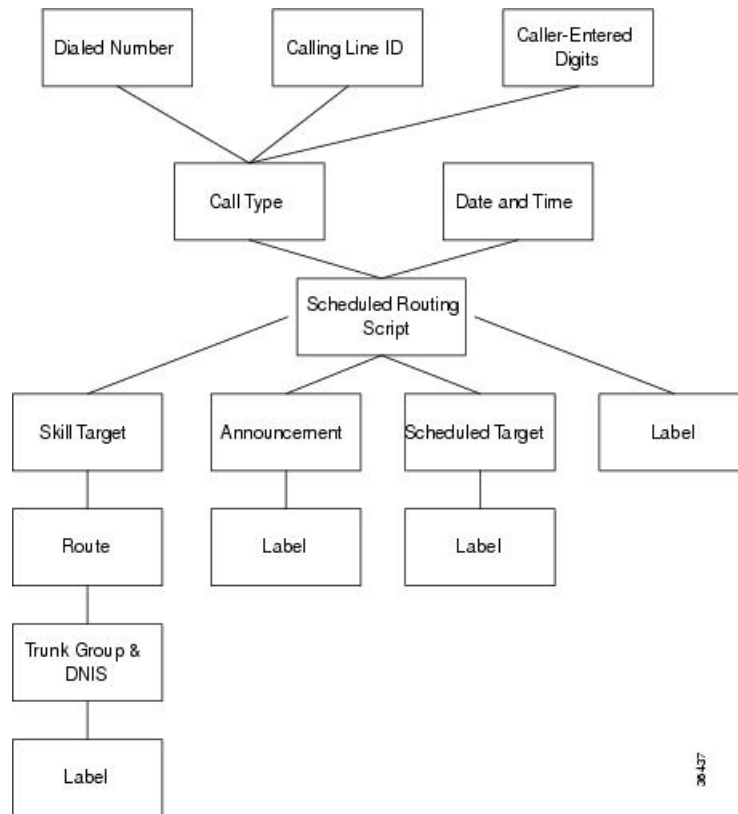
The following subsections describe this processing.

Determine Call Type

When the system software receives a route request for a call, it first determines the call type of the call. A *call type* is a category of incoming Unified Intelligent Call Management (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)

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

While chat sessions and blended collaboration are different from email and require call variables, the call variables are not part of the call type definition.

For example, you might define three call types to correspond to three sales regions within the country. You might have a network prompt that lets the caller enter 1 for sales, 2 for support, and 3 for information. If a call arrives for the dialed number 800.486.0029, with a CLID from the 403 (San Jose region) area code, and the caller enters 1 (sales) in response to the prompt, that call is classified as Western Sales.

If another call arrives with the same dialed number, but with a CLID from the 212 (New York City) area code, and the caller-entered digit 1, that call is classified as Eastern Sales.

You can define a general default call type and a specific default call type for each routing client. If the call qualifiers do not map to a specific call type, the system software uses a default call type defined for the routing client. If no default call type is defined for the routing client, the system software uses the general default call type.

Run Script

Each call type has specific routing scripts scheduled for different times of day and different days of the year. The system software finds the script currently scheduled for the call type and runs it. If that script fails to find a suitable destination (that is, a label, announcement, or skill target) for the call, the system software uses a default target associated with the DN value.

If the system software finds an announcement or scheduled target for the call, it can immediately resolve that to a label to return to the routing client. If the system software finds a skill target for the call, it must perform a few extra steps before it finds a label.

Determine Route

If the system software finds a skill target for the call, that target has an associated route. You specify the route when you set up the target within the routing script. A route represents the combination of a skill target and a service. That is, a route represents the destination for a call and the type of service to be provided to the caller. Every call routed to a peripheral must have an associated service.

For example, the skill target for a call might be the skill group *Denver.PostSales* and the associated service might be *Denver.TechSupport*. Another call might also be routed to the *Denver.PostSales* group with the associated service *Denver.Upgrades*.

Note If the destination is itself a service, for example *Chicago.Sales*, the associated service must also be *Chicago.Sales*. To associate a service skill target with a route for a different service would skew the statistics for those services.

Determine Trunk Group and DNIS

After it has determined a route for a call, the system software finds an associated peripheral target (trunk group and DNIS). It is possible to have several peripheral targets associated with the same route, but typically only one of those targets is valid for the routing client. For example, if you have switched access lines, two IXCs could direct calls to the same trunk group and DNIS, but each requires a different label value for that target. Therefore, you need to define two separate peripheral targets for the route. If more than one peripheral target is associated with the route, the system software chooses the first peripheral target that maps to a valid label for the routing client.

Determine Label

Each peripheral target, scheduled target, or announcement maps to one or more labels. The system software finds the first label that is valid for the routing client and dialed number and returns that label to the routing client. It is then up to the routing client to interpret the label.

Default Label

It is possible that the system software may fail to find a call type for a route request. Also, the system software may run the script currently scheduled for a call type and fail to find a destination for the call. In these cases, it uses a default label that is defined for the dialed number. If no default label is defined for the dialed number, the system software returns an error to the routing client.

The routing client itself also has some default action defined. When you set up each routing client, you can specify the maximum time that client can wait for a response to a routing request. It may happen that the system software has not returned a destination for the call before the time limit is reached. Also the system software may return an error. In both these scenarios, the routing client performs its own default action.

Routing Client

The routing client begins by requesting a route for a call from the system software. The system software processes the request as described in the preceding section and returns a label to the routing client.

The routing client has its own internal mappings for labels to announcements, scheduled targets, and peripheral targets.

It uses these mappings to interpret the label from the system software:

- **Busy**. Routing client plays a busy signal for the caller.

- **Ring**. Routing client plays an unanswered ring for the caller.

- **Normal** and the label maps to an **announcement**. Routing client plays the announcement for the caller.

- **Normal** and the label maps to a **scheduled target**. Routing client delivers the call to that target.

- **Normal** or **DNIS Override** and the label maps to a **peripheral target** (that is, a trunk group and a DNIS). Routing client delivers the call and the specified DNIS value to that trunk group. The peripheral then has responsibility for dispatching the call to the appropriate skill target.

Peripheral Processing

When a peripheral receives a call, it determines the trunk group on which the call arrived and the DNIS value, if any, associated with it. The peripheral must be programmed to map these values to the same service and skill target determined by the system software.

The peripheral, acting as a routing client, can also send a routing request to the system software.

Translation Routes

Translation routes allow you to send additional information to a skill target along with the call..

A translation route is a temporary destination for a call. When the system software returns a translation route label to the routing client, it also sends a message directly to the peripheral gateway (PG) at the targeted peripheral. This message alerts the PG that a call will be arriving that requires route translation.

The message contains the following information:

- The trunk group on which the call will arrive and the DNIS value associated with it.

- A label to be used by the PG to determine the ultimate skill target of the call. This is a label that the PG can interpret to find the correct destination.

- Instructions for further processing to be performed by the PG. This further processing might include, for example, looking up an account number in a database.

When the peripheral sees the call arrive on the specified trunk group and with the specified DNIS value, it passes this information to the PG. The PG then combines it with the information it has received from the system software. It then sends the call along with this information to the skill target specified by the label it received. At the same time, the peripheral might, for example, send a message to a host computer that controls the display on the agent's workstation. This allows data, such as the caller's account information, to be displayed on the screen when the call arrives. The PG coordinates communication among the network, the peripheral, and the computer application that controls the display.

To set up translation routing, you must do the following:

- Set up a translation route associated with the peripheral. You do not need a separate translation route for each possible skill target at the site, but you need at least one for each peripheral that performs translation routing.

- Set up one or more routes and associated peripheral targets for the translation route. Typically, all peripheral targets for a translation route refer to the same trunk group, but with different DNIS values.

- Set up a label for the original routing client for the call to access each of the peripheral targets associated with the translation route. For example, if the routing client is an IXC, you must set up a label to the targets with the IXC. This allows the call to be initially sent to the translation route at the peripheral.

- For each peripheral target that you want to be able to ultimately access via a translation route, set a label with the peripheral as the routing client. For example, you might want to be able to send calls to the Atlanta Support skill group through a translation route. To do this, you must configure a label for that skill group with the Atlanta peripheral as the routing client. This allows the peripheral to determine the ultimate destination for the call.

- To display data on the agent's workstation when the call arrives, you must configure the peripheral to inform the PG which agent is receiving the call.

Timeouts and Thresholds

In setting up your configuration, you need to specify several timeout and timing threshold values.

For routing clients, you must specify the maximum time the system software can spend before responding to each routing request. You must also specify the maximum time for the routing client to wait for a response before it stops sending new requests to the system software.

For each service at a peripheral, you must specify your goal for the maximum time a caller must wait before the call is answered. The system software uses this value in calculating the service level.

You can specify how to count abandoned calls in the service level calculation. You can also specify the minimum time a call must be in the queue before it can be considered abandoned.

For specific information about configuring routing clients, peripherals, and services, see Chapters 4 through 7.

Routing Client Wait Time

In some cases, a routing client might be unable to receive routing responses from the system software. Sometimes this affects only a single request, but other times the routing client loses contact with the system software for longer periods. You can specify the amount of time for the routing client to wait before giving up on a single request and the amount of time to wait before it stops sending any requests to the system software.

Timeout Threshold

For AT&T Intelligent Call Processing (ICP) connections, set the timeout threshold to 1500 milliseconds.

Late Threshold

You can specify a second threshold, the AT&T Intelligent Call Processing (ICP) connections, by setting the late threshold to 500 milliseconds.

Timeout Limit

The system software is designed to be a highly reliable system. Distributed duplicated hardware and software fault-tolerance ensure very high availability. However, the NIC uses a timeout limit to provide a safety net to ensure that your calls continue to be routed even if the system software were to become completely unavailable. If the routing client receives no responses from the system software within the timeout limit (and a minimum number of requests have been made), it stops sending requests to the system software. You can set the minimum number of requests that must be made (the consecutive timeout limit) when you set up the NIC software. The default is 10.

When a routing request first exceeds the timeout threshold, the NIC for the routing client starts a timer. If the timer reaches the timeout limit before the routing client receives any on-time routing responses from the system software, the NIC tells the routing client to stop sending routing requests to the system software. An on-time response is a response within the timeout threshold. You can specify the timeout limit in seconds. For example, for AT&T ICP connections, set the timeout limit to 10 seconds.

Abandoned Call Wait Time

When a call is delivered to a peripheral, the caller might be placed in a queue waiting for an agent to become available. Generally, if the caller hangs up before they connect with an agent, the call is considered abandoned. A high number of abandoned calls might mean that you are losing business because callers are being made to wait too long.

However, if a caller hangs up almost immediately after they are placed in a queue, you might not want to count that as an abandoned call. In these cases, caller impatience or excessive queue times are not the problem; the caller probably hung up for another reason. Tracking these as abandoned calls can be misleading.

Therefore, you can specify a minimum amount of time that a caller must wait before the call can be considered abandoned. This value is called the *abandoned call wait time*. You can set this value for each peripheral. A typical value might be 10 seconds. This means that if the caller hangs up in the first 10 seconds, the call is

not considered abandoned, nor is it counted as a call offered. If the caller waits at least 10 seconds and hangs up, the call is counted as both offered and abandoned. (In the real-time data, a call is counted as offered as soon as it arrives at the peripheral. Therefore, a short call might appear as a call offered in the real-time data, but is not counted as offered in the historical data.)

Service Level

Service level is a measure of how well you are meeting your goals for answering calls. For each service, you can set a goal for the maximum time a caller spends in a queue before being connected to an agent. This value is the *service level threshold*. The service level is usually expressed as the percentage of calls that are answered within the threshold.

To calculate the service level for a period of time, the system software determines the number of calls that have had a service level event within that period.

A service level event occurs when one of three things happens to a call:

- It is answered within the service level threshold.

- It is abandoned within the service level threshold.

- It reaches the service level threshold without being answered or abandoned.

All calls that have a service level event within a specified period are considered as service level calls offered for that period. This differs from a simple call's offered value, which counts each call at the time it is first offered to the service.

Service Level Threshold

The *service level threshold* is the number of seconds you set as a goal for connecting a call with an agent. When you set up a peripheral, you can specify a default service level threshold for all services associated with that peripheral. When you set up each service, you can choose to either use the default threshold set for the peripheral or specify a threshold for the service itself in the Service Level Threshold field. If you do not specify a service level threshold for an individual service, the default threshold you specified for the peripheral is used. Typically, you must set these values to match the service level thresholds being used by the peripheral itself.

Service Level Types

Different peripheral types use slightly different formulas to calculate service level. The system software provides a uniform calculation across all peripherals. This allows you to apply uniform metrics and performance goals across all peripherals. However, the system software also tracks the service level as calculated by the peripheral itself. This is called the *peripheral service level*. You can use this value, for example, to continue to compare performance to historical norms.

Some peripherals let you select one of several types of service level calculation. You can specify which of these types of service level you want the system software to track.

The uniform service level calculation performed by the system software can be done in any of three ways:

- **Abandoned calls ignored**. The number of calls answered within the threshold divided by the number of calls that had a service level event minus the number of calls that were abandoned before exceeding the service level threshold. Calls abandoned before the service level threshold expired are removed from this calculation.

- **Abandoned calls have a negative impact on service level**. The number of calls answered within the threshold divided by the number of calls that had a service level event. This treats these abandoned calls as though they had exceeded the threshold.

- **Abandoned calls have a positive impact as service level**. The number of calls answered within the threshold plus the number of calls abandoned within the threshold, all divided by the number of calls that had a service level event. This treats these abandoned calls as though they were answered within the threshold.

The following example illustrates these different ways of calculating service level.

Example service level calculations

```
Call Counts

Answered within service level threshold: 70

Abandoned within service level threshold: 10

Exceeded service level threshold: 20

Total service level events: 100

Service Level Calculations

Abandoned calls ignored: 70 / (100 - 10) = 77.7%

Abandoned calls negatively impact: 70 / 100 = 70.0%

Abandoned calls positively impact: (70 + 10) / 100 = 80.0%
```

The value of the service level type field for the service determines how the system software treats abandoned calls. You set this value when you configure the service.

Configure Service Levels

Service level is set in various configurable windows in Configuration Manager, which you can define in different ways depending on the kind of information you want it to provide. See:

Configure Service Level for All Call Types

Service levels are set at the System Information level for all call types. To view or change the default system-level settings for all call types:

Step 1	In the Configuration Manager, select **Tools** > **Miscellaneous Tools** > **System Information**.
Step 2	Specify a value for Service level threshold in seconds.
	The default is *20 seconds*.
Step 3	Select the Service level type.
	The options are: *Abandoned Calls have Negative Impact*, *Abandoned Calls have Positive Impact*, and *Ignore Abandoned Calls*.
	The default is *Ignore Abandoned Calls*.
Step 4	Click **Save**.

Configure Service Level for Specific Call Types

To configure service levels for specific call types that override the System Information settings:

Step 1	In the Configuration Manager, select **Tools** > **List Tools** > **Call Type Lists**.
Step 2	Click **Retrieve**.
Step 3	Select the call type whose service level you want to set.
Step 4	For service level threshold, check the box to the right of the field to override the default from the System Information (*20 seconds*).
	Specify a service level threshold value in seconds for this call type.
Step 5	For service level type, check the box to the right of the field to override the default.
	Select from *Ignore Abandoned Calls*, *Abandoned Calls have Negative Impact*, and *Abandoned Calls have Positive Impact*.
Step 6	Click **Save**.

Configure Service Level for MRDs, Peripherals, and Skill Groups

Service level settings for media routing domains (MRDs), peripherals, and skill groups are hierarchical and are interpreted as follows:

Procedure

- **MRD** - The highest level. It is set in **Configuration Manager** > **Tools** > **List Tools** > **Media Routing Domain**.

  The default settings for the MRD are service level threshold = *30 seconds* and service level type = *Ignore Abandoned Calls*. Ignore Abandoned Calls is the only value, and it is protected.

- Peripheral - Is set in **Configuration Manager** > **Tools** > **List Tools** > **Service Level Threshold List**.

  The default settings for a peripheral are taken from its MRD. You can override them.

- Skill group - Is set in **Configuration Manager** > **Explorer Tools** > **Skill Group Explorer** > **Advanced** tab.

Skill group default settings are taken from their peripheral. You can override them.

This example explains the configuration.

1. The MRD has two peripherals. Each peripheral has two skill groups. The service level threshold for the MRD is set to the default of 30 seconds, By default, the service level thresholds for both peripherals is 30 seconds and the service level thresholds for all four skill groups is 30 seconds.

Figure 4: MRD Hierarchy Example 1: Service Level Threshold at the MRD
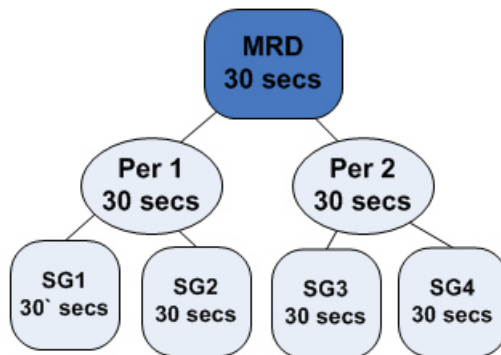
2. If you change the service level threshold of peripheral 1 to 20 seconds, the service level thresholds of skill groups 1 and 2 become 20 seconds. The service level thresholds of skill groups 3 and 4 remain at 30 seconds.

Figure 5: MRD Hierarchy Example 2: Changing the Peripheral
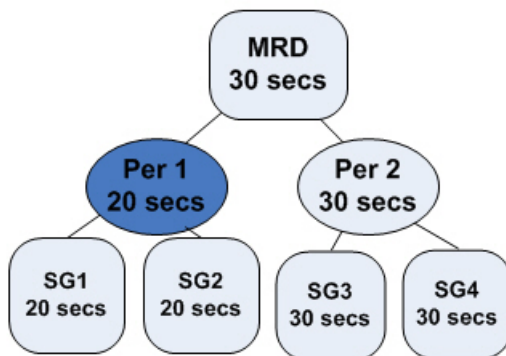
3. If you want the service level threshold of skill group 1 to be 45 seconds, you can independently configure skill group 1 to have a service level threshold of 45 seconds.

Figure 6: MRD Hierarchy Example 3: Changing the Skill Group
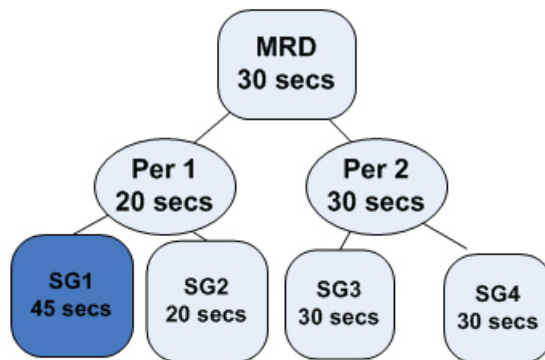
Configure Service Level for the MRD

To configure the service level settings for the MRD:

Step 1   In the Configuration Manager, select **Tools** > **List Tools** > **Media Routing Domain List**.

Step 2   Select the routing domain with the service level you want to modify.

Step 3   Click **Retrieve**.

Step 4   Select the MRD that has the service level you want to set.

Step 5   Specify a value in seconds for service level threshold. The default is 30 seconds.

Step 6   Service level type is protected and always shows *Ignore Abandoned Calls*.

Step 7   Click **Save**.

Configure Service Level for a Peripheral

To configure service level settings for a peripheral:

Step 1   In the Configuration Manager, select **Tools** > **List Tools** > **Service Level Threshold List**.

Step 2   Click **Retrieve** to populate the list with the peripherals.

Step 3   Select the peripheral that has the service level you want to modify.

Step 4   Specify a value for service level threshold. The default is inherited from the MRD.

Your options are to:

- Retain the default from the MRD.

- Check the Override MRD default box to unprotect the value and enter a new value in seconds for the peripheral service level threshold.

Step 5   For Service level type, check the box to override the default. Select from *Abandoned Calls have Negative Impact*, *Abandoned Calls have Positive Impact*, and *Ignore Abandoned Calls*.

For a non–Unified CCE peripheral and a voice MRD, select from *Abandoned Calls have Negative Impact*, *Abandoned Calls have Positive Impact*, and *Ignore Abandoned Calls*. For other MRDs, service level type is protected and always shows Ignore Abandoned Calls.

Step 6   Click **Save**.

Configure Service Level for Skill Groups

To configure service level settings for a skill group:

Step 1   In the Configuration Manager, select **Explorer Tools** > **Skill Group Explorer**.

Step 2   Click **Retrieve**.

Step 3   Select the skill group and click the Advanced tab.

Step 4   The service level threshold defaults to that of the peripheral.

Your options are to:

- Keep the service level threshold setting of the peripheral.

- Check the Override Peripheral default box to unprotect the value and enter a new value in seconds for the skill group service level threshold.

Step 5   The service level type defaults to that of the peripheral.

Your options are to:

- Keep the setting of the peripheral.

- From the drop-down menu, change to: *Abandoned Calls have Negative Impact, Abandoned Calls have Positive Impact*, or *Ignore Abandoned Calls*.

Step 6   Click **Save**.

Configure Service Level for the Precision Queue

To configure service levels for precision queues:

Step 1   Use the Precision Queue gadget to select the precision queues whose service level you want to set.

Step 2   Specify a value for service level threshold.

Step 3   Click **Save**.

Configure Service Level for an Aspect Call Center PG

To configure service level settings for an Aspect Call Center PG:

Step 1   In the Configuration Manager, select **Explorer Tools** > **PG Explorer**.

Step 2   Click **Retrieve**.

Step 3   Select and expand the PG.

Step 4   Select the peripheral and click the Peripheral tab.

For all peripherals except Aspect Call Center, the peripheral service level type field is protected and shows *Calculated by Call Center*.

For Aspect Call Center, choose the type of calculation to be performed by default. You can override the default for each individual service.

Unified CCE Administration

Unified CCE Administration Applications

Unified CCE Administration is a web-based user interface that contains multiple applications used to manage agents, calls, bulk jobs, and settings.

This section provides a brief description of each application. For detailed information about each application, see the online help that accompanies it.

Infrastructure Settings

Use the Infrastructure Settings to configure the following:

- Inventory: Deployment model and the components in the inventory for that model.

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

- Smart Licensing: Licensing model that delivers visibility into your license ownership and consumption. For more information on Smart Licensing, see the *Smart Licensing* section in *Administration Guide for Cisco Unified Contact Center Enterprise* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_5_1/administration/guide/ucce_b_administration-guide-for-cisco-unified12_5.html

Call Settings

Use the Call Settings to configure the following:

- Route Settings (Media Routing Domain)
- Bucket Interval

User Setup

This provides details of all the Agents configured.

Organizational Setup

Use the Organizational Setup to view and configure the following:

- Skills: This allows you to configure Precision Queue and Attributes.
- Business Hours: This feature allows you to configure Normal day business hours and Special Day business hours, in addition to holiday configurations.

Bulk Import

Use the Bulk Import tool to view and import in bulk, Agents and Single Sign-on settings

Features

Use the Features tool to view and configure features like Single Sign-on.

Configure Unified CCE Administration for Remote Access

To access Unified CCE administration remotely using Internet Explorer 11, you must add the configuration sever address to the list of trusted sites.

Note Administration clients and administration workstations can support remote desktop access. But, only one user can access a client or workstation at a time. Unified CCE does not support simultaneous access by several users on the same client or workstation.

Step 1 Launch Internet Explorer 11.

Step 2 Go to Tools > Internet Options.

Step 3 Select the **Security** Tab.

Step 4 Select **Trusted Sites**.

Step 5 Click the **Sites** button.

Step 6 In Add this website to the zone, type in the configuration server address as : **https://<IP address or FQDN>**.

Step 7 Click the **Add** button.

Step 8 Click the **Close** button.

Step 9   Click the **OK** button.

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

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 24
Understanding the License consumption Calculation	License Consumption Calculation, on page 36
Migration to Smart Licensing	Migrate to Smart Licensing, on page 38
Smart Licensing tasks in CCEADMIN	Smart Licensing Task Flow, on page 26
Best Practices	Best Practices, on page 41

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-Prem Cisco SSM.

  - **On-Premise:**

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

    2. Configure 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`

   - `-import keytool.exe <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>`

3. Enter the truststore password when prompted.

4. Enter 'Yes' when prompted to trust the certificate.

5. Restart the Tomcat service.

Related Topics

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

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

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

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

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

Step 3 Generate the Product Instance Registration Token.

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

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

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CCE and Cisco SSM.

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

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

Step 3 Select the connection method to Cisco SSM:

- **Direct**—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.

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

Select License Type

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

- **Flex**—Flex license is a recurring subscription of Standard and Premium license. These subscriptions are renewed periodically, for example 1, 3, or 5 years.

- **Perpetual**—Perpetual license is a permanent and one-time payment license that offers a Premium license.

- **Production**—Production mode is when the licenses are used on live systems to handle actual production traffic. Yes

- **Non-Production**—Non-production mode is used for labs, testing and/or staging areas, and not for live systems handling actual end-consumer traffic.

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

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

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

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

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

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

License Type	Licenses
Flex Production	**Unified CCE and Packaged CCE:** • 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

License Type	Licenses
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.

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
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

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.

Status	Description
Registration Expired	Product registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months.

Authorization Status

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

Table 4: Authorization Status

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

License Entitlement Status

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

Table 5: License Entitlement Status

Status	Status Description
Authorization Expired	Product authorization has expired, when the product has not communicated with Cisco for 90 days.
Not Authorized	Product instance is not authorized.
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
In Compliance	Product is in authorized or in compliance state. Authorization is renewed every 30 days.

Status	Status Description
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

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 7: License States
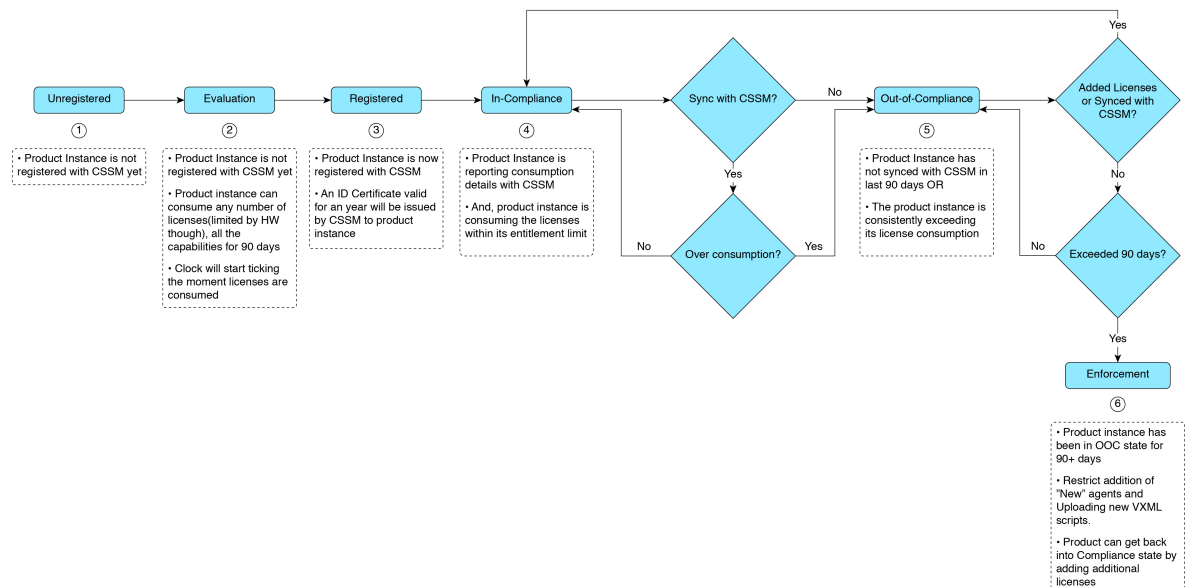
Notifications and Alerts

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 8: 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.

For more information, see *Cisco Unified Contact Center Express Reporting User Guide*.

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 9: License Computation

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

CCE Premium Agents Purchased = 100
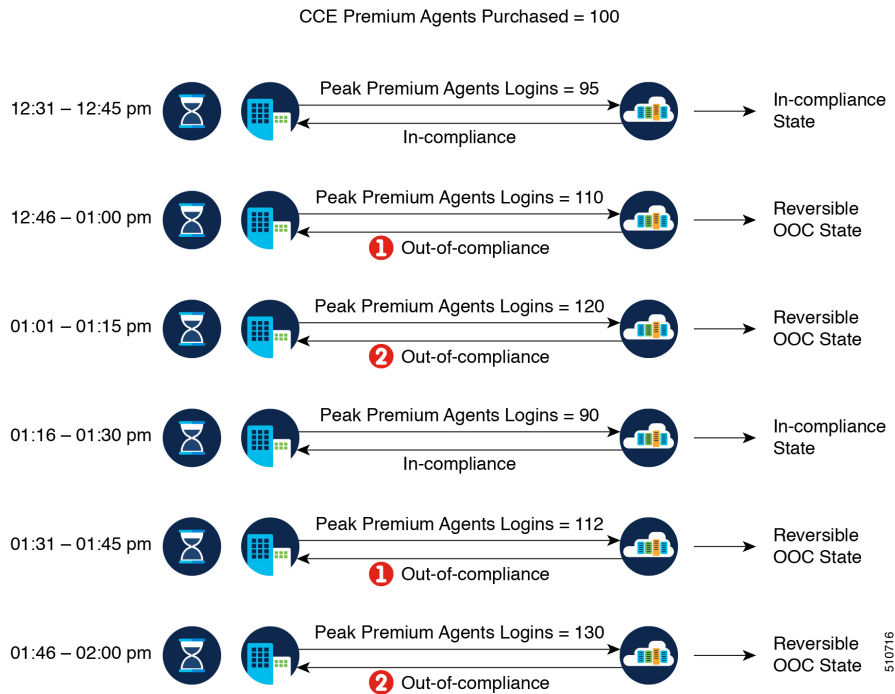
In the example, the Product Instance is back to In-compliance state after two instances of overage. The next time the Product Instance goes Out-of-Compliance, the count will be 1 of 5. So, you get 45 min (after the first Out-of-Compliance notification from Cisco SSM) to bring back the consumption within 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

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

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

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

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

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

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

Renew Registration

Use this procedure to manually renew your certificates.

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

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

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

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

Reregister License

Use this procedure to reregister 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.

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.

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.

Configuration Manager

Access Configuration Manager

To access the Configuration Manager do one of the following:

Procedure

- Double-click the **Unified CCE Administration Tools** folder icon, then double-click the **Configuration Manager** icon.
- From the **Start** menu, select **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Configuration Manager Menus

When you start the Configuration Manager, the Configuration Manager window appears. The figure following shows the window with the top-level directories displayed for all its menus.

Figure 10: Configuration Manager
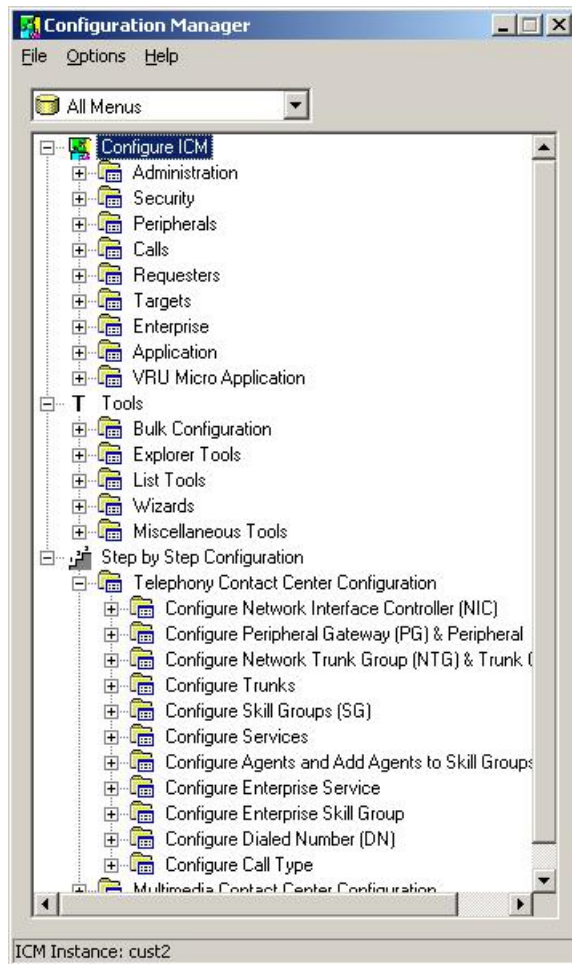
The Configuration Manager lets you view and update configuration information in the Unified ICM database. The configuration information describes the people, groups, and devices that are part of your enterprise.

To set up the configuration of a new system when you are a new user, follow the steps in the menu bar's Step by Step Configuration selection list.

Use the tools in the Telephony Contact Center Configuration menu in the order given to configure, first NICs, then peripherals. After you configure the system software for your telephony contact center, you can configure the software for multimedia applications.

The tools in the MultiMedia Contact Center Configuration menu are also in the order in which you generally use them. For example, you must have a media class before you can create an MRD for that class. And you must have an application instance before you can specify the path to that application.

To access:

- The configuration tools according to the menu selections of the former Configure ICM tool, in the menu, select **Configure ICM**.

- All the tools you can use in the Configuration Manager, in the menu bar, select **Tools**.

Online Help

For information about any Configuration Manager tools, menu options, or other interface features, refer to the online help.

You can activate help from within the system software in any of three ways:

- Click **Help** in the tool bar or in the dialog

- Select **Help** > **Help Contents** from the menu bar

- Press the **F1** key

Configuration Manager Tools

Use the menu bar in the Configuration Manager window to select the task or tool you want.

Table 6: Tools Summary

Tools	Description
Bulk Configuration Tools, on page 45	Enable you to configure multiple records at a time.
Explorer and List Tools, on page 46	Enable you both to view records and their related records and to define, edit, and delete them and their relationships. Explorer tools manage records that have more than one relationship; List tools manage records that have no or only one relationship to other records.
Miscellaneous Tools, on page 48	Help you perform configuration tasks for which the previous tools are not appropriate.
Wizards, on page 49	Guide you through configuration tasks.
Outbound Option	Adds outbound dialing functionality to the existing inbound capabilities of the system software. **Note** Refer to the *Outbound Option Guide for Unified Contact Center Enterprise* and the online help for detailed information about Outbound Option.

Note   Refer to each tool's online help for detailed information.

Bulk Configuration Tools

Use Configuration Manager's bulk configuration tools to configure multiple records at a time.

The bulk configuration tools enable you to bulk configure the following individual database table records.

The tools are named for the records they manage:

- Agents

- Call types

- Dialed number plans

- Dialed numbers

- Device targets

- Labels

- Network trunk groups

- Network VRU scripts

- Peripheral targets

- Person bulk tool

- Regions

- Region prefixes

- Routes

- Trunks

- Trunk groups

- Scheduled targets

- Services

- Skill groups

- VRU port maps

Note Refer to each tool's online help for detailed information.

Related Topics

Explorer and List Tools

Use Configuration Manager's Explorer and List tools to configure and manage individual database records.

Explorer Tools

Use the Explorer tools to configure and manage database records that have hierarchical relationships to other records. In this way, at one time, you can see and update both the individual records and their relationships. You can configure and manage the following records with the Explorer tools.

The tools are named for the type of records they manage:

- Agent Explorer

- Announcement Explorer

- Database lookup Explorer

- Device target Explorer

- ICM instance Explorer

- Network VRU Explorer

- Network trunk group Explorer

- NIC Explorer

- PG Explorer

- Region Explorer

- Scheduled target Explorer

- Service Explorer

- Service array Explorer

- Skill group Explorer

- Translation route Explorer

Note   Refer to each tool's online help for detailed information.

List Tools

Use the list tools to configure and manage database records that have limited or no hierarchical relationship to other records. You can configure and manage the following individual records with the list tools.

The tools are named for the type of records they manage:

- Agent desk settings list

- Agent targeting rule list

- Agent team list

- Application gateway list

- Application instance list

- Bucket intervals list

- Business entity list

- Call type list

- Class security list (on partitioned systems only)

- Dialed number/script selector list

- Enterprise route list

- Enterprise service list

- Enterprise skill group list

- Expanded call variable list

- Expanded call variable payload list

- Feature control set list

- Label list

- Media class list

- Media routing domain list

- Network VRU script list

- Person list

- Reason code list

- Service level threshold list

- Supervisor list

- User list

- User group list

- User variable list

- VRU currency list

- VRU defaults list

- VRU locale list

Note   Refer to each tool's online help for detailed information.

Miscellaneous Tools

The following Configuration Manager tools enable you to do miscellaneous functions not available with the other tools:

- **Deleted objects**: Enables you to view all records deleted from the database and to permanently delete them if you no longer want them.

- **Integrity check**: Allows you to perform specific integrity checks on the configuration data in the Unified ICM database.

- **Region editor**: Allows you to:

    - View, create, update (cut, copy, paste, move, or edit), and delete custom regions.

  • View, copy, move, or delete predefined regions, but not edit them.

- **Script reference**: Allows you to generate a report that shows which routing scripts reference a specific configuration record.

- **System information**: Allows you to view and set general and application gateway information about your enterprise.

- **Unreferenced objects**: Lists the database tables that have unreferenced records. Use this tool to find specific integrity problems within the database.

Wizards

Two wizards guide you through the configuration of:

- Translation routes (Translation route wizard)

- Call center applications (Application wizard)

Use these wizards for step-by-step guidance.

Explorer, Bulk, and List Tools Common Features

The Explorer, Bulk, and List tools have the following common features:

- **Common filter access**

  To access data from the database, in the *Select filter data* box of the Bulk, List, or Explorer Configuration Insert tool window, select the type of data you want and click the **Retrieve** button.

- **Record status symbols**

  When you make an edit, the record's status symbol updates accordingly. This appears to the left of the record name in the list box of the Explorer or List tool and in the State column of the bulk tool.

Table 7: Record Status Symbol Descriptions

Symbol	Description
☑	A green check mark means the object has not changed since you retrieved it from the database or made a save. **Note** This feature is not common to the Explorer tools.
☒	A red X means the object is marked for deletion and will be deleted when you click the **Save** button.
➡	A yellow arrow means that the object's data has been changed and the changes have not yet been saved in the database.
➕	A yellow addition sign means the object is to be inserted into the database when you click the **Save** button.

Symbol	Description
	A red circle with a red slash through it indicates the object was created using an application and is controlled by the application object filter (AOF) or by peripheral auto-configuration.

Other common features:

- **ID status box**

  The label in the ID box at the bottom of the screen identifies the Unified ICM system (instance) on which you are working.

- **Delete/Undelete button**

  When a record is selected and you click the **Delete** button, that button toggles to **Undelete** and a red X marks the record for deletion. As soon as you save your database changes, marked records are deleted from the database.

- **Save button**

  No changes are made to the database until you click the **Save** button.

Explorer and List Tools Common Features

The list and Explorer tools share the following features.

- **List box of retrieved records**

  Both the Explorer and list tools have a list box that displays retrieved records. Selecting a record in this list displays that record's properties in the right side of the tool window. After the record is displayed, you can edit it if you have maintenance access to it.

  Retrieved records:

  - **Tree** (only in Explorer tools)

    In an Explorer window, the retrieved list is called a directory *tree*, which you can expand or contract to show a hierarchy of records. A *legend* above the tree identifies the types of records that you can display in the tree.

    With the mouse, you can select a record in a tree and move it to another part of the tree, as long as its object type belongs in that tree location.

  - **UNASSIGNED** (only in Explorer tools)

    The Explorer tree can also contain UNASSIGNED records. These are stored in an UNASSIGNED directory for the selected directory tree object.

    A record is named UNASSIGNED if it was not assigned (mapped) to a parent object. For example, a label created in the bulk configuration tool might not have been assigned to a peripheral target, or a route might not have been assigned to a service.

    You can also use the label bulk configuration tool to take the output of a switch and create 20 or 30 labels. Then, using an Explorer tool, you can attach the labels to an appropriate location.

  - **List** (only in List tools)

In a list window, the retrieved list is called a *list* and has no legend above it since its records have no or only one relationship to another record.

- **Adding new records**

  The **Add** button is enabled only after you use the Select filter data section of the window.

  In the Explorer tools, when a record in the tree is selected, you can add another record of the same kind or a record immediately below it in the tree hierarchy. In the List tools, the **Add** button is enabled only for the single type of records listed.

- **Deleting Records**

  Selecting a record and clicking **Delete** marks the record (with a red X) for deletion. However, the record is not deleted until you click **Save**.

  Delete toggles to **Undelete** when you select an object marked for deletion. To undelete an object marked for deletion, select it and click **Undelete**.

- **Options menu**

  In the Explorer and List tool windows, right clicking on a retrieved record displays an options menu containing all the editing options for that record.

> **Note** The options menu is not available in the List tools if you have read-only access.

Database Records Access

The Bulk Configuration, List, and Explorer tools enable you to access records from the database in the same way. In these tools, use the Select filter data box to select and retrieve data from the database. Until you retrieve database data, no data is displayed.

In the top left of the Bulk Configuration Insert, the Explorer, and the List Tool windows is a *Select filter data* box similar to the following.

Figure 11: Select Filter Data Box

In this example, all records belonging to the Boston_PG_1 peripheral and having Jo in their names are selected for retrieval from the database.

The filters used to select data vary according to the type of data. In the preceding example, data is first selected by peripheral and then by name. Some filter selection boxes have only optional filters.

To achieve maximum response time when retrieving records:

- Always select a specific member from the primary filter, even if only one exists. For example, for the Dialed number/script selector list tool, always select a specific routing client and customer. In addition to reducing the number of records loaded and listed, this also improves response time when navigating through the list of records and when adding new ones.

- Specify an optional filter whenever possible to further reduce the number of records retrieved. For example, when using the Dialed number/script selector list tool, this could be a **Name**, **Dialed number string**, or **Description**.

- Separate the operation of adding records from editing existing records. In addition to selecting the targeted primary filter, specify a unique optional filter for the new record that will result in no existing records being loaded. For example, when using the Dialed number/script selector list tool, specify the exact dialed number string to be added. The retrieval response time will be almost instantaneous and the list of records being added will be easier to manage.

If any editable field is changed, an additional dialog appears (below the *Select filter data* dialog) displaying the original filter settings. In addition, the Tree List box and all buttons except **Retrieve**, **Close**, and **Help** are disabled.

Clicking **Close** cancels the filter changes and returns the fields to their original settings. Clicking **Retrieve** closes the *Select filter data* dialog and enables the display (in the tree list box) of the record retrieved based on the selected filter criteria.

The following table describes how the optional filters, the check box, and the filter buttons work for all the Bulk Insert, Explorer, and List tools.

Table 8: Common Filter Functions

Filter item	Function	
Optional filter	**None** in the optional filter box means no optional filtering. All data is displayed for the selected records. The optional fields to filter on differ by record type according to both the fields in a record and the fields considered useful as filters.	
Condition	**If the selected optional filter is**	**Then**
	None	The Condition filter is ignored.
	A text filter (for example, description)	Select one of the text conditions (Contains, Ends With, Starts With, Is Blank) and enter an appropriate entry in the value field.
	A numeric filter (for example, trunk number)	Select one of the numeric conditions (Equal, Greater Than, Less Than, Not Equal) and enter an appropriate entry in the value field. The available numeric conditions can change depending on the record data. For example, Equal or Not Equal might be the only choices.

Filter item	Function
Value	The entry in this field is based on the selections made in the optional filter and condition fields. If None is selected in the optional filter field, this field is ignored.
Save check box	If checked, indicates that the current settings are saved so that when you next open the list tool for this type of record, the current settings will be selected. However, no data is displayed until you click the **Retrieve** button.
Retrieve button	This button displays the data selected in the Select filter data box.
Cancel filter changes button	If you change the optional filter settings after a retrieve, clicking this button resets the filter settings back to the preceding ones.

Save Configuration Data to Database

When you have completed adding information in an open configuration window, click **Save**.

The system software saves the configuration data and immediately applies your changes to both the local and central Unified ICM database.

Note

- Whenever any data is retrieved by a configuration tool, the tool notes the last change mark on that data at this point in time. If you attempt to change that item, the tool first checks the current copy in the database for its change mark. If the change marks do not agree, another user has changed this item since you last retrieved it, and an error is returned. You must then discard any changes, using **Retrieve** to obtain the latest information for editing.
- This approach is called *optimistic* locking, and assumes that it is rare to have two people needing to change the same item at the same time. This prevents the performance and maintenance issues involved with hard-locking items, while still preventing one person from accidentally overwriting another user's changes.

Feature Control

In general, feature control addresses the need of restricting users, or classes of users, from all functionality of the system software. Feature control is a method of security for prohibiting access to the system software features.

Script Editor feature control addresses the need of restricting users, or classes of users, from some or all of the functionality of the Script Editor software. In a possible deployment scenario, a system software administrator can restrict certain people from doing specific types of script editing. Similar functionality was previously available in the system software in the Limited (Single Instance) Administration & Data Servers feature control.

An administrator has two means to restrict access to the editing features of Script Editor and Internet Script Editor:

- Edit options

• Script node control

It is also possible for an administrator to use a combination of both feature control options.

Refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* for more feature control information.

Script Node Control

Script node control allows an administrator to create feature sets that can be assigned to users. The feature set controls which script nodes are accessible to the user.

Node Control Table

The node control table (in the Configuration Manager Script Editor Feature Control dialog) has two columns, the Node column and the Available column. This table allows an administrator to create feature control sets that can be assigned to users. The feature control set controls which script nodes are accessible to the user.

If a script is opened that contains a disabled node, you can browse or monitor the script but you cannot put the script into edit mode. If you attempt to put this script into edit mode a message indicating you are not authorized to enter edit mode is displayed. However, you can still Quick Edit the script, just not the node.

Node Column

A *node* is an executable element within a script. A *script* consists of nodes, connections, routing targets, and comments. Every script begins with a Start node. The node column lists of all the nodes that can be used in a script.

Available Column

Each checked node in the available column appears on the editing pallet of the feature-control-set user, regardless of the edit mode (Full Edit or Quick Edit Only).

There are two possible presentation effects:

• Enabled nodes are displayed on the object palette

• Disabled nodes are removed from the object palette

Configuring a Feature Control Set

Configuring a feature control set consists of:

• Creating a feature controls set (see Create a Feature Control Set, on page 54)

• Assigning users to a feature controls set (see Assign Users to a Feature Control Set, on page 55)

• Selecting the script nodes available in a feature controls set (see Select Script Nodes for a Feature Control Set, on page 55)

Create a Feature Control Set

The system administrator can create a feature control set using the Configuration Manager on the Unified ICM Administration & Data Server:

Step 1	Ensure any users to be assigned a feature set are configured.
Step 2	Start the Configuration Manager by clicking open **Administration Tools** > **Configuration Manager**. . The Configuration Manager dialog opens.
Step 3	Select **Tools** > **List Tools** > **Feature Control Set List**.
Step 4	In the Feature Control Set section (on the left), click **Add**.
Step 5	Select the **Attributes** tab.
Step 6	Enter the name of the feature control set. The name appears in the left section when **Enter** or **Tab** is pressed.
Step 7	Enter a description (optional).

Assign Users to a Feature Control Set

The system administrator can assign users to a feature control set:

Step 1	Start the Configuration Manager by clicking open **Administration Tools** > **Configuration Manager**. . The Configuration Manager dialog opens.
Step 2	Select **Tools** > **List Tools** > **User List**.
Step 3	Select the user to whom a feature control set is to be assigned.
	Note If no users appear, add users (who already exist in Active Directory) using the User List tool.
Step 4	On the **Attribute** tab, select the feature set for the selected user.
Step 5	Click **Save** when you are finished assigning feature sets.

Select Script Nodes for a Feature Control Set

To select script nodes:

Step 1	Select the name of the feature control set to be assigned.
Step 2	Select the **Attributes** tab.
Step 3	Select **Script Editor** > **Advanced**.
Step 4	In the Script Editor Feature Control dialog, select the nodes for this feature control set and an edit option (Full Edit or Quick Edit).
Step 5	Click **OK**.
Step 6	Click **Save**.

Configuration Data Validation

After making changes or additions to your configuration, you must always check that the configuration is internally consistent and complete.

| **Note** | It is especially important to perform integrity checks if you have imported data from another source. |

Check Integrity of Configuration Data

To check the integrity of your configuration data, perform the following:

Step 1 In the Configuration Manager, select **Miscellaneous Tools** > **Integrity Check**. The Integrity Check dialog appears.

Step 2 Choose the type of check option that you want to perform or click **Select All** to choose all the check options. (For specific information about each of these options and the tables and fields they check, refer to the Configuration Manager online help.)

Step 3 Click **Perform Check**. The Configuration Manager performs the check and one of the following happens:

a) If the check discovers a problem, the Configuration Manager displays messages in the Integrity Problems text box. Double-click on a message to receive specific information about the records in the data table at the bottom of the window.

b) If the check completes without finding any invalid data, the Configuration Manager displays a message saying the integrity check completed successfully.

Step 4 When all checks are complete, click **Close**. The Integrity Check dialog closes.

Many database records need references to related records. For example, each peripheral target must reference a route and each trunk group must reference a network trunk group.

Check Record References

To check record references, perform the following:

Step 1 In the Configuration Manager menu, select **Miscellaneous Tools** > **Unreferenced Objects**. The Unreferenced Objects dialog appears listing the database tables containing objects that are missing references.

Step 2 To see the specific rows that are missing references in a table, double-click on the table name. Double-clicking on a table name entry displays that table showing the records that are missing references.

Configuration Record Deletion

At some point, you might want to remove configuration records from your database; for example, if data has been entered in error or changes occur in your business.

Delete a Record

To delete a record:

Step 1 Within Configuration Manager, open any one of the tools in which you can configure that type of record and retrieve the record.

Step 2	Select the retrieved record.
Step 3	Click **Delete**. A red X (marked for deletion) appears in the window next to the name of the record. The **Delete** button toggles to **Undelete**. To undelete the record, select it and click **Undelete**.
Step 4	Click **Save** to save the deletion to the database. The record is deleted from the database and is removed from the window.
	Note — Some deleted records can still be viewed, as described in Configuration Record Deletion.
Step 5	Click **Save**. The deletion is saved to the database and the record disappears from the window.

Related Topics

Configuration Record Deletion, on page 56

Types of Deletion

Depending on the record involved, the Configuration Manager performs one of two types of deletion:

- **Immediate deletion**. The system software immediately removes the record from the database. (Also known as *physical deletion*.)

- **Logical deletion**. The system software sets the record's Deleted field to **Y** (yes), but the record remains in the database. The Configuration Manager and the CallRouter treat the record as though it were deleted. The record remains in the database, however, for historical reporting purposes.

Immediate Deletion

Some tables — for example, the Skill Group Member table, which maps agents to skill groups — do not have a Deleted field. When you delete a record from such a table, the system software immediately removes the record from the central and local database.

Logical Deletion

Other tables, for example, the Skill Group table, which describes a skill group associated with a peripheral — do have a Deleted field. When you delete a record from such a table, the system software does not remove the record from the central and local database. Instead, the system software sets the record's Deleted field to **Y** to indicate that it is logically deleted.

Logical deletion ensures that any references to the record — for example, references to a skill group in call detail records — remain valid. However, the Configuration Manager and the Script Editor treat the record as though it were deleted.

⚠
Caution Never attempt to set a configuration record's Deleted field directly. Changing a Deleted field directly can compromise the integrity of your Unified ICM database. Use the Configuration Manager **Tools** > **Miscellaneous Tools** > **Deleted Objects** option to permanently remove logically deleted records.

Deletion Dependencies

How a configuration tool processes a record deletion request depends on whether, and how, the record is referenced by other configuration records:

- If no other records reference the current record, the configuration tool deletes the record.

- If other records reference the current record — and the configuration tool can neither modify the references nor delete the other records — the configuration tool does not delete the record.

Administering Deleted Records

The Configuration Manager lets you view logically deleted records. It also allows you to permanently delete these records.

How to View Deleted Records

To view deleted records, perform the following:

Step 1 In Configuration Manager menu, select **Tools** > **Miscellaneous Tools** > **Deleted Objects**. The Deleted Objects dialog appears, indicating the tables in which records are marked for deletion and the number of records so marked.

Step 2 To see the specific records marked for deletion within a table, double-click on a table name. If you double-click on a table name entry, a list window appears showing records from that table that are marked for logical deletion.

Step 3 To remove records from the database entirely, select a record from the list (or use the **Select All** button to select all) and click **Delete Permanently**. The Configuration Manager displays a message indicating the operation completed.

You must have access rights to a record to be able to delete it permanently.

Step 4 Click **Close** to close the dialog.

Bucket Intervals

You can configure call type intervals in relation to your service levels. For example, if your service level threshold is 15 seconds and you want to see when callers are abandoning within that service level, you can set intervals of 5 seconds, 10 seconds, and 15 seconds.

Associate Bucket Intervals with Call Types

Step 1 From the Configuration Manager, open the Call Type List tool.

Step 2 Click **Add**.

Step 3 In the **Name** field of the Attributes tab, assign the new list a name.

Step 4 Select the **Customer** from the pull-down menu.

Step 5 Check the **Override System Information Default** box for the Bucket Intervals section.

Step 6 Using the pull-down menu, select the desired Bucket Intervals list.

Call Types on the Child Central Controller

Access the Configuration Manager on the Child Administration & Data Server to configure call types.

Configure Call Types on the Child Central Controller

To configure call types on the Child Central Controller with the Configuration Manager Call Type List Tool:

Step 1   Start the Call Type List Tool.

Step 2   In the Main window of the Call Type List Tool, click **Retrieve**.

Step 3   Click **Add**.

The Call Type Attributes tab appears.

Step 4   Set **internal_2500CT** as the Name, then select **bh03** as the Customer setting.

Step 5   Click **Save**.

The call type appears in the tree list.

Step 6   Repeat this process to add two more call types (**internal_2501CT** and **internal_2502CT**).

When finished, you have the following call types:

- internal_2500CT

- internal_2501CT

- internal_2502CT

Step 7   Click **Save** next to the green checkmark, and then **Close** to exit the Call Type List Tool.

Supervisors with Teams on Multiple Peripherals

You cannot assign agents from different peripherals to the same supervisor's team. However, you can create supervisors on multiple peripherals that use the same Person record.

✎

Note   Use the **Select Person** drop-down list to create separate supervisors for each peripheral.

To see all their teams, the supervisor uses a different URL to open the Finesse instance for each peripheral. Open each Finesse instance in a different browser window. Each browser shows only the teams from the Finesse instance that is configured for that peripheral.

CHAPTER 5

Multiple Record Configuration

Access Bulk Configuration Tools

Step 1 Double-click **Configuration Manager** in the Administration Data Server group or the Administration Client group.

Step 2 In the Menu selection box, select **Tools** > **Bulk Configuration**.

Step 3 From the submenu selection list, select **Insert** if you need to insert data or **Edit** if you need to edit.

Step 4 In the next menu selection list, select the type of table with which you need to work.

Bulk Configure Data

From the Bulk Configuration menu, you can choose to create or update records in the database tables.

Start by selecting the **Bulk Configuration Insert** or **Edit** menu. Then select the database table you want to modify.

✎

Note If you have any questions, refer to the online help. The help contains table record and field definitions and procedures for all that you can do with the Bulk Configuration tool.

The following sections briefly describe the tool and how to use it.

Insert and Edit Windows

Depending on whether you select **Bulk Configuration Insert** or **Edit**, the Bulk Configuration Insert or Edit window for the selected database table opens.

These two windows have the following features:

- *Same Options*

  Both windows have the same options except for Insert (Insert window) and Retrieve (Edit window).

  Note The reason for having both an Insert and an Edit window is to prevent confusion when editing records since some configuration objects can only be edited when inserted into the database, the database being a relational one. For example, when you insert the record of a label, you can edit all its fields. However, after you define its routing client (and save it in the database), the only way you can redefine the routing client is by deleting the label and creating a new one.

- *Saving Changes*

  The changes you make in the Insert or Edit window are not applied to the database until you click **Save** or **Close**. The **Close** button closes the window and allows you to save or cancel database changes.

- *Initial Display*

  Initially, both windows open without data and wait for your retrieval command (in the Edit window) or insert/import command (in the Insert window).

- *Editable Data Table Fields*

  Columns with an asterisk (*) next to the title indicate required fields. You cannot directly modify fields shaded in **blue**. However, in some cases setting or changing one field makes another field updateable.

- *Record State*

The first data column contains a symbol indicating the condition of a row's record.

Symbol	Indicates the record is
☑	*Not changed* since you retrieved the record or saved it.
⇨	*Changed* in the current editing session but not yet saved.
⊕	*To be inserted* into the database when you save your edits.
☒	*To be deleted* from the database when you save your edits.

Multiple Record Configuration

In some cases, you might need to work with multiple records of configuration data simultaneously.

For example, you might want to:

- Import records from a text file

- Modify a specific field in multiple records

- Insert a set of records

This chapter shows you how to use the Configuration Manager Bulk Configuration tool to insert and update multiple configuration records in a single transaction from a single screen.

The Bulk Configuration tool lets you perform these operations on several Unified Intelligent Contact Management (Unified ICM) data tables simultaneously. This tool supplements the Configuration Manager Explorer and List tools, which allow you to insert and update single records.

Note   Refer to the Bulk Configuration tool's online help for detailed information.

Bulk Configuration Features

You can do the following with the Bulk Configuration tool:

- Retrieve records from the database (Edit window only)

- Sort records by a single column or by multiple columns

- Use the search tool to find data in a list of records

- Apply a single value to a range of fields or apply a range of values to a range of fields

- Insert additional new rows (records) into the database table (Insert Window only)

- Import multiple record data (either whole records or record fields)

- Export multiple record data (either whole records or record fields)

- Set or change security settings to multiple records at a time

- Delete records. After deletions are saved to the database (or after you close your editing session), you can no longer undelete deleted records.

- Undelete records that are marked for deletion in the current editing session

The following sections describe how to use the Bulk Configuration tool.

Record retrieval from database

Use the *Select filter data* box in the Edit window to retrieve records from the database.

Edit Existing Records

To retrieve and edit existing records, follow these steps:

Step 1   Within the **Bulk Configuration** > **Edit** menu, select the name of the database table you want to modify. The appropriate Edit window appears. (Initially, no records are shown.)

Step 2   Do one of the following:

- To retrieve a range of records, specify values in the **Select filter data** fields. For example, you could enter values that would retrieve only dialed numbers associated with a specific customer, with a specific routing client, or both.

- To retrieve all records, leave the Customer and Routing Client fields set to **All.**

Step 3   Click **Retrieve**. The appropriate rows are displayed in the Edit window as in the following example.

Figure 12: Example Bulk Configuration Edit Window
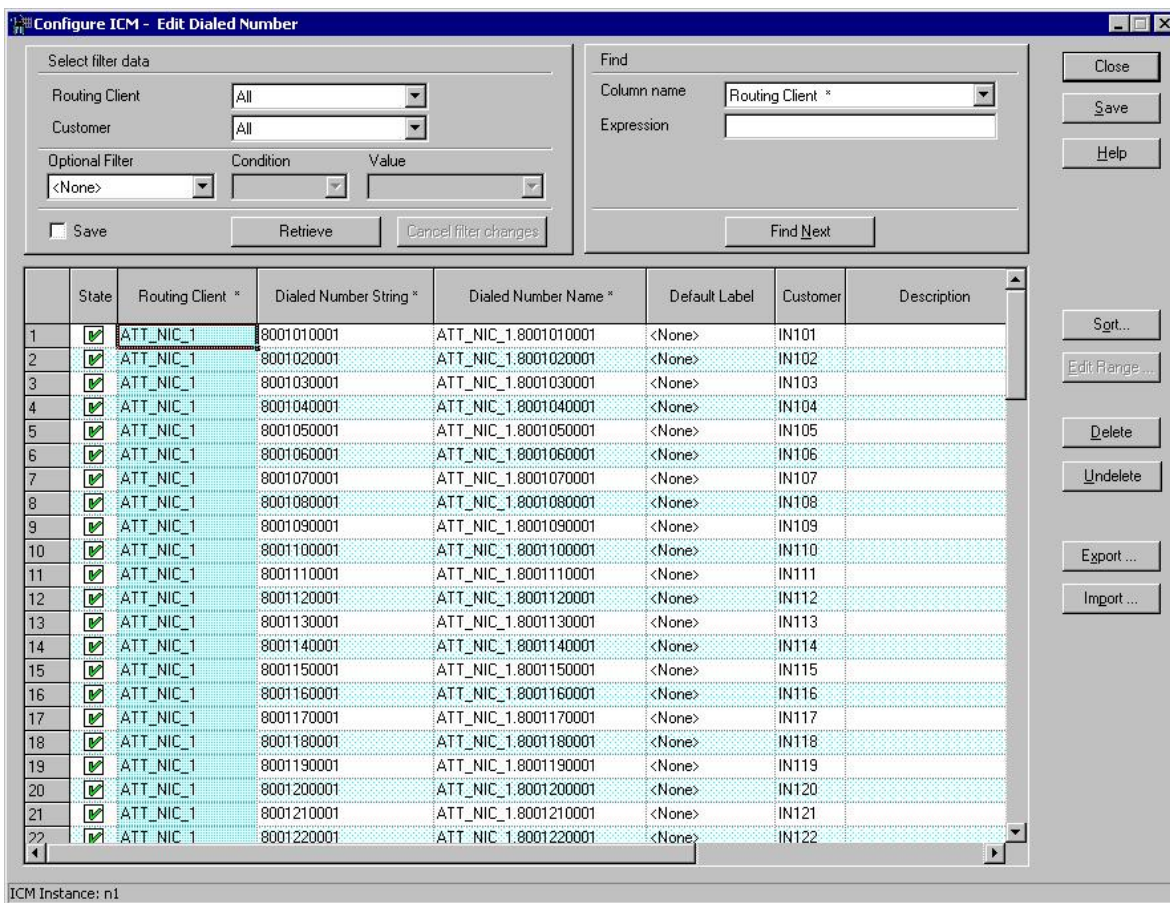
Step 4   After you retrieve the records you want to edit, you can edit individual records or a range of records. In a range of records, you can enter a range of values or the same value. You can also delete, import, export, and sort records.

Sorting Records

You can sort records (rows) in two ways: by one column or by multiple columns.

You might want to sort by multiple columns if the first column(s) to sort by has the same value in more than one field, for example, the same routing client, label, or customer name.

- To sort records by one column: double-click that column's header. To reverse the sort, double-click a second time. When you double-click, an A (Ascending) or D (Descending) appears after the header to indicate the sort order.

- To sort records by multiple columns, see the following procedure.

Sort Records by Multiple Columns

Step 1   In the Insert or Edit window, click **Sort**. The Sort dialog displays.

Step 2   In the *Columns available for sort* list, select each column by which you want to sort and click **Add**.

The primary sorting column will be the first column listed in the Columns selected for sort list. To change the column sort order, select a column and click the up or down arrow.

The data within each column is sorted in Ascending order unless you deselect the check box beside the column.

Step 3   Click **OK**.

Specific Records Within a Set

After you have retrieved a set of records, you can use the Find area of the Edit window (Column Name and Expression fields) to search for specific records within the set.

Find Data in a List of Records

To find data in a list of records, follow these steps:

Step 1   In the Find box of the Edit or *Insert* window, select the database column in which you want to search for data.

Note   You can also select a column by clicking in that column.

Step 2   In the Find box Expression field, enter the value for which you want to search. You can enter a full value or a sub-string.

Step 3   Click **Find Next** to locate the first record that matches the search criteria. The first row that contains the specified expression in the selected column is highlighted.

Select Data

You can select whole records for importing, exporting, setting security, deleting, or undeleting. Or, you can select the same field in multiple records for simultaneous editing.

Select Records

Click in the left-most numbered field in a row to select that row and highlight it. Click in any other field in a row to select the row but not highlight it.

Select One Field in Multiple Records

You can select one edit-control field (when there is no section box in the field) in multiple records in any of the following three ways:

- Click the field where you want to start and, keeping the left mouse button held down, move the cursor to the last field.

- Click the field where you want to start. While holding down the **Shift** key, click the last field.

- Click the field where you want to start. While holding down the **Shift** key, click the down arrow to select.

- Press **Ctrl,** then click on each field you wish to select. This allows you to select a discontinuous group of fields.

Edit Range of Data

You can edit a range of data in a table column in three ways:

Procedure

- Apply a single value to a range of edit-control fields
- Apply a single value to a range of selection-box fields
- Apply a range of values to a range of fields

Apply a Single Value to a Range of Edit-Control Fields

An *edit-control field* is one you can edit that does not contain a selection box.

To apply a single value to a range of edit-control fields:

Step 1   Make your selection: click the field where you want the range to start and, keeping the left mouse button held down, move the cursor to the last field in the range.

Step 2   Type the new entry that you want to appear in all the fields.

Step 3   Click **Enter** or **Tab**. This applies the change to all the records in the range and moves the focus to the next data field.

Apply a Single Value to a Range of Selection-Box Fields

To apply a single value to a range of selection-box fields:

Step 1   Select the first field where you want the range to start.

Step 2   Press the **Shift** key and hold it down for steps 3, 4, and 5.

Step 3   Click the selection-box down arrow but keep the left mouse button held down and select the fields you want in the range.

Step 4   Click the last field in the selection to display the selection list. You can also open the selection box by pressing **Alt** + an arrow key.

Step 5   Click your selection.

Step 6   Click **Enter** or **Tab** (or any other field). This applies the change to all the records and moves the focus to the next data field.

Apply a Range of Values to a Range of Fields in a Column

To apply a range of values to a range of fields in a column:

Step 1   Select the range of fields in a database column. This enables the **Edit Range** button.

    Note   The **Edit Range** button does not work for selection-box fields.

Step 2   Click **Edit Range**. The Edit Range dialog displays.

Figure 13: Edit Range Dialog Box
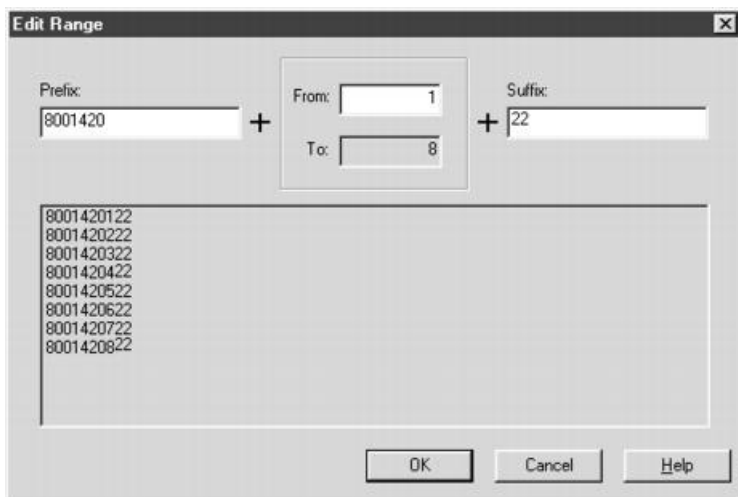
Step 3   In the Edit Range From field, enter the first number of the range.

Step 4   In the Prefix and Suffix fields, you can optionally enter substrings to appear before or after each value. The Edit Range dialog lists the generated values.

    Note   When entering a numeric range, you may also enter leading zeros to ensure proper alignment (that is, 001 to 999).

Step 5   Click **OK**. This applies the changes to the fields you selected in the Insert or Edit window.

Remove a Domain Name from Supervisor Usernames

In Release 11.5, the SSO feature added a requirement that supervisor usernames use UPN-based or SAM-based format. Non-SSO solutions also had to follow this requirement. Supervisors could no longer sign in with an unqualified username.

With the addition of the **Default domain name** option on the **System Information** dialog, non-SSO solutions can revert to using unqualified usernames for supervisor sign-ins. To do so, you assign a **Default domain**

name and use the **Bulk Configuration** tool to remove the domain name that is in `LoginName` on the `Person` table.

Step 1 Set a **Default domain name**:

a) Open the Configuration Manager's **System Information** dialog and set a **Default domain name**.

b) Save your change.

Step 2 Create a text file to use in the **Bulk Configuration** tool:

a) Create a text file.

b) Insert the following header to identify the Table and Columns in the file:

```
__TABLE
Person
__COLUMNS
```

Step 3 Query the Administration & Data Server to find the supervisors with domain names in their `LoginName`:

a) Use SQL Server Management Studio to connect to the Administration & Data Server.

b) Select the AWDB and run the following query with **Results to Grid**:

```
DECLARE @DomainName AS varchar(190);
SET @DomainName = 'yourDomain.com';

SELECT P.PersonID, P.FirstName AS 'FirstName', P.LastName as 'LastName',
REPLACE(P.LoginName,'@'+@DomainName,'') AS 'LoginName', '0' as 'SSOEnabled'
FROM Person P
JOIN Agent A on (P.PersonID = A.PersonID)
WHERE A.SupervisorAgent = 'Y'
AND P.SSOEnabled = '1'
AND P.LoginName like '%'+@DomainName+'%'
```

Where *yourDomain.com* is the domain name that is currently part of the `LoginName`.

c) Select all the results and select **Copy with Headers** from the context menu.

d) Paste the results into your text file.

Step 4 Verify that the query retrieved the correct records and save the file.

Note The column values must be Tab-delimited.

Step 5 Use the text file to edit the AWDB with the **Bulk Configuration** tool:

a) Open the **Configuration Manager** on the Administration & Data Server.

b) Select **Tools** > **Bulk Configuration** > **Edit** > **Person Bulk Edit**.

c) Select **Retrieve**.

d) Select **Import…** and open your text file.

e) In the **Import Person** dialog, ensure that the five columns are selected for import, as shown:
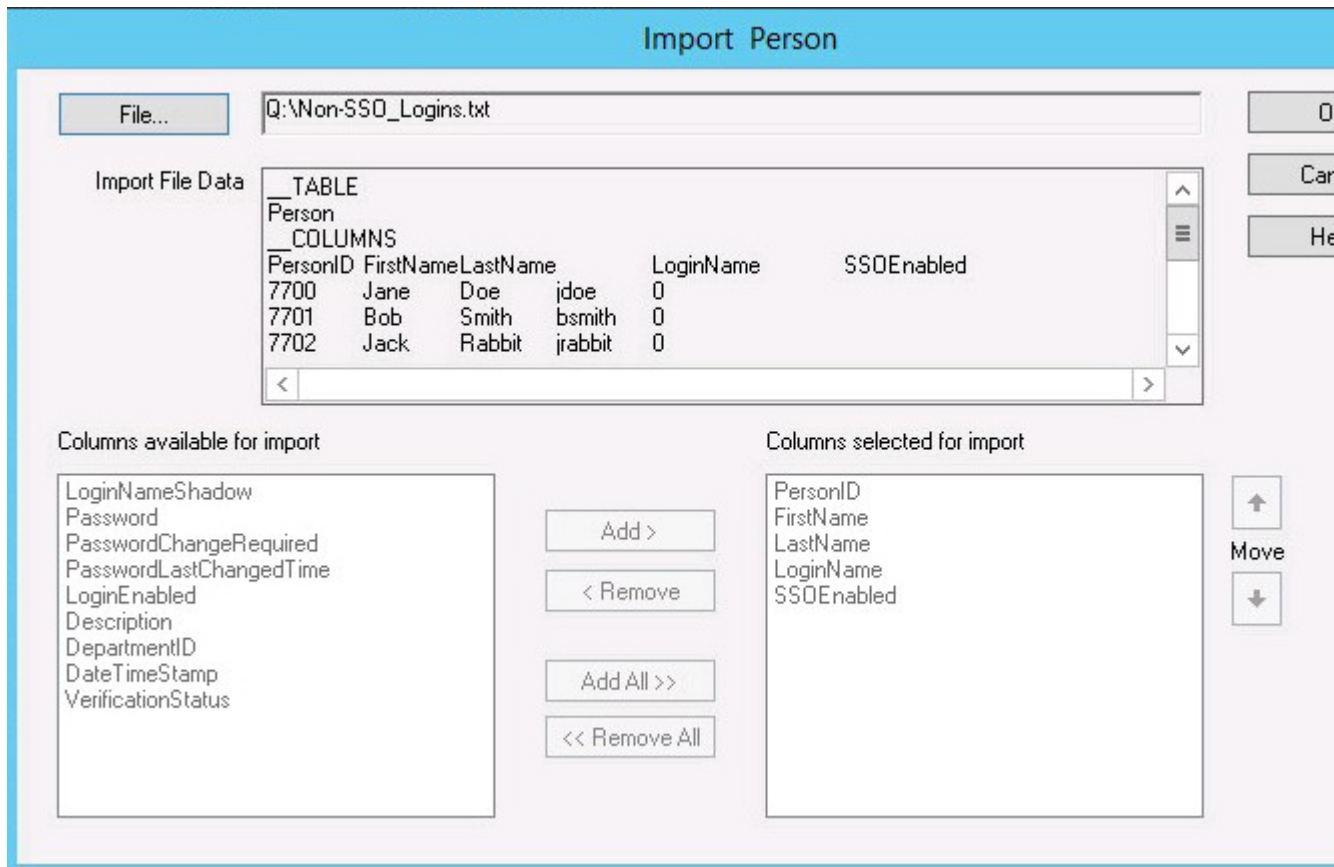
f) Click **OK** to import the data.

Step 6 In the **Person Bulk (Edit)** dialog, verify the edits and save your work.

Add New Records

You can add records by inserting multiple blank rows (records) and filling in the data or by importing the data.

You can also edit the data you insert when you insert it.

Insert New Records

To insert a new record:

Step 1 In the **Bulk Configuration** > **Insert** menu, select the name of the data table to which you want to add records. The appropriate Insert window opens, automatically displaying one new row.

Step 2 To create additional rows, enter the number of additional rows in the Quantity field and click **Insert**. The additional rows are added in the Insert window.

Step 3 Enter the data in the rows:

a) If you want to edit individual fields in the new rows, type the information you want in each of the fields and skip to Step 8.

b) If you want to edit a column in multiple rows so that a range of values is entered, continue to Step 4.

> **Note** For other ways of entering data into multiple rows, see

Step 4 Select the rows in the column you want to modify.

Step 5 Click **Edit Range**. The Edit Range dialog appears.

Step 6 Enter a prefix (optional), the start value for the range, and a suffix (optional). The generated values are listed in the dialog.

Step 7 Click **OK** to close the Edit Range dialog and apply the values to the column you selected.

Step 8 When you have finished setting fields in the new rows, press **Enter** to apply your changes to the Unified CCE database.

> **Note** You can leave empty rows, the system ignores them. No changes are made to the database until you press **Enter**.

Import Data

You can import data from a specified text file into the opened database table. You can import whole records or only columns of data if the data matches (see Step 3 of the following procedure). The process cancels if any error occurs during the import process.

Step 1 In the Insert or Edit window, click **Import**.

Step 2 In the Import dialog, click **File**.

Step 3 In the File Open dialog, select the file containing the data that you want to import and click **Open**.

The Import File Data area displays the first few lines of the opened file.

- When importing data in the Edit mode, the following rules apply:

    - The Bulk Configuration tool reads only those records whose primary key values match those of records in the Edit window.

      If a record does not match the primary key value, the record is considered to be an error and a message box with the primary key value pops up to ask you to correct the problem.

    - If any field in the import record is null, the corresponding field value in the grid window become blank for an edit cell or uses the default value for a drop-down list cell.

    - If any field is missing in the import file, the corresponding field in the Edit window remains unchanged.

    - If there is a larger number of records in the file to be imported than the number of rows in the grid, it is considered an error and a message box pops up asking you to correct it.

    - If there is a duplicated primary key in the file to be imported, it is considered an error and a message box with the duplicated primary key value pops up asking you to correct it.

    - After importing, all records imported (including records marked for deletion in the grid) are marked as "Changed" regardless of whether the value is changed or not.

    - After importing, the records display in index order (ordered by logical keys). If you did not sort before importing, the order appears the same after the import.

- When importing data in the Insert mode, the following rules apply:

    - Only a single import is supported and any existing rows are removed from the grid. When you click **Import**, the following message box pops up if there is any record in the grid:

      ```
      All the existing data will be replaced by the data to be imported. If you
      want to retain the current data on the grid please click the Cancel button
      then save or export the existing data. Click the OK button to proceed with
      the importing.
      ```

    - After importing, all rows are marked as "New" and the ordering is the same as that in the file imported from.

    - In the Import Insert mode, the tool reads only those records whose primary key values are not presented. If the primary key field is selected for file to be imported, it is considered an error and a message box with the primary key field name pops up asking you to correct the problem.

    - If any field in the import record is null, the corresponding field value in the grid window becomes blank for an edit cell or uses the default value for a drop-down list cell.

      Note   If headers are included in the imported file, the **Add** and **Remove** buttons are not enabled and you can only import the records as a whole. In that case, skip to Step 6.

Step 4   If the imported data does not contain headers, in the Available Fields list box, select the names of the fields to import that match the data and click **Add**.

Step 5   To change the order of the columns, select a column and move it within the list by clicking **Up** or **Down**.

Step 6   Click **OK**. The data is imported into the data table.

Data File Format

The import and export files used by the Bulk Configuration tool can optionally include a header that identifies the table and columns in the file. The header is followed by one line for each row of data.

The following rules apply to file headers:

- A line beginning with a number sign (#) is a comment and is ignored.

- Blank lines are also ignored.

- The header content is indicated by a line beginning with two underline characters and the word **TABLE** or **COLUMNS**. The following line contains the name of the table or the name of the columns. For example:

  ```
  __TABLE

  Call_Type __

  COLUMNS

  CallTypeID EnterpriseName Description Deleted CustomerDefinitionID
  ```

- All column names must be on a single line and are separated by Tab characters.

  The following rules apply to the data in the files:

    - One row of table data per line.

- Column values must be in the same order in all rows. If columns are specified in the header, the columns in the data rows must be in the same order.

- Column values are separated by a single Tab character.

- Fields intentionally left blank must be represented by two adjacent Tab characters or a Tab character at the end of a line. On import, the default value is used for such a value.

- String values may include spaces.

- An error occurs on import if a line contains too few or too many values.

Note   A simple way to create the import file with a valid format is to use Excel and save the file as Text (Tab delimited) (*.TXT).

Export Function

The export function saves the selected records or fields to a tab-delimited text file that you can import into the Unified ICM database or into a database tool such as Microsoft Excel. If any error occurs during the export process, the process is cancelled.

Export Data

To export data, follow these steps:

Step 1   Select the rows with fields you want to export.

Note   If you intend to import this data into the Edit window, you must export a primary key field along with any other fields. The primary key field has the same column name as the database table name.

Note   All rows selected (including records marked for deletion) are exported.

Step 2   Click **Export**.

Step 3   Select the Header option if you want to include a header containing the table name and column names in the output file. Including the header clarifies the content of the file.

Step 4   In the Export dialog, select the columns you want to export and click **Add** or **AddAll**.

Step 5   To change the order of the columns to export, select one of them and move it within the list by clicking **Up** or **Down**.

Step 6   Click **File** and specify the file name and directory to which to save the data.

Step 7   Click **OK**.

Record deletion and undeletion

You can delete one or more records at a time and you can undelete records marked for deletion.

Delete a Record

To delete records, follow these steps:

Step 1   Select the rows to be deleted.

Note   Selecting a range of fields in a column selects all the rows those fields belong to.

Step 2   Click **Delete**. The selected rows are marked for deletion.

Step 3   Click **Save**. The rows marked for deletion are deleted from the database.

Note   You can no longer undelete records marked for deletion after you save your changes to the database.

Undelete a Record

To undelete a record:

Step 1   Select the rows marked for deletion.

Step 2   Click **Undelete**. The deletion mark is removed from the records.

Step 3   Click **Save**. The change is saved to the database.

Routing Clients

The Routing Client Subsystem

A *routing client* is an entity that sends route requests to the system software.

A routing client can be:

• A public network interexchange carrier (IXC), such as AT&T, BT, or MCI

• A private network peripheral, such as an Aspect automatic call distribution (ACD)

The following figure shows the elements of the routing client subsystem.

Figure 14: Routing Client Subsystem
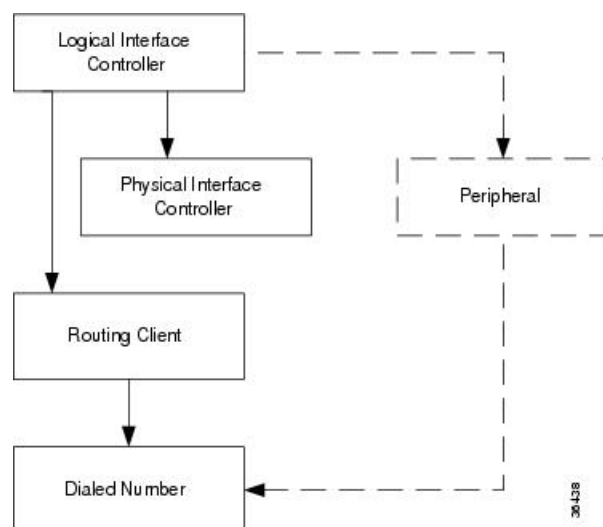
Interface Controllers

Each routing client must be associated with an interface controller. An interface controller operates on two levels: *physical* and *logical*. A physical device is a single instance of a device. A logical device is either a single physical device or more than one physical device running duplexed.

A physical interface controller can be a:

- **Network Interface Controller (NIC)**. An NIC communicates directly with the IXC's signaling network, reading call routing requests from the network and transferring them to the Central Controller. This chapter describes how to set up a **NIC**.

- **Peripheral Gateway (PG)**. A PG communicates with the ACD, PBX, or VRU at a contact center, monitoring status information from the peripheral and sending it to the Central Controller. The PG can also act as a routing client, sending routing requests to Unified ICM software.

Related Topics

Routing Client Subsystems Examples

You can associate more than one routing client with a single logical interface controller. For example, if a Unified ICM NIC is serving two AT&T Intelligent Call Processing (ICP) subsystems, as shown in the following figure, you can define each as a separate routing client through the single logical interface controller.

Figure 15: Two Clients / One Logical Interface Controller
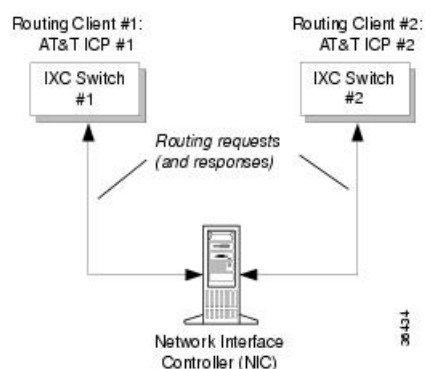
On the other hand, if you have two ACDs performing private network routing through two different peripheral gateways (PG), as shown in the following figure, you must define each as a routing client because each Peripheral Gateway is a separate logical interface controller.

Figure 16: Two Clients / Two Logical Interface Controllers
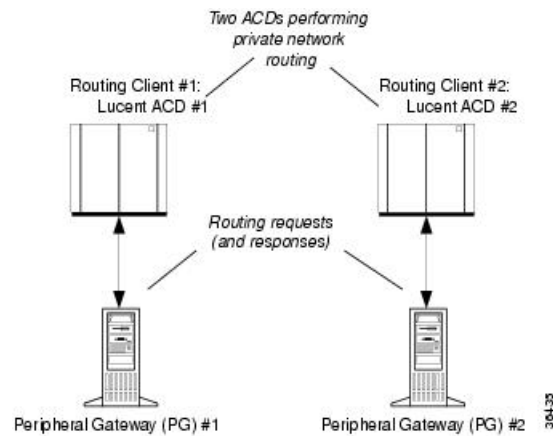
NIC Configuration

Use the NIC Explorer to view, define, modify, or delete NIC information and its associated routing client information.

The NIC is the interface between the ICM platform and the Interexchange Carrier signaling network. Within the Unified ICM software the NIC reads call routing requests from the network and transfers them to the Central Controller. It consists of a logical interface controller and one or two physical interface controllers. The number of physical interface controllers permitted depends on the client type.

The NIC Explorer generates records that set up a logical interface controller, one or more physical interface controllers, and one or more routing clients.

Related Topics

View NIC and Routing Clients, on page 77

View NIC and Routing Clients

To view a NIC and its routing clients, follow these steps:

Step 1 From the **Configuration Manager** menu, select **Tools** > **Explorer Tools** > **NIC Explorer**.

The NIC Explorer window appears.

Step 2 In the **Select filter data** box, select the filters you want.

Step 3 Click **Retrieve**. The names of retrieved NICs are listed in the tree list box.

Step 4 In the **tree list** box, select the NIC whose records you want to view. The configuration information displays in the fields on the right.

Step 5 To view a routing client record, in the tree list box, expand the tree branch for the selected NIC and select the routing client icon.

The routing client configuration information displays in the window on the right.

Related Topics

NIC Explorer Tab Descriptions

The following tables describe the tabbed property fields and buttons that configure a NIC and its routing clients.

Logical Interface Controller Tab

The Logical Interface Controller tab allows you to view (and define or edit, if you have maintenance access) the properties of the selected logical interface controller.

Table 9: Logical Interface Controller Tab Field Descriptions

Field/Button	Description
Controller ID (required)	A unique identifier for the **NIC's** logical controller. This is a read-only field. When you create a new **NIC**, the system places **UNASSIGNED** in this field and automatically creates an **ID** when you save your edits.
Name (required)	The enterprise name for the NIC's logical controller. This name also identifies the NIC and must be unique for all logical controllers in the enterprise.
Client Type (required)	The type of routing client serviced by the NIC. For example, Lucent, MCI, and so on. When defining a new NIC, select one from the pop-up selection box. Selecting a type of routing client automatically places that type's default values in the Routing Client's Timeout Threshold, Late Threshold, Timeout Limit, Use DN/Label Map, and Client Type fields.
Configuration Parameter	A string containing information such as logon information, specific to the interface controller device. For example: *-rtuser UserName -rtpswd Password*.
Description	Additional information about the Logical interface controller.
Add Physical Interface Controller	Click this button to add one or more physical interface controllers. This button is disabled when there is no client type, as in a new NIC record, or when the NIC node reaches its upper limit of Physical Interface Controllers.

Physical Interface Controller Tab

The Physical Interface Controller tab allows you to view (and define or edit, if you have maintenance access) the properties of the selected NIC's physical interface controllers.

Table 10: Physical Interface Controller Tab Descriptions

Field/Button	Description
Associated Physical Interface Controllers	A duplexed **NIC** has two entries in the Physical Interface Controller table and a single entry in the Logical Interface Controller table.
ID	A unique identifier for the NIC's associated physical interface controller. This is a read-only field. When you create a new NIC, the system places **UNASSIGNED** in this field and automatically creates an **ID** when you save your edits.
Name	The enterprise name of the routing client associated with the **NIC**. This name must be unique for all physical controllers in the enterprise.
Description	Any other information about the physical interface controller.
Modify	To edit the name or description of the physical interface controller, click this button. In the Physical Interface Controller dialog enter your edits and click **OK**.
New	To enter a record for a new associated physical interface controller, click this button and in the Physical Interface Controller dialog, enter its enterprise name and click **OK**. The system assigns an ID to the controller when you save it to the database. The NIC can represent multiple physical devices. The limit is different for different client types.
Delete	Deletes the selected physical interface controller.

Routing Client Tab

The Routing Client tab allows you to view (and define or edit, if you have maintenance access) the properties of the selected routing client. The routing client is the entity that sends routing requests to the system software.

Table 11: Routing Client Tab Descriptions

Field	Description
Name (required)	The enterprise name of the routing client associated with the NIC. You can have more than one routing client associated with a NIC. Typically, each routing client maps to a subsystem within the ICX network.
Timeout threshold (required)	The maximum time, in milliseconds, that the routing client can wait for a response to a routing request. The NIC sends a default response slightly before this threshold.
Late threshold (required)	A threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the Timeout Threshold.

Field	Description
Timeout limit (required)	The maximum time, in seconds, that the routing client waits for a response. This is the maximum time the routing client will tolerate consecutive response timeouts before it stops sending requests to the system software.
Default call type	An enterprise name for the call type. Initially, you can leave this field blank. For information on this field, refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.
Configuration parameters	A string containing any initialization parameters that must be passed to the routing client. For a public network, this might include the subsystem number. A null value indicates no configuration parameters are provided.
Use DN/Label map	Indicates whether the Dialed Number (DN) Label table is used to determine which labels are valid for each dialed number. If not, all labels for the routing client are valid for all dialed numbers.
Client type (required)	The type of routing client that ultimately routes the call on the requesting Unified ICM system. This field is enabled only for the routing client associated with an intelligent network call routing protocol (INCRP) NIC. In all other cases, it is the same as the logical interface controller's client type.
Description	Additional information about the routing client.
Network routing client	A name used to associate routing clients across instances. The same string value for the routing client on the network analysis module (NAM) and the corresponding routing client on the Unified ICM (applies only for a network Unified ICM).
Default Media Routing Domain	(selection list) The MRD associated with the routing client.
Congestion Treatment Mode	This field sets the congestion treatment mode for routing clients. The default value is 0 when you add a new routing client. The congestion treatment mode definitions are as follows: • 0 - Use Congestion Control settings. • 1 - Use Dialed Number (DN) as default label for call treatment. • 2 - Use routing client as default label for call treatment. • 3 - Use global user-defined label for call treatment. **Note** To configure a user-defined label, use the Congestion Setting Configuration tool. • 4 - Dialog fail with an appropriate error code. • 5 - Release message to the routing client.

Field	Description
Default Label	Indicates the default label for the routing client to treat the call when the system is congested. Also see the following section: Gate Keeper (GK) NIC.

Gate Keeper (GK) NIC

If you specify GK NIC as the type of routing client, the NIC Explorer automatically creates two labels that are associated with the new routing client.

The following two fields are dimmed:

- Congestion Treatment Mode (with default value as 4: to treat the calls on congestion with Dialog Fail)

- Default Label (will be empty)

When a GK NIC routing client record is deleted, the preceding labels associated with the routing client are also deleted.

Related Topics

Modify NIC and Routing Clients

To modify a NIC and or its routing clients, follow these steps:

Step 1 Follow the steps for viewing a NIC.

The selected NIC's configuration information displays in the fields on the right.

Step 2 Edit the configuration information.

You can modify all fields in the Logical Controller, Physical Controller, and Router Client tabs that are not dimmed.

When you make a modification, the **Changed** icon appears next to the edited item (NIC or routing client) in the tree list box.

Step 3 Click **Save**.

The modified data in the Unified ICM database is saved and the **Changed** icon is removed from the display in the tree list box.

Related Topics

Define NIC

To define a NIC, follow these steps:

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

Step 2 In the **Select filter** data box, click **Retrieve**. This enables the **Add NIC** button.

Step 3 Click **Add NIC**. A new NIC and its routing client display in the tree list box. Next to each is a **To Be Inserted** icon ⊞.

On the right of the tree list box, tabbed fields also display for the new NIC's and routing client's configuration information.

Step 4 Fill in the tabbed fields.

Step 5 Click **Save**. The newly defined NIC is saved in the database and the **To Be Inserted** icon is removed from the tree list box.

Related Topics

NIC Explorer Tab Descriptions, on page 78

Define Routing Client

To define a routing client, follow these steps:

Step 1 Follow the steps for viewing a NIC. The selected NIC's configuration information displays in the fields on the right.

Step 2 In the tree list box, select the NIC to which you want to add a routing client. This enables the **Add Routing Client** button.

Step 3 Click **Add Routing Client**. A new routing client icon appears under the selected NIC in the tree list box and a new Routing Client tab appears in the window on the right.

Step 4 Enter the needed routing client configuration information in the fields on the right.

Step 5 Click **Save**.

Related Topics

View NIC and Routing Clients, on page 77

Routing Client Tab, on page 79

Delete NIC

Follow these steps to delete a NIC:

Step 1 Follow the steps for viewing a NIC.

The selected NIC's configuration information displays in the fields on the right.

Step 2 In the tree list box, select the NIC whose records you want to delete.

Step 3 Click **Delete**. This places a **Marked for Deletion** icon ⊠ next to the NIC in the tree list box. This also toggles the **Delete** button to **Undelete**.

To undelete a NIC marked for deletion, select it in the tree list box and click **Undelete**.

Step 4 Click **Save**.

This deletes from the database the NIC marked for deletion and removes it from the tree list box. After you do this, you cannot undelete the NIC.

Related Topics

View NIC and Routing Clients, on page 77

Dialed Number/Script Selectors

After you have set up a routing client, you need to define the dialed number/script selectors serviced by it. A dialed number/script selector can represent an actual number dialed by a caller or any string passed by a routing client to indicate the number dialed.

The Configuration Manager's Dialed Number/Script Selector List tool allows you to list the dialed number/script selectors currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones. The following instructions show you how to configure individual dialed number/script selectors.

Related Topics

Peripherals and Trunk Groups, on page 87

Manage Dialed Number/Script Selectors

Note   Dialed Numbers on the Child Central Controller, on page 84 contains an example of how to configure dialed numbers on a child deployment.

Follow the steps below to view, define, delete, or modify dialed number/script selectors:

Step 1   From within the **Configuration Manager** menu, select **Tools** > **List Tools** > **Dialed Number/Script Selector List**. The Dialed Number/Script Selector List window appears.

Step 2   In the **Select filter data** area, select the **Routing client** and **Customer** associated with the dialed number/script selector.

Note   Once you have saved a Dialed Number record to the Unified ICM database, you cannot update the Routing Client field.

If you are viewing or modifying a previously created record and you want to limit the number of records retrieved from the database, also select one of the optional filters.

Step 3   Click **Retrieve**. This enables the **Add** button and displays a list of the retrieved dialed number/script selectors.

The properties of the dialed number/script selector selected in the Dialed Number/Script Selector list box on the left side of the window are displayed in the property tabs on the right side of the window:

The following properties are displayed:

• The Attributes tab allows you to view and (if you have maintenance access) to define, edit, or delete the attributes of the selected dialed number/script selector. Attributes with an asterisk are required.

> • The Dialed Number Label tab allows you to map labels (in addition to a default label) to the selected dialed number/script selector.

Step 4 This step depends on what you want to do:

> • To add a new dialed number/script selector, click **Add** and enter the appropriate values in the tabbed property fields on the right side of the window.

> • To delete a dialed number/script selector, select that number in the **Dialed Number/Script Selector** list box and click **Delete**.

> • To edit a dialed number/script selector, select that number in the **Dialed Number/Script Selector** list box and edit the appropriate values in the tabbed property fields on the right side of the window.

Step 5 Click **Save** to enter any edits into the database.

The dialog closes, and for a new dialed number/script selector, the Unified ICM database manager automatically generates a unique Dialed Number ID for the routing client.

Dialed Numbers on the Child Central Controller

Access the Configuration Manager on the Child Administration & Data Server to configure dialed numbers.

Configure Dialed Numbers on the Child Central Controller

To configure dialed numbers on the Child Central Controller with the Configuration Manager Dialed Number/Script Selector List Tool:

Step 1 Start the **Dialed Number/Script Selector List Tool**.

Step 2 On the Main window of the Dialed Number/Script Selector List Tool, click **Retrieve**.

Step 3 Click **Add**.

The Dialed Number Attributes tab appears.

Step 4 Select **IPCC_RC** as the Routing Client.

Step 5 Select **Cisco_Voice** for the Media Routing Domain.

Step 6 Set the Dialed Number String/Script Selector to **2500** (the route point set up on the Unified CM.

Step 7 Set **IPCC_RC_2500** as the Name, then select **bh03** as the Customer setting.

Step 8 Check **Permit Application Routing** on the route points controlled by the Parent (the Post route points and the Translation route points).

This provides the link between the Parent and the Child. It gives the Parent visibility to the Dialed Number so it can handle it.

Step 9 Click **Save**.

The dialed number appears in the tree list.

Step 10 Repeat this to add two more dialed numbers (one for each skill group).

When complete, you have the following DNs:

- 2500
  - Connects to all of the skill groups.
  - Named IPCC_RC_2500.

- 2501
  - Connects to SG01.
  - Named IPCC_RC_2501.

- 2502
  - Connects to SG02.
  - Named IPCC_RC_2502.

Step 11 Click **Save**, then **Close** to exit the Skill Group Explorer Tool.

Peripherals and Trunk Groups

- Peripheral Subsystem, on page 87
- Peripheral Gateways, on page 88
- Peripherals and Trunk Groups, on page 88
- Peripheral Gateway Records, on page 88
- Trunk Groups and Trunks, on page 106

Peripheral Subsystem

A *peripheral* is a switch, such as an ACD, PBX, VRU, or Unified Communications Manager (Unified CM). Calls arrive at the peripheral through *trunks* that are organized into trunk groups. The Unified Intelligent Contact Management (Unified ICM) system software monitors activity at each peripheral and can route calls to targets at each peripheral.

The logical interface controller and physical interface controller represent the peripheral gateway (PG) through which the peripheral communicates with the system.

To view the elements in a peripheral subsystem, see the following figure.

Figure 17: Peripheral Subsystem
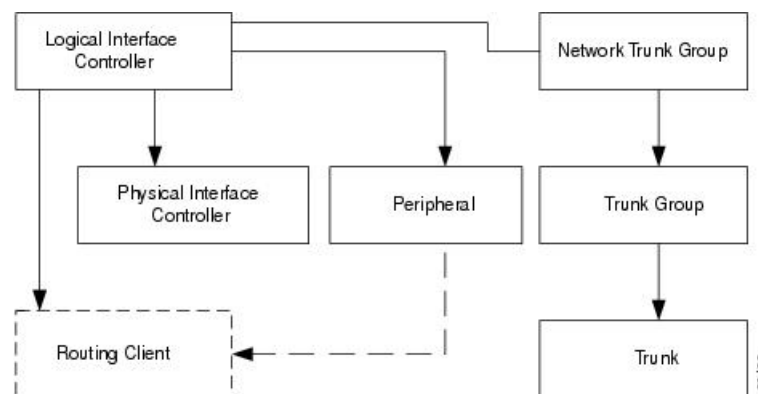
The routing client figures into this subsystem only if the peripheral acts as a routing client (that is, if it sends routing requests to the system software).

Related Topics

The Routing Client Subsystem, on page 75

Peripheral Gateways

Each peripheral communicates with the system software through a peripheral gateway (PG). The PG is a interface between the Unified CM platform and third-party hardware like the ACD, PBX, VRU, monitoring status information from the peripheral and sending it to the Central Controller. If the peripheral acts as a routing client, the PG sends routing requests to the system software.

The PG can be a single simplex system or a pair of duplex systems. A single PG can service more than one peripheral; however, each peripheral uses one, and only one, PG.

Note Although a PG may consist of a pair of duplex systems, only one of them is active at a time, so that the system software sees it as a single, logical and physical PG.

Peripherals and Trunk Groups

This chapter describes how to configure peripherals and the trunk groups associated with them.

It includes:

- An introduction to the peripheral subsystem
- Instructions on how to view, define, delete, or modify:
    - peripheral gateways
    - peripherals
    - network trunk groups
    - trunk groups
    - trunks

Related Topics

Peripheral Gateway Records

Use the PG Explorer to view, define, modify, or delete peripheral gateway records.

The PG Explorer generates and maintains PG records for a logical interface controller, a physical interface controller, associated peripherals, and, if appropriate, an associated routing client.

Note If you are configuring a PG for a duplexed pair, you need to define the information only once.

The following figure shows the records generated by the PG Explorer.

Figure 18: Records Generated by PG Explorer
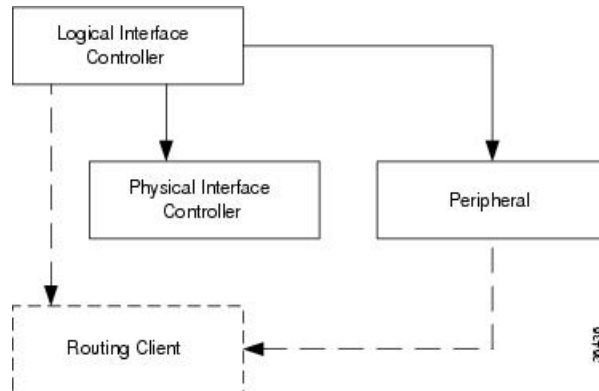
View PG Records

To view PG records, follow these steps:

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

Step 2   In the **Select filter data** box, select the filters you want.

Step 3   Click **Retrieve**. Names of retrieved PGs appear in the tree list box.

Step 4   In the tree list box, select the PG whose records you want to view. The configuration information displays in the tabbed fields on the right.

Step 5   To view a peripheral's record: in the tree list box, expand the tree branch for the selected PG, and select the PG's peripheral icon.

The peripheral configuration information displays in the window on the right. For field descriptions, see the online help.

PG Explorer Tab Descriptions

The following tables describe the tabbed property fields and buttons that configure a PG. Use these fields to define and update PGs and their associated peripherals.

Logical Controller Tab

Use the Logical Controller tab to view, define, and update PG definitions. In the Unified CCE database, a PG is identified by its logical controller.

Table 12: Logical Controller Tab Field Descriptions

Field	Description
Logical Controller ID (required)	A unique identifier used to reference the PG's Logical Interface Controller table. This is a read-only field. When you create a new PG, the system places UNASSIGNED in this field and automatically creates an ID when you save your edits.
Physical Controller ID (required)	A unique identifier for the PG's physical controller. This is a read-only field. When you create a new PG, the system places UNASSIGNED in this field and automatically creates an ID when you save your edits.
Name (required)	An enterprise name for the PG. This name must be unique for all PGs in the enterprise. An enterprise name: • Is a character-string name commonly used to identify an object in the database. • Must be unique among all objects of a specific type. For example, each service must have an enterprise name that is unique among all services. • Can be up to 32 characters. The valid characters are upper-case and lower-case letters, digits, periods (.) and underlines (_). The first character of the name must be a letter or digit. **Note** This name is used in composite names, which are limited to a 32 character length, for example, an agent enterprise name. Therefore, keep the name short.
Client Type (required)	(selection list) The type of client that the PG services. When defining a new PG, select one from the pop-up selection box. Selecting a type of peripheral automatically places that type's default values in the associated peripheral's Client type, Peripheral Service Level type, Service Level type, and Service Level Threshold fields.
Configuration Parameters	A string containing information, such as logon information, specific to the PG. For example: `-rtuser UserName -rtpswd Password`
Description	Additional information about the PG.
Physical Controller Description	Information about the physical controller.

Field	Description
Primary CTI Address	Address for computer telephony integration (CTI) server as <IP>:<port> in either dotted numeric or name format. If a CTI server is installed at the PG, enter its address. This address is needed if an agent is connected through a CTI server rather than through a peripheral.
Secondary CTI Address	Address for CTI server as <IP>:<port> in either dotted numeric or name format. The secondary CTI address is needed if a CTI server is installed at the PG and the Unified CCE system is duplexed. **Note** If you use a simplex system, fill in both the addresses.
Reporting Interval	The system software stores historical information in either 15-minute or half-hour summaries (but not both), based on the reporting interval option set. The Router sends these records to the Logger, which in turn writes them to the Central Database. Select the **15 Minute** or **30 Minute** reporting interval option (default is 30 Minute). **Note** Be aware that the 15 Minute interval requires a larger amount of space than the 30 Minute interval. This setting controls populating interval data only in the following tables: • Agent_Interval • Agent_Skill_Group_Interval • Peripheral_Interval • Service_Interval • Skill_Group_Interval • System_Capacity_Interval There is another Reporting Interval setting on the PG Explorer's Logical Controller tab that controls populating interval data for a different set of tables. **Important** If your solution uses Precision Queues, choose the same interval (15 minutes or 30 minutes) for both this setting and the setting on the **Logical Controller** tab.

Field	Description
Time Source	The time source that the PG uses to copy the historical interval data (15 or 30 minute) and send to the CallRouter. Any change made to the time source requires simultaneous shutdown (PG services to be stopped and restarted simultaneously) on both PG sides.

Two time source options are available:

- **Use Central Controller Time**. The PG uses the Central Controller CallRouter time source to obtain the historical interval (15 or 30 Minute) data and send to the CallRouter (default time source when adding or upgrading a PG).

- **Use ACD Time**. The PG uses the corresponding ACD time source to obtain only the 30-minute historical interval data and send to the CallRouter. (15-minute historical data is not supported for PGs that use the ACD time source.)

| **Note** | If the **Use ACD Time** option is enabled, the CallRouter-generated Call Type and Call Type Skill Group data will not align with the Peripheral-generated Skill Group data. |

This option is available only for the following client types for the defined PG:

- Avaya Communication Manager

- Aspect Call Center

- UCC Enterprise Gateway |

Peripheral Tab

Use the Peripheral tab and its associated tabs to view, define, and update the peripherals associated with a PG.

Table 13: Peripheral Tab Field Descriptions

Field	Description
Peripheral ID (required)	A unique identifier for the peripheral. This is a read-only field. When you create a new PG, the system places UNASSIGNED in this field and automatically creates an ID when you save your edits.
Name (required)	An enterprise name for this peripheral. The name must be unique among all peripherals in the enterprise.
Peripheral Name (required)	The name of the peripheral as it is known at the local site. Unlike the Enterprise Name field, the value of this field does not have to be unique. For example, at each site you might label the peripherals Switch1, Switch2, and so forth.

Field	Description
Client Type (required)	The type of peripheral. The value for this field comes from the Logical Controller Client Type field.
Location	The peripheral's location; for example: the name of a city, building, or department.
Abandoned Call Wait Time (required)	Minimum time in seconds an incoming call must be queued before being considered an abandoned call if the caller hangs up.
Configuration Parameters	A string containing any parameters that must be sent to the device to initialize it. In most cases, leave this string blank.
Call Control Variable Map	A string that describes the mappings of the peripheral's call control variables to the system software's call control variables.
Default Desk Settings	(selection list) Default desk settings for agents associated with the peripheral. **Note** If NONE is the only option in the selection list, you need to create desk settings. To create desk settings, use the Configuration Manager's Agent Desk Settings List tool.
Peripheral Service Level Type (required)	The default type of service level calculation to be performed by the peripheral for its associated services. Specify one of the following: • If the peripheral type is Aspect Call Center, choose the type of calculation to be performed by default. You can override the default for each individual service. • If the peripheral type is not Aspect Call Center, choose **Calculated by Call Center**.
Agent Phone Line Control (required)	Indicates whether this agent peripheral supports multi-line control for all agents with more than one line configured on the phone. Specify one of the following agent phone line control options: • **Single Line**: Enables single line monitoring and reporting (default). • **All Lines**: Enables multi-line monitoring and reporting. **Note** For any configuration changes to reflect, an exit_opc or termination of both PG sides are required.

Field	Description
Non ACD Line Impact (required)	Indicates how many non-ACD calls the agent initiated on one of the non-ACD lines. (This field is populated only when the **All Lines** option is enabled.) Specify one of the following non-ACD line impact options: • **Available Agent Goes Not Ready**: Agent state is set to NOT READY with a system reason code when agent answers or places a call on a secondary line while in the AVAILABLE or NOT READY state. • **Available Agent Stays Available**: Agent state is unchanged when agent is on a call on a secondary line. **Note** Non-ACD lines are not a part of hunt group in UCCE.
Description	Additional information about the peripheral.
Enable Post Routing	If checked, indicates that post-routing is enabled. When this is enabled, the Routing Client tab is also enabled. If you check **Enable Post Routing** in the Peripheral tab, also enter the properties in the Routing Client tab.
Peripheral Auto-Configured	Checked, indicates peripheral is auto configured.

Advanced Tab

The Advanced tab allows you to view (and define or edit, if you have maintenance access) the advanced properties of the selected peripheral.

Table 14: Advanced Tab Field Descriptions

Field	Description
Available Holdoff delay (required)	The number of seconds to wait after the end of a call before recording the agent as available. The value you enter here is the default for all skill groups associated with the peripheral. You can change the value for individual skill groups.
Default Route	The default route associated with this peripheral.
Answered Short Calls Threshold	The maximum length, in seconds, for a short call to the peripheral. Any calls with a duration below the threshold are considered short. You might then choose to factor out short calls from handle times you calculate.
Network VRU	The type of network VRU. If the peripheral is a VRU, that is, used as a network VRU, select the name of the network VRU from the drop-down list.

Field	Description
Agent Auto-Configuration	Specifies whether agent auto-configuration is enabled for the peripheral.
	Note Agent Reporting implies Auto Configuration. Agent Reporting without auto-configuration is NOT supported. Unified ICM does not support Agent Reporting on manually configured agents with auto-configuration off.
	Internal IPTA only
	Specifies whether the peripheral belongs to internal IPTA.

Skill Group Mask Tab

This tab allows you to view (and define or edit, if you have maintenance access) the default number of sub-skill groups associated with the selected peripheral.

☞

Important   Sub-skill groups are not supported for Unified Contact Center Enterprise; however, they are supported for certain TDM peripheral gateways (as configured in an Avaya Communication Manager PG). Sub-skill groups are also not supported for non-voice skill groups. That is, you cannot create sub-skill groups for these media classes: single-session chat, multi-session chat, blended collaboration, and email.

Note   For some peripherals, the Configuration Manager can automatically create subgroups (primary, secondary, and so on) for each skill group.

Sub-Skill Group Check Boxes

Note   These check boxes are enabled only for supported TDM peripherals.

The maximum number of subgroups that may be created depends on the peripheral's client type, and may be none. Where subgroups are available, a default selection has been made. You may change this default, either to none or any number up to the maximum number allowed for this client type.

If you later edit the subgroup selection, removing any previously used subgroups may cause loss of reporting information and must be done carefully. Changes done here will be reflected in all skill group entries that currently exist for this peripheral, which do not explicitly override the settings in the peripheral.

Check a box for each sub-skill group for each non-enterprise skill group you want to be associated by default with the peripheral. For each box you check, a skill group record is created in the database if the primary skill group uses the peripheral's default.

The number of sub-skill groups used by a primary skill group is specified in the Subgroup Mask tab of the Skill Group Explorer. There, you can add more sub-skill groups than are defined for the peripheral if the selected skill group requires additional ones.

Note The Sub-Skill group check boxes are dimmed for enterprise skill groups.

Routing Client Tab

A routing client represents an entity that sends routing requests to the system software through a logical interface controller. Use the Routing Client tab to view, define, or update a PG's routing clients.

Table 15: Routing Client Tab Field Descriptions

Field	Description
Name (required)	An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
Timeout Threshold (required)	The maximum time, in milliseconds, the routing client can wait for a response to a routing request. The NIC sends a default response slightly before this threshold.
Late Threshold (required)	The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the TimeoutThreshold.
Timeout Limit (required)	The number of seconds to wait for routing responses before the routing client terminates communication with the system software. When a response from the CallRouter exceeds the time-out threshold, the routing client starts a timer. If the timer reaches the specified time-out limit before the routing client receives any responses from the CallRouter, the routing client assumes the Unified ICM system is off-line and stops sending it routing requests.
Default MR Domain ID (required)	(selection list) The MRD associated with the routing client.
Default Call Type	The call type to be used for any route request that does not match a defined call type mapping. The drop-down list contains all configured call types.
	The system software uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, the system software uses a general default call type.
Configuration Parameters	An optional string containing the configuration parameters to be used by the controller to initialize the routing client. For a public network client, this field generally specifies the subsystem for the NIC to use.
Use DN/Label Map	Indicates that the Dialed Number (DN) Label table is used to determine which labels are valid for each dialed number (if checked), or that all labels for the routing client are valid for all dialed numbers (if not checked). You can leave this field unchecked.
Client Type	Indicates the type of client. It is the same as the PG's Client Type.

Field	Description
Description	Additional information about the routing client.
Network Routing Client	A name used to associate routing clients across instances.
Network Transfer Preferred	Checked, indicates network transfer is preferred. When the target of a call transfer is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that pre-routed the call, this option indicates which choice is preferred.
Congestion Treatment Mode	Congestion treatment mode for routing clients. The default value is 0 when you add a new routing client. The congestion treatment mode definitions are as follows: • 0 - Use Congestion Control settings. • 1 - Use Dialed Number (DN) as default label for call treatment. • 2 - Use routing client as a default label for call treatment. • 3 - Use global user-defined label for call treatment. **Note** To configure a user-defined label, use the Congestion Setting Configuration tool. • 4 - Dialog fail with an appropriate error code. • 5 - Release message to the routing client.
Default Label	Indicates the default label for the routing client to treat the call when the system is congested.

Related Topics

Routing a Call, on page 5

Peripheral Monitor Tab

A *peripheral monitor* is an entity that you want to monitor at the peripheral. Not all peripherals require peripheral monitor records.

You must configure peripheral monitor records for Extension numbers on a Definity switch.

Table 16: Peripheral Monitor Tab Field Descriptions

Field	Description
Current Peripheral Monitor Entries	Lists the current peripheral monitor data (Type, Extension, and Configuration Parameter) entered for the selected PG. **Note** The peripheral monitor records are initially sorted by PeripheralMonitorID (the default sort order). Click any column header to reverse the sort order (ascending-to-descending or descending-to-ascending). The indicator to the right always points to the lowest item in the current list order.
Type (required)	The type of entity to be monitored: ACD Directory Number (ACD DN), Meridian Position, Queue, Route Control Group (RCG), Routing Device, Station, Avaya Aura Contact Center (AACC) CDN, Trunk, Vector Directory Number (VDN), or Virtual Routing Device.
Extension	For an Avaya (Definity), if there is a single extension number, enter the number here (for example, 6002) and do not enter it in the parameter string. If there is more than one number, leave this field blank and enter the numbers as a range in the parameter string.
Configuration Parameters	A parameter string to be passed to the peripheral along with the extension string to start monitoring on the specified extension: • For an Avaya (Definity), if there is more than one extension number, enter them here as a range, for example, 6001-6020. If there is only one extension number, leave the parameter string blank.
New	Click this button to enter new monitor data. Then select a type from the Type selection list, fill in any other appropriate field information, and press the **Enter** key.
Delete	Click this button to delete the selected row item from the list of current peripheral monitor entries.
Extension	Displays the extension of the selected current peripheral monitor entries for editing purposes. Click **Save** when you finish editing to save your changes.
Configuration Parameter	Displays the configuration parameter of the selected current peripheral monitor entries for editing purposes. Click **Save** when you are done editing to save your changes.
Type	Displays the type of the selected Current peripheral monitor entries for editing purposes. Click **Save** when you are done editing to save your changes.

Default Route Tab

Use this tab to create a default route for each MRD that is associated with a peripheral.

Table 17: Default Route Tab Descriptions

Field/Button	Description
Current Default Route Entries	**Media routing domain** The media routing domain configured for the selected default route entry. **Route** The default route configured for the media routing domain of the selected default route entry. **Note** The default route configured for the media routing domain of the selected default route entry. Click any column header to reverse the sort order (ascending-to-descending or descending-to-ascending). The indicator to the right always points to the lowest item in the current list order.
New	Click to enter new default route data. Then, enter a media routing domain and a route.
Delete	Click to delete the selected row item from the list of current default route entries.
Media Routing Domain (required)	Enter the media routing domain when creating a new default route entry.
Route	Enter the route when creating a new default route entry.

Agent Distribution Tab

Use the Agent Distribution tab to list and view the agent distributions currently defined in the Unified ICM database and (if you have maintenance access) to define new agent distributions and edit or delete existing ones. This data is stored in the database Agent Distribution table.

Note The PG Explorer (and the assigning of agent distribution) is not available on a *limited* Administration and Data Server.

Table 18: Agent Distribution Tab Field Descriptions

Field	Description
Enable Agent Reporting	Specifies whether agent reporting is enabled for the peripheral. Select this option if you want the peripheral to report agent-level statistics to the system software. **Note** Agent Reporting implies Auto Configuration. Agent Reporting without auto-configuration is NOT supported. Unified ICM does not support Agent Reporting on manually configured agents with auto-configuration off. **Note** If the peripheral's client type is CUCM, select an agent desk setting in the PG Explorer's Peripheral tab before you can enable agent reporting. The peripheral's client type is indicated in the PG Explorer's Peripheral tab.
Agent Event Detail	Specifies whether agent event detail reporting is enabled for the peripheral. This check box is enabled only if the **Enable agent reporting** checkbox is selected. Making this selection results in agent reason codes being added to agent reporting. **Note** This checkbox is enabled by default if you are adding a CUCM PG.
Agent Distribution Entries	Lists the agent distributors (Administration Clients or Administration & Data Servers) available for distributing agent report data for the selected peripheral. **Site name** One or more names of agent distribution sites associated with the selected peripheral. **Agent real-time data** **N** indicates that agent real time data is not enabled. **Y** indicates that agent real time data is enabled. **Agent historical data** **N** indicates that agent historical data is not enabled. **Y** indicates that agent historical data is enabled.

Field	Description
Currently Selected Site	**Administration & Data Server site name**
	The name of the currently selected site in the agent distribution entries list.
	Agent real time data
	If checked, enables the flow of agent real time data from the peripheral to the Administration & Data Server. Unchecked, disables the flow of agent real time data.
	Agent historical data
	If checked, enables the flow of agent historical data from the peripheral to the Administration & Data Server. If unchecked, disables the flow of agent historical data.
	Note If you configured a site name, you must enable both the Agent real-time data and Agent historical data if needed. Then restart the Distributor Service. If you did not configure a site name, the agent historical data flows from the peripheral to the Administration & Data Server by default only for the AW-HDS-DDS type.
New	Click to add a new Administration & Data Server site. This places *NEW* in the **Administration & Data Server site name** input box and in the **Agent Distribution Entries** list. Replace *NEW* in the Administration & Data Server site name input box with the name you want. Then check the check box if you want to enable it, and click **Save**.
Delete	To delete an Administration & Data Server site, select that site's name in the Agent Distribution Entries list and click this button. Then click **Save**.

✎

Note For information on how to use the agentcfg.exe command line utility to import agent data, see Agents, on page 165

PG and Peripheral Definitions

Use the PG Explorer to define a PG and its associated peripherals.

Related Topics

Configuration Manager Menus, on page 43

Define a PG

✎

Note Unified CCE System Peripheral Gateways contains an example of how to define a PG on a child deployment.

To define a PG, perform the following:

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

Step 2   In the Select filter data box, click **Retrieve**. This enables the **Add PG** button.

Step 3   Click **Add PG**. A new PG appears in the tree list box with a **To Be Inserted** icon ⊞ next to it. Tabbed fields also appear on the right for the new PG's configuration information.

Step 4   Fill in the tabbed fields.

Step 5   If desired, set security settings on the records.

Step 6   Click **Save** to save the newly defined PG in the database.

> **Related Topics**
> Configuration Manager Menus, on page 43

Define a Peripheral

To define a peripheral:

Step 1   Follow the steps for viewing a PG.

The selected PG's configuration information appears in the fields on the right.

Step 2   In the tree list box, select the PG to which you want to add a peripheral. This enables the **Add Peripheral** button.

Step 3   Click **Add Peripheral**. A peripheral is added to the selected PG in the tree list box. Also, a new set of tabbed fields appear on the right for the new PG's configuration information.

Step 4   Enter the needed peripheral configuration information in the fields on the right.

Step 5   If desired, set security settings on the records.

Step 6   Click **Save**.

After you have defined a peripheral, you can define the trunks, agents, groups, and services associated with that peripheral.

> **Related Topics**
> Peripherals and Trunk Groups, on page 87
> Apply Security Settings

Unified CCE System Peripheral Gateways

On the Administration & Data Server, run the Configuration Manager to add the Unified CCE system peripheral gateways.

Configure Unified CCE System PGs

To configure Unified CCE system PGs with the Configuration Manager tools:

Step 1   Select **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager** .

Step 2   Start the PG Explorer Tool, then in the Main window click **Retrieve**.

Step 3 Click **Add PG**.

This creates both the peripheral gateway and the peripheral.

a) Enter **UCCE** for the Name.
b) Select **UCCE System** for the Client Type.
c) If no desk settings are set, set them now. Click **OK**.

The Agent Desk Settings List Tool appears.

d) Click **Add**.

The Attribute tab appears.

e) Enter the Name **default**.
f) Leave all other settings at their defaults and click **Save**.
g) Close the Desk Settings List Tool.

Step 4 Go back to the PG Explorer Tool.

a) Select **UCCE-1** as the peripheral.
b) On the Peripheral tab, set the Default Desk Settings to **default**.
c) On the Agent Distribution tab, click **New**.
d) Set the Administration & Data Server site name to **BELO-5C-Site 1** and leave all other settings at their defaults.
e) On the Routing Client tab, enter the Name **UCCE_RC** and leave all other settings at their defaults.
f) Click **Save**.

The Logical Controller ID (5000) and the Physical Controller ID (5000) are now indicated on the Logical Controller tab.

g) Reboot the system peripheral gateway servers (BELO-5A and BELO-5B).

The Central Controller setup and configuration is now complete. The peripheral gateways can now be installed and configured to communicate with the Central Controller.

Add Instance

This task is performed on the child system peripheral gateway servers BELO-5A (PG1A) and BELO-5B (PG1B).

To add the instance with the Web Setup Tool after the reboot:

Step 1 Enter **http://BELO-5B/setup** (or BELO-5A, as applicable) and log in to the Web Setup Tool to add the Instance. The main Web Setup Tool window appears.

Step 2 Click **Instance Management**, then click **Add**.

The Add Instance dialog appears.

Step 3 Select **BELO** (the facility), then **bh03** (the Instance to add).

Step 4 Click **Save**.

Step 5 Click **Log Out**.

PG or peripheral modification

Use the PG Explorer to modify a PG or a peripheral.

Modify PG and Peripheral Records

To modify a PG and peripheral record:

Step 1 Follow the steps for viewing a PG.

The selected PG's configuration information displays in the fields on the right.

Step 2 Edit the configuration information.

Note You cannot modify fields that are greyed out.

Table 19: Rules for Changing a PG Client Type

If the PG Client Type is	Then it must be
Generic	Changed to Non-Generic (ACD or VRU).

When you make a modification, the **Changed** icon ⊡ appears next to the selected item (PG or peripheral) in the tree list box.

Step 3 Click **Save**.

The modified data is saved in the Unified ICM database and the **Changed** icon is removed from the PG or peripheral in the tree list box.

PG or Peripheral Deletion

Use the PG Explorer to delete a PG or a peripheral.

Delete a PG or Peripheral

To delete a PG or a peripheral:

Step 1 Follow the steps for viewing a PG.

The selected PG's configuration information displays in the fields on the right.

Step 2 In the tree list box, select the PG or peripheral whose records you want to delete.

Note If you select a PG, the records for all peripherals associated with it will also be deleted. If you select a peripheral, only its records will be deleted.

Step 3 Click **Delete**. This places a **Marked for Deletion** icon ⊠ next to the selected item in the tree list box. This also toggles the **Delete** button to **Undelete**.

To undelete an item marked for deletion, select it in the tree list box and click **Undelete**.

Step 4   Click **Save**.

This deletes from the database the PG or peripheral marked for deletion and removes it from the tree list box. Once you do this, you cannot undelete the deleted item.

Agent Targeting Rules

If you're routing calls to agents on a PG from another PG/routing client, configure agent targeting rules. This helps you to route the calls successfully. Using agent targeting rules to configure call routing for Unified CCE agent PGs is simpler and significantly reduces the amount of time spent on configuration. The agent attempts to log in to an extension to which the router can't target a call based on configured agent targeting rules. In this scenario, the peripheral gateway rejects the login request and returns an error. The error includes the cause for login failure.

Agent targeting rules are supported for system PGs, and CallManager PGs in Unified Contact Center Enterprise (Unified CCE) deployments.

It supports a standalone Unified CCE, Unified CCE child of a Unified ICM parent. A Unified ICM Unified CCE Enterprise in a network analysis module (NAM) deployment is also supported.

In a NAM environment, you can use agent targeting rules on the Unified ICM side in a Unified CCH deployment to target agents. However, if the NAM side requires label validation you can either define all the labels. The agent targeting rules at the CICM on the NAM side generate these labels. You can also turn off label validation. The **Validate Returned Labels** checkbox in the ICM Gateway node must be *unchecked* for calls routed using agent targeting rules to work. The calls fail at the NAM for not defining the labels, and turning on label validation. This happens even though a response with a valid label was sent from the CICM.

Note   Hunt groups aren't supported on monitored agent lines. Agent extensions can't be added to hunt lists or hunt groups. PG can be Single Line or Multiline mode.

If the PG is in the single-line mode, the hunt groups are supported on the unmonitored (non-ACD) line; however, the hunt groups aren't supported on the agent extension. The agent line can't be part of a hunt list or a hunt group.

If the PG is in multiline mode, hunt groups aren't supported on any of the agent's extensions when the agent is logged in. If the agent has multiple lines, none of the lines on the first four lines monitored by the Unified CCE are a part of the hunt group.

Hunt groups aren't supported on an agent's monitored lines while the agent is logged in.

Configure Agent Targeting Rules

You can define one or more rules for a peripheral. However, each rule must cover a different agent extension range for the same routing client. In other words, if there are multiple rules that a routing client can use to target a peripheral, there must be no overlapping extension ranges in those rules.

Note   To use agent targeting rules, you must have both the Central Controller and the PGs upgraded to the same version of Unified ICM that supports the Agent Targeting Rules feature.

To configure agent targeting rules:

Step 1 Using the PG Explorer tool, Define a PG that directly targets an agent. On the Advanced tab, select the **Rules Preferred** option, which indicates that the CallRouter will use the agent targeting rule (if one exists). Save the PG.

Step 2 Using the Agent Targeting Rule List tool, create the rule:

a) Add a name for the rule in the **Name** field.

b) Select the PG you just defined in the **Peripheral** field.

c) Select the **Rule type**:

- **Agent Extension**: Enter the agent extension prefix. This option directly targets the agent. The agent is identified by an ID, which will display in the PreCall and Connect messages. (The agent's extension is included as the label.)

- **Substitute Agent Extension**: Enter the agent extension length. When using this type, the label returned will be the combined Agent Extension prefix and the actual agent extension. For example, if the call from Unified Customer Voice Portal (Unified CVP) goes through the target agent on a CallManager PG, use this option.

- **Translation Route**: A translation route is used to move the call. This option allows pre-routing of calls directly to an agent without requiring direct-inward-dial (DID) to all agents. Translation routes require the generation of a second label, used to target the agent from the peripheral's local routing client. For example, select a translation route associated with the peripheral and define the extension range.

d) Select the routing client in the Routing client group box by clicking **Add** (defines where the call comes from).

e) Add the phone extension range in the Extension Ranges group box by clicking **Add**.

f) Click **Save**.

When the CallRouter routes a call, it will check if there is a rule for that routing client. The CallRouter decides which rule to use based on routing client, PG, and extension range. When the CallRouter finds a rule, it uses the rule type to decide how to construct a label to send to the routing client.

Note When configuring an agent targeting rule for a translation route, if you are using agent targeting rule type 3 (translation route), you must also configure the translation route DNIS as dialed numbers associated with the target agent's peripheral routing client in Unified ICM. The dialed numbers must be mapped to the route points that are configured in Unified CM and associated with the Java telephony API (JTAPI) user. This is necessary to complete the translation route rule.

Trunk Groups and Trunks

Every peripheral has one or more associated trunk groups, with each trunk group containing one or more physical trunks. Trunk groups map to trunk sets defined by the peripheral.

A peripheral dispatches a call to the appropriate skill target based on the trunk group on which the call arrives and the DNIS value that accompanies it. The peripheral treats all trunks with a particular trunk group the same, but it might treat trunks within another trunk group differently.

When setting up trunk groups and trunks, you must specify:

- Each trunk group that can receive calls

- How many trunks are in each trunk group, or configuration information for each trunk in the group

This section describes how to configure the trunk groups and trunks that will be used by routing clients and peripherals.

Network Trunk Groups, Trunk Groups, and Trunks

Routing clients deliver calls to trunk groups at the peripheral. However, a routing client might group the trunks differently from the way the peripheral groups them. The groups as seen by the routing client are called network trunk groups.

A network trunk group:

- Is a collection of peripheral trunk groups.

- Can map directly to a single trunk group at the peripheral or to multiple trunk groups.

- Can also map to trunk groups at different peripherals, provided that all the peripherals are associated with the same PG. (Only valid for VRU peripherals.)

View a Network Trunk Group, Its Trunk Groups, and Trunks

To view a network trunk group, its trunk groups, and trunks:

Step 1 From the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Network Trunk Group Explorer**. The Network Trunk Group Explorer window appears.

Figure 19: Example Network Trunk Group Explorer Window
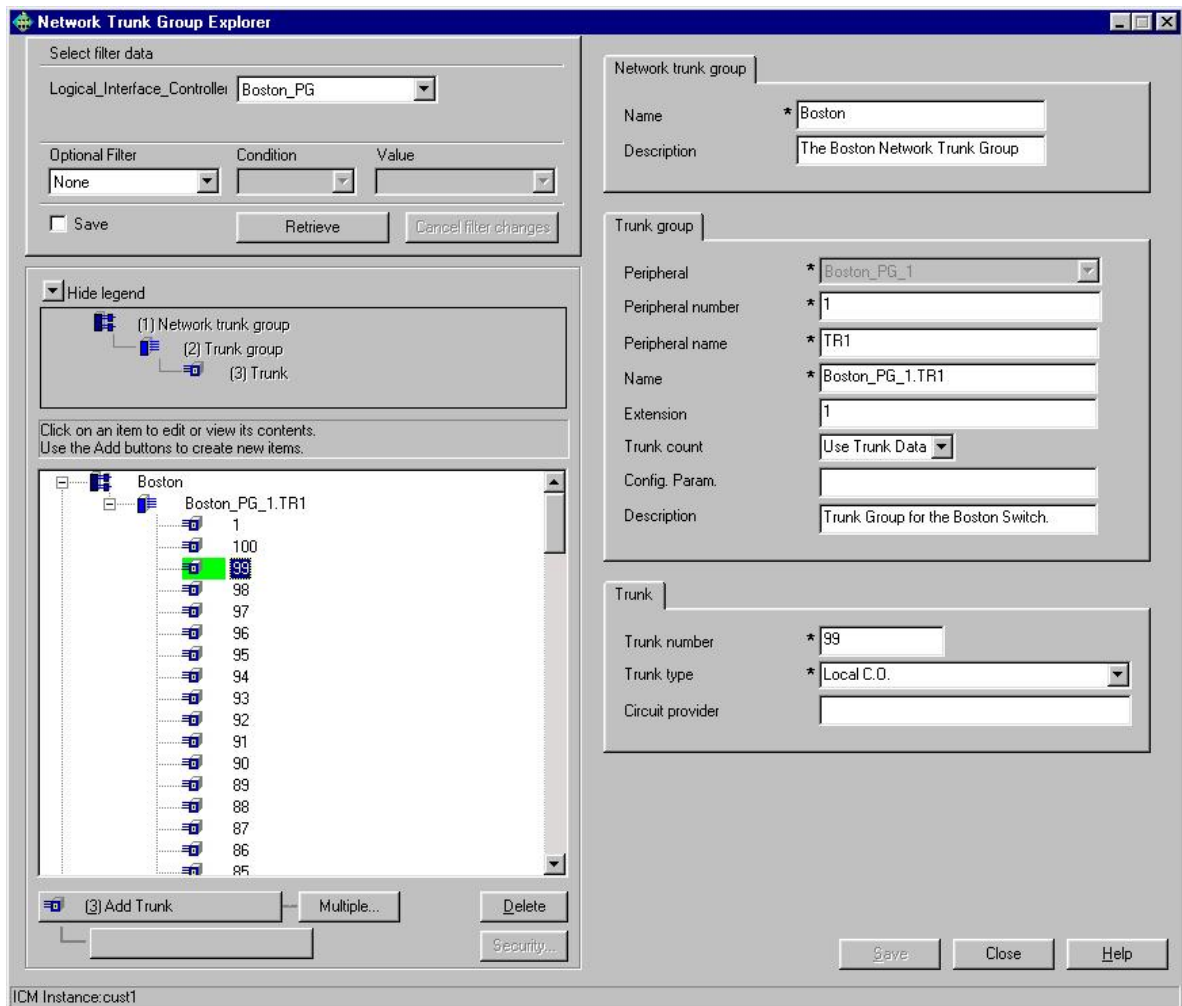
Step 2   In the **Select filter data** box, select the filters you want.

Step 3   Click **Retrieve**. This enables the **Add** button and displays a list of the retrieved network trunk groups in a tree list box on the left side of the Explorer window.

Step 4   In the tree list box, select the network trunk group whose records you want to view or modify. The selected network trunk group's configuration information displays in the tabbed fields on the right.

Step 5   To view trunk group or trunk data, expand the tree and select the tree item whose properties you want to view or edit. In the above figure, Trunk 99 is selected. This trunk belongs to the Boston_PG_1 trunk group, which belongs to the Boston network trunk group.

The property tabs on the right side of the Explorer window display the properties of the item selected in the tree list box. Properties with an asterisk are required. If you have maintenance access, you can define or edit these properties.

Edit a Network Trunk Group, Its Trunk Groups, and Trunks

To edit a network trunk group, its trunk groups, and its trunks:

Step 1 From the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Network Trunk Group Explorer**. The Network Trunk Group Explorer window appears.

Step 2 In the **Select filter data** box, select the filters you want.

Step 3 Click **Retrieve**. This displays a list of retrieved network trunk groups in a tree list box on the left side of the Explorer window.

Step 4 In the tree list box, select the item you want to edit. Expand the tree if necessary. This displays the selected item's property tab on the right side of the window.

Step 5 Edit the appropriate properties.

Step 6 Click **Save**.

Related Topics

Network Trunk Groups, Trunk Groups, and Trunks, on page 107

Define a Network Trunk Group, Its Trunk Groups, and Trunks

Follow the steps to define a network trunk group, its trunk groups, and its trunks:

Step 1 From the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Network Trunk Group**. The Network Trunk Group Explorer window appears.

Step 2 In the **Select filter data** box, select the filters you want.

Step 3 Click **Retrieve**. This displays a list of the retrieved trunk groups and enables the add functionality.

Step 4 This step depends on what you want to do:
   a) To add a new network trunk group, click **Add Network Trunk Group**.
   b) To add a new trunk group, select the network trunk group to which you want to add a group, and click **Add Network Trunk Group**.
   c) To add a new trunk, select the trunk group to which you want to add a trunk, and click **Add Trunk**.

Step 5 Enter the appropriate values in the tabbed property fields on the right side of the window.

Step 6 Click **Save**.

Related Topics

Network Trunk Groups, Trunk Groups, and Trunks, on page 107

Delete a Network Trunk Group, Its Trunk Groups, and Trunks

Follow the steps to delete a network trunk group, its trunk groups, and its trunks:

Step 1 From the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Network Trunk Group Explorer**. The Network Trunk Group Explorer window appears.

Step 2 In the **Select filter data** box, select the filters you want.

Step 3 Click **Retrieve**. This displays a list of the retrieved network trunk groups.

Step 4   In the tree list box, select the network trunk group, trunk group, or trunk whose records you want to delete.

       Note   If you select a network trunk group, the records for all trunk groups and trunks associated with it will also be deleted. If you select a trunk, only its records will be deleted.

Step 5   Click **Delete**.

Step 6   This places a **Marked for Deletion** icon ☒ next to the selected item in the tree list box. This also toggles the **Delete** button to **Undelete**.

       To undelete an item marked for deletion, select it in the tree list box and click **Undelete**.

Step 7   Click **Save**.

       This deletes from the database the item marked for deletion and removes it from the tree list box. Once you do this, you cannot undelete the deleted item.

Define Multiple Trunks

You can quickly define multiple trunks of the same type for a specific trunk group by using the **Multiple** button in the Network Trunk Group Explorer window.

To define multiple trunks:

Step 1   From within the **Network Trunk Group Explorer**, select the trunk group to which you want to add trunks. This enables the **Multiple** button.

       Note   You must have an existing trunk from the peripheral defined before you click **Multiple**.

Step 2   Click **Multiple**. The Multiple Trunk Creation dialog appears.

Figure 20: Multiple Trunk Creation Dialog
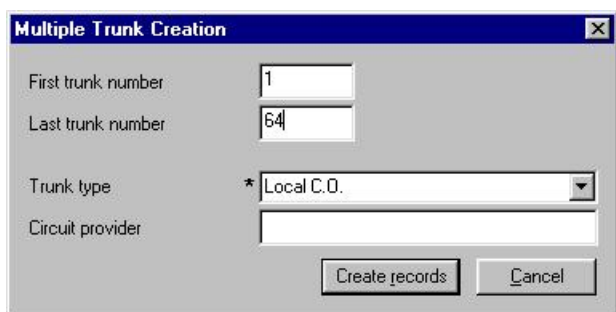
Step 3   Set the **First trunk number** and the **Last trunk number** fields so that you define the range of trunks you want.

Step 4   In the Trunk type field, select the trunk type.

Step 5   (optional) In the Circuit provider field, enter the name of the carrier that provides the circuit for this trunk.

Step 6   Click **Create records**. The tree list box will display a list of the numbered trunks beneath the selected trunk group and the Trunk tab on the right side of the window will display the properties of the trunk at the end of the series of numbers.

Step 7   In the Network Trunk Group Explorer window, click **Save**.

Note   If a trunk number in the range you specified has already been used, that trunk number is selected in the tree list box and a message displays. Before you can save the data, you must edit the trunk number.
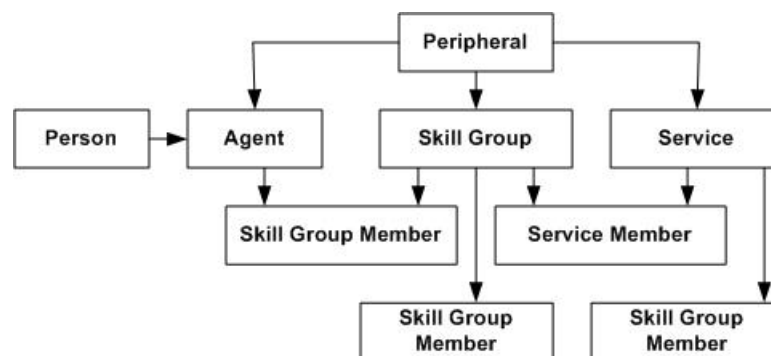
Skill Targets

Skill Targets Subsystem

After you define a peripheral, you must define the skill targets associated with the peripheral. The following figure shows the elements in a skill targets subsystem.

Figure 21: The Skill Targets Subsystem

Skill targets are the entities that the system software chooses to handle calls at a peripheral: services, skill groups, and agents.

The other members in the skill target subsystem define relationships among skill targets:

- Agents are members of skill groups.

- Skill groups are members of services.

- An enterprise skill group is a collection of skill groups, usually from different peripherals.

• An enterprise service is a collection of services, usually from different peripherals.

The rest of this chapter describes how to define these skill targets and establish the relationships among them.

Services

You must provide information about each service associated with a peripheral. A *service* is a type of caller need that the peripheral handles; for example, sales, support, and information might all be services.

Use the Service Explorer to configure services and their associated records.

Service Explorer

The following sections show you how to use the Service Explorer to view and configure a service and its associated routes, peripheral targets, and labels.

View Service

To view a service, follow these steps:

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

Step 2   In the **Select filter data** box, select the peripheral associated with the service you want to view. You can choose the name from the drop-down list.

Note	Once you have saved a service record to the Unified ICM database, you cannot change the peripheral to which it is associated.

Step 3   Select any other filters you want. **None** in the Optional filter box means all services associated with the selected peripheral will be displayed.

Step 4   Click **Retrieve**. This lists in the tree list box the names of retrieved services.

Note	A tree object is unassigned if it was made by another configuration tool and was not assigned (mapped) to a parent object; for example, a label might not have been assigned to a peripheral target or a route might not have been assigned to a service, and so on.

Step 5   In the tree list box, select a service to display its configuration information on the right side of the window.

Step 6   If the service has a route associated with it, click its icon in the tree list box to display its configuration information. Do the same for a peripheral target associated with the route and a label associated with the peripheral target.

Modifying, Defining, and Deleting Services

The following sections show you how to modify, define, and delete services.

Modify a Service

To modify a service, do the following:

Step 1   Follow the steps for viewing a service.

Step 2   Edit the configuration information.

> **Note**   You cannot modify fields that are greyed out.

> With the mouse, you can select an object and then move it to another part of the tree, as long as its object type belongs in that tree location. For example, to move a route to another service, select it and then move the pointer to that service. When that service becomes highlighted, lift your finger off the mouse. You can also use the Bulk Configuration tool to take the output of a switch and create 20 or 30 labels. Then, using the Service Explorer, you can attach the labels to an appropriate location.

> When you make a modification, the **Changed** icon appears next to the selected item in the tree list box.

Step 3   Click **Save**.

> The modified data is saved in the Unified ICM database and the **Changed** icon is removed from the edited object in the tree list box.

> **Related Topics**
> View Service, on page 114

Define a Service or Associated Record

To define a service and/or its associated records, follow these steps:

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

Step 2   In the *Select filter data* box of the Explorer window, click **Retrieve**. This enables the **Add Service** button.

Step 3   Click **Add Service**. A new service appears in the tree list box with a **To Be Inserted** icon

next to it. Tabbed fields also appear on the right for the new service's configuration information.

Step 4   Fill in the tabbed fields.

Step 5   Click **Add Route** and fill in its configuration records.

Step 6   Click **Add Peripheral Target** and also **Add Label** and fill in those records.

> Selecting an item in the tree list box enables the **Add** button for more items of that type and for the associated item immediately beneath it in the tree, if it can have one.

Step 7   If desired, set security settings on the records.

Step 8   Click **Save**.

> **Related Topics**
> Apply Security Settings

Delete a Record

To delete a record:

Step 1   In the Explorer tree list box, select the item or associated items whose records you want to delete.

| Note | Deleting any item in the tree list box with branches beneath it also deletes those branches. For example, if you delete a service, you also delete its associated route, peripheral target, and label, if it has such. Deleting a label deletes only that label. |

Step 2   Click **Delete**. This places a **Marked for Deletion** icon ☒ next to the selected item in the tree list box. This also toggles the **Delete** button to **Undelete**.

To undelete an item marked for deletion, select it in the tree list box and click **Undelete**.

Step 3   Click **Save**.

This deletes from the database items marked for deletion and removes them from the tree list box. Once you do this, you cannot undelete deleted items.

Skill Groups

Enter information about each skill group associated with each peripheral. A *skill group* is a collection of agents that share a common set of skills.

Use the Configuration Manager's Skill Group Explorer to view, modify, or define a skill group.

Skill Group Explorer

The following sections show you how to use the Skill Group Explorer to view and configure a skill group and its associated routes, peripheral targets, and labels.

View a Skill Group

To view a skill group, follow these steps:

Step 1   In the Configuration Manager's menu, select **Tools** > **Explorer Tools** > **Skill Group Explorer**. The Skill Group Explorer window appears.

Step 2   In the **Select filter data** box, select the peripheral associated with the skill group you want to view. You can choose the name from the drop-down list of peripheral enterprise names.

Step 3   Select any other filters you want. None in the Optional filter box means all skill groups associated with the selected peripheral will be displayed.

Step 4   Click **Retrieve**. This lists in the tree list box names of skill groups.

Step 5   In the tree list box, select a skill group to display its configuration information on the right side of the window.

Step 6   If the skill group has a route associated with it, click its icon in the tree list box to display its configuration information. Do the same for a peripheral target associated with the route and a label associated with the peripheral target.

Note A tree object is unassigned if it was made by another configuration tool and was not assigned (mapped) to a parent object; for example, a label might not have been assigned to a peripheral target or a route might not have been assigned to a service, and so on.

Modifying, Defining, and Deleting Skill Groups

The following sections show you how to modify, define skill groups.

Modify a Skill Group

To modify a skill group, follow these steps:

Step 1 Follow the steps to view a skill group.

Step 2 Edit the configuration information.

With the mouse, you can select an object and move it to another part of the tree, as long as its object type belongs in that tree location. For example, to move a route to another skill group, select it and move the pointer to that skill group. When that skill group becomes highlighted, lift your finger off the mouse. You can also use the Bulk Configuration tool to take the output of a switch and create 20 or 30 labels. Then, using the Explorer, you can attach the labels to an appropriate location.

Note You cannot modify fields that are greyed out.

You cannot update the Peripheral field. To modify the Peripheral Number, you can use the Cisco Unified Contact Center Management Portal (CCMP).

When you make a modification, the **Changed** icon ⇨ appears next to the selected item in the tree list box.

Step 3 Click **Save**.

The modified data is saved in the Unified ICM database and the **Changed** icon is removed from the edited object in the tree list box.

Related Topics

Define a Skill Group or Its Associated Records

✎

Note contains an example of how to configure skill groups for a child deployment.

To define a skill group and/or its associated records, follow these steps:

Step 1   In the Configuration Manager's menu, select **Tools** > **Explorer Tools** > **Skill Group Explorer**. The Skill Group Explorer window appears.

Step 2   In the **Select filter data** area of the Explorer window, click **Retrieve**. This enables the **Add Skill Group** button.

Step 3   Click **Add Skill Group**. A new skill group appears in the tree list box with a **To Be Inserted** icon next to it. Tabbed fields also appear on the right for the new skill group's configuration information.

Step 4   Fill in the tabbed fields.

      Note   These fields are not automatically populated.

Step 5   Click **Add Route** and fill in its configuration records.

Step 6   Click **Add Peripheral Target** and also **Add Label** and fill in those records.

      Selecting an item in the tree list box enables the **Add** button for more items of that type and for the associated item immediately beneath it in the tree, if it can have one.

Step 7   If desired, set security settings on the records.

Step 8   Click **Save**.

        Related Topics

           Apply Security Settings

Skill groups on the Child Central Controller

Access the Configuration Manager on the Child Administration & Data Server to configure skill groups.

Configure Skill Groups on the Child Central Controller

Use the Configuration Manager Skill Group Explorer Tool to configure skill groups SG01 and SG02 on the Child Central Controller.

To configure skill groups on the Child Central Controller:

Step 1   Start the **Skill Group Explorer Tool**.

Step 2   On the Main window of the Agent Explorer Tool, click **Retrieve**.

Step 3   Click **Add Skill Group**.

      The Skill Group tab appears.

Step 4   Complete all the fields and click **OK**.

      The skill group name appears in the list, as with all Explorer tools.

Step 5   Select the **Skill Group Member** tab and click **Add**.

      The Add Skill Group Member dialog appears.

Step 6   Select the agents to add to the skill group, then click **OK**.

      The agents become members of the skill group.

Step 7   Select the skill group in the tree list, then click **Add Route**.

The Route tab appears.

Step 8   Provide the Route Name and click **Save**.

The route name appears in the tree list and the skill group is added to the peripheral.

Step 9   Repeat this to add one more skill group.

Step 10   Click **Save**, then **Close** to exit the Skill Group Explorer Tool.

Skill Groups–to–Services Mapping

When you define services and skill groups, you can establish the mappings of skill groups to services. Each skill group can be mapped to zero, one, or more services; each service can be mapped to zero, one, or more skill groups.

You can define some service member skill groups as being primary for the service. The system software uses the primary attribute in determining the destination for a call to the service. For example, the Longest Available Agent (LAA) for a service is really the LAA for primary groups configured for that service.

Map Skill Groups to Services

To map skill groups to services, follow these steps:

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

Step 2   Select the filters you want and click **Retrieve**. The retrieved services appear in the list box.

Step 3   Select the service you want and click the **Service Members tab**.

Step 4   This step depends on whether you want to add or to remove skill groups:

   a) To remove skill groups, select a skill group's name and click **Remove**.

   b) To add skill groups, click **Add** and in the **Add Service Member** dialog, select the skill groups and click **OK**.

   The available skill groups are all those defined for the selected peripheral.

Step 5   In the Service Members tab, select the **Primary** check box for any skill groups that you want to be primary.

Step 6   When finished, in the Skill Group Explorer window, click **Save**.

Skill Groups Per Agent Limit

Unified ICM and Unified CCE impose a default limit on the number of skill groups that you can assign to a single agent. Once this limit is reached, more skill groups cannot be assigned.

You can use the Configuration Limit Tool to specify your own limit on the number of skill groups that can be assigned to an agent. For optimum performance, you can specify a limit far lower than the system default.

For performance considerations in choosing a skill groups per agent limit, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

Warning Setting a default value for skill groups per agent that is higher than the system default can adversely affect system performance. Cisco does not support configurations that exceed the default value.

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 the Setup or Config Groups in Active Directory for the chosen customer instance. For more information about the Configuration Limit tool, see the *Outbound Option Guide for Unified Contact Center Enterprise*.

Change Skill Groups Per Agent Limit

To change the skill groups per agent limit using the Configuration Limit tool, complete the following steps:

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 currently configured parameter limits, run the following command:

```
cl /show
```

Step 3 To change the skill groups per agent limit, enter a command in the following format:

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

Where:

- id 1 = the ID of the skill groups per agent limit.

- ConfigLimitCurrentValue = the parameter limit. In this case, the parameter limit is the skill groups per agent limit.

For example, to change the skill groups per agent limit to 5, enter the following:

```
cl /id 1 /value 5 /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 will be enforced immediately. Note that the new limit will *not* affect 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 will be enforced, preventing you from adding additional skill groups.

Exceeding the Default Limit

If you modified the skill groups per agent limit to be higher than the system default (despite the preceding warning), certain deployments require additional changes to your system to use the new limit. These additional changes (listed in the following sections) also allow you to add more skill groups.

UCCE Gateway PG

For UCCE Gateway deployments, modify the following registry keys on your UCCE Gateway PGs to include the new value. A change to the registry will require that the PG service be restarted.

Cisco Unified Contact Center Enterprise Gateway Peripheral Interface Manager (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
```

Cisco Unified Contact Center 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
```

Persons

Associate every agent with a person record. The person record stores the login name, first name, last name, and password. On Unified ICM you can have multiple agents per person. An agent is an "extension" of a person on a given peripheral.

The Person List tool allows you to list the persons currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones.

✎

Note   If you are using the Enterprise Chat and Email feature, you can create Agents in CCE Configuration Manager. Creating Agents in the Enterprise Chat and Email makes them available in Configuration Manager. However, if you create the agent in Configuration Manager, you must enable the agent in Enterprise Chat and Email.

Available person records are records that have not been mapped to any agent records (including logically deleted ones) at the peripheral selected in the Agent Explorer. To free a person associated with a logically deleted agent, use the Configuration Manager's Deleted Objects tool to permanently delete the logically deleted agent.

Agents

An *agent* is a person who handles calls from a peripheral or supervises those who do. You need to set up each agent associated with each peripheral.

An *agent gadget* is an application which handles calls from a peripheral. You need to set up each agent gadget associated with each peripheral.

Use the Configuration Manager's Agent Explorer to configure agents.

Related Topics

Modify Agent Record

To view or modify agents records, follow these steps:

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. Enter any other filters you want and click **Retrieve**.

The retrieved enterprise names for the agents are displayed in the list box.

Step 3   Select the agent name whose properties you want to view and use the tabs on the right side of the window to view the properties.

Step 4   Edit the properties appropriate. See the online help if you have questions.

Step 5   When finished, in the Agent Explorer window, click **Save**.

Create an Agent

An *agent* is a person who handles calls from a peripheral or supervises those who do. You need to set up each agent associated with each peripheral.

When you create a new agent, you can also identify the agent as a supervisor.

Note   contains an example of how to configure agents for a child deployment.

⚠️

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.

To create an agent:

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**.

Step 4 In the property tabs on the right side of the window, enter the appropriate property values. (See the online help for field definitions.) Use the Agent tab to define the agent (and optionally designate the agent as a supervisor) and the Skill Group Membership tab to map the agent to any skill groups.

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**.

Agent Configuration on the Child Central Controller

Access the Configuration Manager on the Child Administration & Data Server to configure agents.

Configure Agents on the Child Central Controller

Use the Configuration Manager Agent Explorer tool to configure agents on the Child Central Controller.

✎

Note When you configure an agent on the Child Central Controller, the agent is automatically assigned to a default skill group. However, if you log onto the parent to view the agent (that you configured on the child), the default skill group appears in the list of assigned skill groups and not in the default skill group box.

To configure agents on the Child Central Controller:

Step 1 Start the **Agent Explorer tool**.

Step 2 On the Main window of the Agent Explorer tool, click **Retrieve**.

Step 3 Click **Add Agent**.

The Agent tab appears.

Step 4   Complete all the fields except the Password and the Peripheral Name fields.

The agent name information appears in the list, as with all Explorer tools.

Step 5   Repeat this process to add at least three agents.

Step 6   Click **Save**, and then **Close** to exit the Agent Explorer tool.

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:

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**.

Agent to Skill Group Assignment

After you have set up skill groups and agents, enter the assignments of agents to skill groups as configured for the peripheral. Each agent can belong to zero, one, or more skill groups.

You can use the Configuration Manager's Skill Group Explorer to map agents to skill groups.

Assign Agents to a Skill Group

Follow these steps to assign agents to a skill group:

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

Step 2   Select the filters you want and click **Retrieve**. The retrieved agents appear in the list box.

Step 3   Select the agent you want assign to a skill group and click the **Skill Group Membership** tab.

Step 4   This step depends on whether you want to add or remove an agent. On the Skill group membership tab:

   a)   To remove the selected agent from a skill group, select the appropriate skill group and click **Remove**.

   b)   To add the selected agent to a skill group, click **Add**, and in the Add Skill Group Member dialog, select the appropriate skill group and click **OK**.

Step 5   When finished, in the Agent Explorer window, click **Save**.

Enable or Disable Agent Data at a Peripheral and Define an Agent Distribution

Follow these steps to enable/disable agent data at a peripheral and define an agent distribution:

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

Step 2   Click **Retrieve**.

Step 3   In the tree list box, expand the appropriate logical controller and select the peripheral.

Step 4   In the Agent Distribution tab, select or deselect the **Enable agent reporting** check box.

Step 5   In the Agent Distribution Entries list box, select an existing distribution site or create a new one by clicking **New** and entering values for the following fields:

   a)   **Administration & Data Server site name**. The Admin site name for the Primary/Secondary Pair (Site) name, as specified in the Web Setup tool.

   b)   **Agent real time data**. If checked, enables the flow of agent real time data from the peripheral to the Administration & Data Server. Unchecked, disables the flow of agent real time data.

   c)   **Agent historical data**. If checked, enables the flow of agent historical data from the peripheral to the Administration & Data Server. Unchecked, disables the flow of agent historical data.

Step 6   Click **Save** to apply your changes.

Agent State Trace

You can set Agent State Trace to track every state (available, talking, and so on) that an agent passes through. To turn on this feature for an agent, in the **Agent Explorer**, on the **Advanced** tab, check the **Agent State Trace** check box.

✎

| Note | When you enable Agent State Trace, the system tracks every state change for each agent you select. This puts an added load on system software resources, such as network bandwidth and database space, and can impact system performance. You may only track up to 100 agents with Agent State Trace at any one time. You should also take the added load into account when planning your system capacity. |

When you check the **Enable agent reporting** check box, configure the **Agent distribution entries** in the **PG Explorer** tool, and check the **Agent State Trace** check box, the Agent_State_Trace table in the database is populated.

Agent Configuration Data from Peripheral

An automatic call distribution (ACD) requires all the available agents to be configured to allow the agents to log in to the call handling devices with their peripheral number (Agent ID) or peripheral name, password, and so on. Also, these agents are configured to handle specific categories of calls based on Skill Group. There are some other data elements configured on the ACD such as last name, first name, and other class of services.

The Unified ICM Agent Level Reporting requires these agents to be configured in Unified ICM to identify them with full name, peripheral name, or enterprise name on both the real-time and historical reports.

The agentcfg.exe command line tool provides a process of configuring the agent configuration data elements available on an ACD into the Agent table in the Unified ICM database. This can also be automated by scheduling the process to run as an AT job at a specific time during a day. The frequency of scheduling the agent configuration process depends on your requirements.

Each peripheral requires the Agent configuration process to run.

Import Agent Data

Follow these steps to import agent data:

Step 1 Retrieve the agent configuration data from the peripheral.

Step 2 Form all the information in a tab-delimited text file with one row per agent. Each row of the file must contain the following fields, in order:

```
PeripheralNumber FirstName LastName Description PeripheralName
```

Step 3 To import data from the file into the system software, enter one of the following commands at the command prompt:

```
AgentCfg <Peripheral ID or Peripheral Name> <Input file name> [<Second input file>] [<Option>]
```

These variables are defined as:

a) <Peripheral ID or Peripheral Name>:

Peripheral ID or Peripheral Name of the peripheral that you want to configure.

b) <Input file name>:

The name of the input file contains the agent *or* skill group member configuration data on the ACD in the appropriate format (described in the next section). The file must contain header information, otherwise the tool assumes the data is for the Agent table.

Full or relative path is allowed.

c) <Second input file>:

If the first file contains Agent data, the second file must contains Skill Group Member data. If the first file contained Skill Group Member data, the second file must contain Agent data.

If no files contain headers, it is assumed that Agent data is in the first file and Skill Group Member data is in the second file. If headers are provided, the files may be specified in either order.

Full or relative path is allowed.

d) <Option>:

/show Only - show configuration changes without committing to the database.

/nodelete - the tool will not perform any delete operations. All inserts and updates will be saved.

Example:

1. `AgentCfg.exe peripheral1 c:\temp\agentData.txt c:\temp\skillGrpMemData.txt`

   This example will configure both agent and skill group member data for peripheral1.

2. `AgentCfg.exe peripheral1 c:\temp\skillGrpMemData.txt`

   This example will configure skill group member data for peripheral. The file must contain header information.

Step 4 When the system software invokes the AgentCfg command, it performs the following steps for each line in the input file:

The following steps are performed for each line in the input file:

a. The system software attempts to match the PeripheralNumber value to a configured agent for the peripheral.

   If it finds a match, it proceeds directly to step b.

   If it cannot find a match, it creates a new agent row in the database using the data from the input file, and proceeds to step b.

b. The system software checks to see if the "temporary" flag is set. If it is, it updates the existing record.

c. The system software checks whether the peripheral name values also match.

   If the FirstName and LastName values match, the system software updates the existing record with the given Description and PeripheralName values. (If the existing record was for a temporary agent, the agent is no longer temporary after the update.)

   If the values do not match, the system software marks the existing record as deleted and inserts a new row with the data from the input file. If an agent is configured for the peripheral in the database, but is not listed in the input file, the system software marks the agent as deleted in the database.

d. The system software does a loop through the Skill Group Member input file container and compares the records in the file with those in the database:

   • If the record is found in the file but does not exist in the database, the record is inserted.

   • If the record is found in the database but does not exist in the file, the record is deleted.

Input File Formats

When using the AgentCfg.exe tool to import data, the input files must be formatted as described below. Note that the _ _TABLE and _ _COLUMNS entries, and the line below each are together considered the header. The header is not always required. The beginning of this section indicates when headers are needed.

Agent Configuration Data File

The input file must contain the list of all the agents configured on the ACD for that peripheral in the following format:

```
_ _TABLE
Agent
```

Indicates the name of the table to which the data will be configured. The table name is always **Agent** (do not change this line).

```
_ _COLUMNS
```

Indicates the tab-delimited column names that correspond to the data values (do not change this line). The columns need to be in the order shown below:

```
PeripheralNumber<tab>FirstName<tab>LastName<tab>Description<tab>PeripheralName

1045<tab>F1045<tab>L1045<tab>Auto Configured by Router<tab>F1045.L1045

1046<tab>F1046<tab>L1046<tab>Auto Configured by Router<tab>F1046.L1046

1047<tab>F1047<tab>L1047<tab>Auto Configured by

Router<tab>F1047.L1047<eof>
```

The following indicates the tab delimited data values that correspond to the column names:

```
1045<tab>F1045<tab>L1045<tab>Auto Configured by Router<tab>F1045.L1045
```

Skill Group Member Configuration Data File

Note that the __TABLE and __COLUMNS entries and the line below each are together considered the header. The header is not always required.

The input file contains the list of all the skill group member data as a relation between skill group and agents, which configured on the ACD for that peripheral in the following format:

```
_ _TABLE
Skill_Group_Member
```

Indicates the name of the table to which the data will be configured. The table name is always **Skill_Group_Member** (do not change this line).

```
_ _COLUMNS
```

Indicates the tab delimited column names that correspond to the data values (do not change this line). The columns need to be in the order shown below.

```
SkillGroupEnterpriseName <tab> AgentPeripheralNumber SkillGroupExterprise1<tab>1045
SkillGroupExterprise2<tab>1046 SkillGroupExterprise1<tab>1046
```

SkillGroupEnterpriseName is the ExterpriseName of the skill group that the agent belongs to.

AgentPeripheralNumber is the agent's login ID assigned at the switch, which is the same as the above Agent Peripheral Number.

The following indicates the tab delimited data values that correspond to the column names:

```
SkillGroupExterprise1<tab>1045
```

Manage Security

The system generates agent passwords using advanced hashing.

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

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

1. All the PG's must be version 12.6 (1) or later.

2. All the agent passwords must be re-entered.

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

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

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

Enterprise Data

Within a script, you often want to examine a set of possible targets on different peripherals before deciding where to send the call. For example, if you are routing a sales call, you might want to check the Sales skill groups at each call center to find which has the longest available agent or shortest expected delay.

An *enterprise service* is a set of services that can be referenced in a script. The individual services can be associated with different peripherals. Similarly, an *enterprise skill group* is a set of skill groups that can be referenced in a script. The individual skill groups can be associated with different peripherals.

In addition to using them within a script, you can track enterprise services and enterprise skill groups through monitoring screens and reports. This allows you to easily follow the performance, for example, of all Support services within the system.

Enterprise Services

Within a routing script, you can use an enterprise service as a shorthand for a set of services. You might want to scan several services to find, for example, the service with the shortest expected delay. Within the script, you can specify individual services to scan or, if you have an enterprise service defined, you can simply specify the enterprise service.

Assign Specific Services

Follow these steps to create an enterprise service and assign specific services:

Step 1   In the Configuration Manager menu, select **Tools** > **List Tools** > **Enterprise Service List**. The Enterprise Service List window appears.

Step 2   In the Select filter data box, select the filters you want and click the Members tab. This enables the **Add** button and lists the currently defined enterprise services for the selected business entities.

Step 3   Click **Add**.

Step 4   In the Attributes tab, enter values for the following fields:

    a) **Name**. A name for the enterprise service. This name must be unique among all enterprise services in the system.

    b) **Business Entity**. Reserved for future use.

    c) **Description**. Any other information you want about the enterprise service. Any other information you want to add about the enterprise service.

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

Step 6   Click the **Attribute** tab.

Step 7   In the **Attribute** tab, click **Add**.

Step 8   In the **Add Services** dialog, select the services you want to add and click **OK**. The dialog closes and the selected services are listed as members in the **Attribute** tab.

Step 9   When finished, click **Save** to save the changes.

Enterprise Skill Groups

Just as you can use an enterprise service as a shorthand for a collection of services, so you can use an enterprise skill group as a shorthand for a collection of skill groups. The skill groups can be defined on different peripherals.

Create an enterprise skill group

Follow these steps to create an enterprise skill group:

Step 1   In the Configuration Manager menu, select **Tools** > **List Tools** > **Enterprise Skill Groups List**. The Enterprise Skill Group List window appears.

Step 2   In the Select filter data box, select the filters you want and click **Retrieve**. This enables the **Add** button and lists the currently defined skill groups for the selected business entities.

Step 3   Click **Add**, and in the **Attributes** tab, enter values for the following fields:

    a) **Name**. A name for the enterprise skill group. This name must be unique among all enterprise skill groups in the system.

    b) **Business Entity**. Reserved for future use.

    c) **Description**. Any other information you want to add about the enterprise skill group.

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

Step 5   Click the **Members** tab.

Step 6 In the Members tab, click **Add**.

Step 7 In the Add Enterprise Skill Group Member dialog, select the skill groups you want to add and click **OK**. The dialog closes and the selected skill groups are listed as members in the Members tab.

> **Note** The Skill Group list includes base skill groups as well as primary and secondary groups for those switches that support them. Typically, add either the base group or the associated primary and secondary groups, but not all three, to the enterprise skill group.

Step 8 Click **Save** to save the changes to the database.

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.

Routing and Routing Targets

Routes and Targets Subsystem

For every routing request it processes, the system software determines an announcement to be played to the caller, a route for the call, or a special action such as ring-no-answer or signal busy.

To see the elements of the routes and targets subsystem and the order in which you must define them, see the following figure. Note that elements in this subsystem depend on elements defined in the routing client and peripheral subsystems. For example, you must define a network trunk group and trunk group, which are part of the peripheral subsystem, before you can define a peripheral target.

Figure 22: Routes and Targets Subsystem
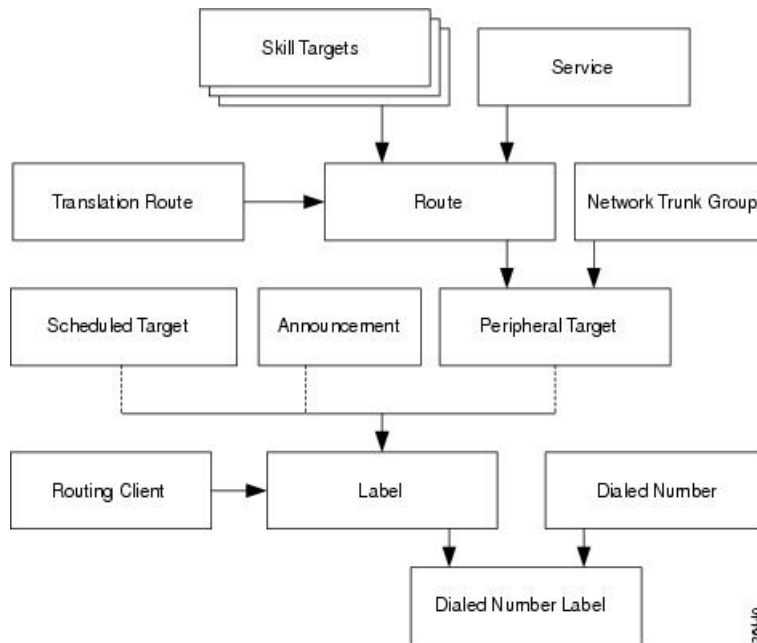
Routing Targets

The system software can route a call to a carrier resource such as an announcement or to a target at a peripheral. A peripheral, such as an ACD, PBX, or Unified Communications Manager (Unified CM) dispatches calls within a contact center.

Peripheral targets

Depending on the capabilities of the peripheral and the type of routing instructions you use, the system software might choose a specific agent at the peripheral to handle the call. In that case, the peripheral merely dispatches the call to the chosen agent. In other cases, the system software might specify only a group of agents or a type of service to be provided to the caller.

The system software can route to three types of peripheral targets:

- **Agent**. A specific individual who receives calls through the peripheral. (The system software, however, cannot guarantee that the specific agent will be available when the call arrives.) The Queue to Agent node allows the targeting of a task (the work performed by an agent) to a script-specified agent. This node enables an agent to receive and operate on more than one task at a time.

- **Skill group**. A group of agents who share a common set of skills and who can, therefore, all handle a specific type of calls. Each skill group contains one or more agents. If supported by the peripheral, each agent can be a member of more than one skill group.

- **Service**. A type of processing the caller requires. For example, a peripheral might have services defined for sales, technical support, or opening new accounts. Each service has one or more skill groups whose members can provide the service. Each skill group can be associated with more than one service.

In the last two cases, the peripheral must choose a specific agent within the group who can provide the service. In each case, the peripheral plays a key role in completing the routing that the system software has determined.

Therefore, the system software and the peripheral must be set up to complement each other. They must have the same understanding of the agents, skill groups, and services available at each site.

Scheduled Targets

Some routing clients also support *scheduled targets*. A scheduled target is a group of agents not associated with a Peripheral Gateway. The system software cannot monitor the group directly. Instead it relies on a periodic schedule to determine the number of agents logged on to the group. The routing client informs the system software when a call to the group ends. Since the system software knows how many calls it has routed to the group, it can determine the number of calls in progress. Based on this and the schedule, the system software can determine whether the target can handle an additional call.

Route Configuration

A route consists of two components:

- The skill target (agent, skill group, service, translation route, or service array) at a peripheral which can handle a call.

- The service by which the peripheral classifies the call.

Note You must have defined the skill target and service before you can configure a route. Follow the steps in the Configuration Manager's Step by Step Configuration menu when configuring your Unified ICM system.

Define a Route

In the Configuration Manager, you can define and update many routes at a time using the Route Bulk tool. Or you can create and update a route using one of the following Explorer tools:

- Agent Explorer
- Skill Group Explorer
- Service Explorer
- Service Array Explorer
- Translation Route Explorer

With the Explorer tools, you can define and update a route at the same time you define and update its target. To access all the tools for creating routes:

Click **ICM Configure** > **Targets** > **Route**.

See following figure.

Figure 23: Configuration Manager Route Tools
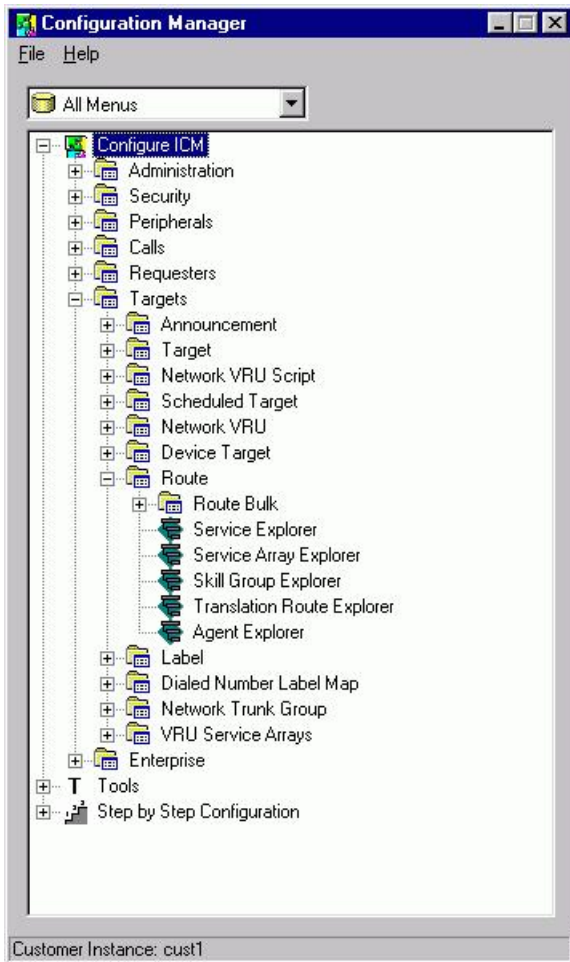
Modify a Route

Use the Configuration Manager's Route Bulk tool to create multiple routes. To create individual routes, use the Configuration Manager's Explorer tool appropriate for the route target. Follow the instructions in the online help.

To modify routes with the Explorer tools:

Step 1   In the appropriate Explorer window:

- To define a new route, select the target for which you are creating the route and click **Add Route**.

- To modify a route, select the route.

Step 2   In the Route tab, enter values for the following fields:

- **Name**. A unique name for the route. You might derive the name for the route from the skill target and service associated with it. For example, you might have a route associated with the Dallas.TeleSales service and the Dallas.Sales skill group. You might name the route *Dallas.TS_Sales*.

- **Description**. Text identifying the route.

- **Service name**. (selection list) Every route must be associated with a service. By choosing a service, you are implicitly associating the route with the peripheral for that service. For a new route, the drop-down list contains all the services defined for the selected peripheral (or PG, in the case of a service array).

  To assign the route to another service, in the tree list, drag it to the desired peripheral. You can also move the route to the UNASSIGNED list.

  Warning   When you break the association between a route and a peripheral, the system software removes the Route ID value from all peripheral targets that reference that route.

Step 3   Click **Save**. The system software saves your changes in the database.

Set a Default Route for Each Peripheral

After you have defined routes, you can set a default route for each peripheral. The system software uses the default route to classify calls for statistical purposes.

For each call that arrives at a peripheral, the system software records monitoring information in the real-time and historical tables for the route associated with that call. If the system software cannot determine a route for the call, it uses the default route defined for the peripheral.

By defining a default route for each peripheral, you ensure that the system software captures route information for every call. You might want to create a special route for this purpose. You can then determine which calls are not being accounted for properly.

To set a default for each peripheral:

Step 1   In the Configuration Manager menu, select **Tools** > **Explorer Tools** > **PG Explorer**. The PG Explorer window appears.
Step 2   In the tree list window, select the peripheral you want to modify and click the **Default Route** tab.
Step 3   In the **Default Route** tab, select the enterprise name of a route from the selection list. The list includes all routes associated with skill targets at the chosen peripheral.
Step 4   After choosing the route, click **Save** to enter your edits into the database.

Network Targets

Routing clients do not send calls directly to services, skill groups, or agents. They send each call to an announcement or to a specific trunk group at a peripheral. If the call is sent to a trunk group, the routing client can also send a DNIS value for the call. The combination of trunk group and DNIS value is a peripheral target.

You must define the announcements and peripheral targets that the routing clients use. These are called *network targets*. Later, you can associate a routing label with each network target.

Define Peripheral Targets

A peripheral target is a combination of a network trunk group and a DNIS value. You must work with your interexchange carrier or other routing client to set up the trunk groups on which you expect to receive calls and the DNIS values that are sent with them.

To define peripheral targets:

Step 1   In the Configuration Manager menu, select **Configure ICM** > **Targets** > **Target** from the menu bar.

The resulting menu (see the following) allows you to create multiple peripheral targets, using the Peripheral Target Bulk configuration tool or creating a peripheral target for a service, a service array, a skill group, a translation route, or an agent. Select the appropriate tool for your needs.

Figure 24: Configuration Manager Target Submenu
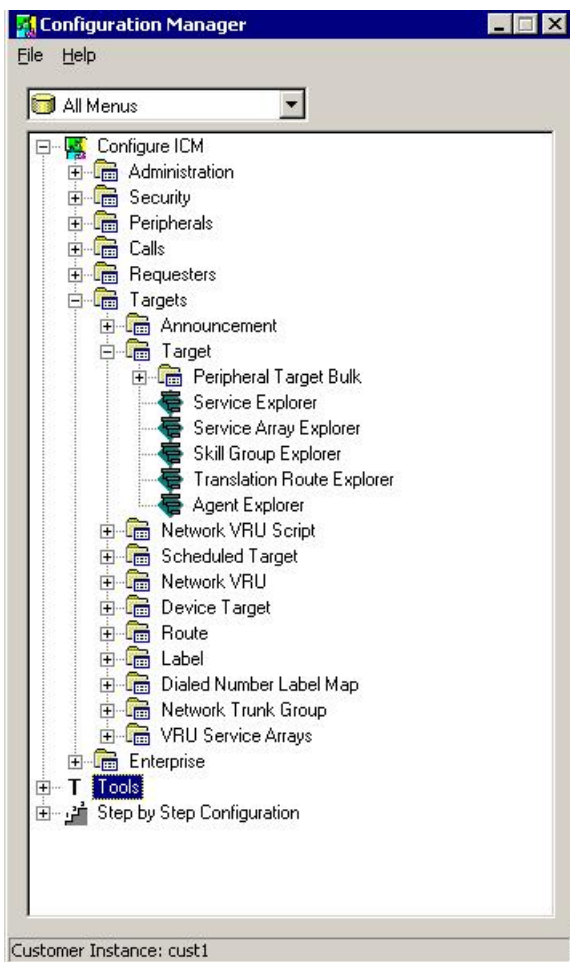
Step 2   Use the online help if you have questions.

Step 3   When finished, click **Save**.

Announcement Configuration Information

You must provide information about any announcements to which you want to route calls. You must work with the IXC or other routing client to set up announcements within the network and assign labels to them. You can then enter information about the labels into the Unified ICM system.

Add Announcement Configuration Information

To add announcement configuration information:

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

Step 2 Click **Retrieve**. This enables the **Add Announcement** button.

Step 3 Click **Add Announcement**.

Step 4 In the Announcement tab, enter values for the following fields:

- **Name**. A unique name for the announcement.

- **Description**. Text identifying the announcement.

Note You can save at this point and then add the label information in the following step.

Step 5 To associate a label with the announcement:

- In the tree list window select one from the UNASSIGNED group and drag it to the announcement.

- Select the announcement and click **Add Label**. Then in the Label tab, enter the appropriate field information.

Note A description of the Label tab fields and buttons is in the online help.

Step 6 Click **Save** to save the announcement configuration settings. The system software automatically generates a unique Network Target ID value.

Labels

After defining announcements and peripheral targets, you must define the labels that your routing clients use to reference network targets. The label is the value that the system software returns to the routing client. The routing client then translates the label to an announcement or peripheral target (trunk group and DNIS) that the peripheral will convert to the skill target and service you specify.

Note For an AT&T ICP connection, the system software treats a CRP code as a label.

Label Types

In defining a label, you must specify a label *type* by selecting an option from the Type drop-down list in the Label Configuration selection box.

Note Each label you define is valid only for a specific routing client; not all label types are valid for all types of routing clients. Check with your carrier for the latest information about supported label types.

The following table lists the configured label types the system software supports. In addition to these labels, a script can create a *dynamic* label, which is defined in real time through a script expression and then passed to a routing client.

Table 20: Supported Label Types

Label type	Description	Routing clients	How to send label
Normal	Maps to a trunk group and DNIS or announcement defined by the routing client.	All	Specify an associated route in a routing script target.
DNIS Override	Sends a value along with the label that overrides the DNIS value of the routing client.	MCI	Specify an associated route in a routing script target.
Busy	Plays a busy signal for the caller.	All	Use a Busy or Termination script node.
Ring	Plays an unanswered ring for the caller.	AT&T GTN	Use a Ring or Termination script node.
Post-Query	Specifies a re-entry point in the network routing plan. The routing client begins processing the routing plan from that point.	All	Use a Return Label script node.

The Normal and DNIS Override types are used for peripheral targets (and hence, for routes) or for announcements. Busy, Ring, and Post-Query labels are not associated with any target in the Unified ICM configuration. The routing client uses its own special targets for labels of these types.

For more information on targets within scripts, refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.

Label Setup

To set up a label, you create configuration information and associate the label with a network target.

Create Label

To create a label, follow these steps:

Step 1   In the Configuration Manager menu, select **Configure ICM** > **Targets** > **Label**.

This displays the following menu options for configuring a label:

- Label Bulk

- Label List

- Service Explorer

- Service Array Explorer

- Skill Group Explorer

- Translation Route Explorer

- Agent Explorer

- Announcement Explorer

- Network VRU Explorer

Step 2   Select the tool you need:

- Use the Label Bulk tool to configure many labels at a time.

- Use the Label List tool to configure individual labels for any network targets.

- Use the remaining Explorer tools to configure labels for a specific network target (services, service arrays, skill groups, translation routes, agents, announcements, network VRUs).

Step 3   Enter values for the following fields. Use the online help if you have questions:

- **Routing Client** (required)

The enterprise name of the routing client that can receive this label.

- **Label** (required)

The literal string of characters to be returned to the routing client.

- **Label Type**. (required)

The type of label. The valid types depend on the type of the routing client.

- **Target type**

(selection list) Indicates the type of the network target associated with the label: Network Announcement, PBX/ACD Peripheral (that is, a peripheral target), a scheduled target, or a network VRU.

> **Note**   The Target type is a filter for the Network target field. The Target type selected is not retained unless a Network target is selected.

- **Network target**. (list and bulk tools only)

(selection list) Indicates the announcement, peripheral target, or scheduled target associated with the label.

- **Customer**. (list and bulk tools only)

The customer associated with the label.

- **Description**.

  Any other information you want about the label.

The following table lists which targets are valid for each label type.

Table 21: Valid Label Targets

Label	ACD/PBX	Network announcement	Scheduled target	Network device	Network VRU
Normal	Valid	Valid	Valid	Valid	Valid
DNIS Override	Valid	Valid	Valid	Valid	Valid
Busy	—	—	—	—	Valid
Ring	—	—	—	—	Valid
Post-Query	Valid	—	Valid	Valid	Valid

Step 4 Click **Save**.

Label Mapping

For some routing clients, all labels are valid for all dialed number/script selectors. For other routing clients, you must specify which labels are valid for each dialed number/script selector. You specify whether the mapping of labels to dialed number/script selectors is necessary when you configure the routing client.

Map Specific Labels to a Dialed Number/Script Selector

To map specific labels to a dialed number/script selector, follow these steps:

Step 1 In the Configuration Manager menu, select **Tools** > **List Tools** > **Dialed Number/Script Selector List**. The Dialed Number/Script Selector List window appears.

Step 2 Select the filters you want and click **Retrieve**. The enterprise names for the retrieved dialed number/script selectors are listed in the list box.

Step 3 Select the enterprise name for the dialed number/script selector you want.

Step 4 Click the **Dialed Number Label** tab.

The Name column displays a list of all labels currently associated with that dialed number/script selector.

Note For a call associated with this dialed number/script selector, the system software can return only labels assigned to the dialed number/script selector.

Step 5 Click **Add**.

Step 6 In the **Add Label** dialog, select a label name and click **OK**.

Note For labels to appear in this dialog selection box, they must have been previously defined for the selected dialed number/script selector's routing client. Use the Label List tool to define labels.

Step 7   Click **Save**.

Set a Default Label for Each Dialed Number/Script Selector

After you have defined labels, you can set a default label for each dialed number/script selector. If the system software fails to find a label by running the routing scripts for the call type, it uses the default label for the dialed number/script selector.

You can use Configuration Manager's Dialed Number Bulk tool to configure many dialed number/script selectors at a time or the Dialed Number/Script Selector List tool to configure one at a time. The following instructions show how to use the Dialed Number/Script Selector List tool.

To set a default label for each dialed number/script selector:

Step 1   In the Configuration Manager's menu, select **Tools** > **List Tools** > **Dialed Number/Script Selector List**. The Dialed Number/Script Selector List window appears.

Step 2   Select the filters you want and click **Retrieve**. The enterprise names for the dialed number/script selectors retrieved are listed in the list box.

Step 3   Select the dialed number/script selector you want and click the **Attributes** tab.

Step 4   In the **Default** label field, select the enterprise name of a label from the selection list. This list includes all labels associated with the same routing client as the dialed number/script selector.

Step 5   After choosing the label, click **Save**.

Note   Within a routing script, you can explicitly invoke the default label for the current dialed number/script selector by using a Termination node.

Service Arrays

Service arrays are closely tied to network trunk groups. Typically, you use service arrays in cases where:

- You have similar peripheral services defined on multiple VRUs.

- The VRUs all share the same network group.

By grouping the services of multiple VRUs into a service array, you can send calls to a single target (a service array) and let the network deliver the call to any one of the peripheral services that make up the service array. For example, if several VRUs each support a Quotes service, you can define a Quotes service array for those services.

Configure Service Arrays

To configure service arrays, proceed along the following steps:

Step 1   In the Configuration Manager menu, select **Configure ICM** > **Targets** > **VRU Service Arrays** > **Service Array Explorer**. The Service Array Explorer window appears.

Step 2   In the Select filter data box, select the appropriate filters and click **Retrieve**. This enables the **Add Service array** button and displays a list of all currently defined service arrays associated with the selected PG.

Step 3   You can define a new service array or modify an existing one:

- To set up a new service array, click **Add Service array**.

Note	To create subsequent service arrays for the same PG, select the PG in the tree list window and then click **Add Service array**.

- To modify an existing service array, select it in the tree list window.

Step 4   In the **Service Array** tab for the selected service array, enter values for the following fields:

- **Name**. A unique name for the service array.

- **Description**. Additional information about the service array.

Step 5   Click the **Members** tab.

This tab lists the services that are current service array members of the selected PG.

- To add service members, click **Add**. Then in the Add Service Member window, select the name of a service from the list of available records and click **OK**. The Available records list contains all the services connected to the peripherals associated with the selected PG.

- To remove a service member, select it in the list and click **Remove**.

Step 6   Add or modify a route associated with the service array:

- To add a route, select the service array in the tree list box, and click **Add Route**. Or in the tree list box, select a route from the UNASSIGNED group and drag it to the service array. Then in the **Route** tab, enter or modify the values in the **Name**, **Description** and **Service name** fields.

- To modify the route, select it in the tree list box, and modify the Name and Description in the **Route** tab.

Step 7   Add or modify one or more peripheral targets for the route:

- To add a peripheral target, select the route and click **Add Peripheral target**. Or in the tree list box, select a peripheral target from the UNASSIGNED group and drag it to the route. Then in the Peripheral target tab, enter the following:

  - **DNIS**. The DNIS value for the peripheral target. The routing client delivers this value to the trunk group along with the call.

  - **Description**. Any additional information about the DNIS value.

  - **Network trunk group**. The group on which to deliver calls for the service array.

Step 8   To add or modify a label for the peripheral target:

- To add a label, select the peripheral target in the tree list box, and click **Add Label**. Or in the tree list box, select a label from the UNASSIGNED group and drag it to the peripheral target. Then in the Label tab, enter or modify the following:

  - **Routing client**. The enterprise name of the routing client that can receive this label.

  - **Label**. The literal string of characters to be returned to the routing client.

  - **Label type**. The type of label. The valid types depend on the type of the routing client.

  - **Customer**. The name of the customer.

  - **Description**. Any additional information about the label.

- To modify the label, select it in the tree list box, and modify the preceding fields in the **Route** tab.

Step 9 Click **Save** to save the changes to the database.

Step 10 Click **Close** to close the Service Array Explorer.

Related Topics

Application Wizard

The Application wizard provides an alternate method for defining labels, peripheral targets, and routes and associating them with services at a peripheral.

Before starting the Application wizard, you must have defined the routing client, peripheral, network trunk groups (and associated trunk groups), and services to be used. Within the Application wizard you can create dialed numbers, labels, peripheral targets, and routes.

Note The Application wizard does not allow you to associate routes and targets with skill groups or agents. It allows you to target only services.

Use the Application Wizard

To use the Application wizard, follow these steps:

Step 1 In the Configuration Manager menu, select **Tools** > **Wizards** > **Application Wizard**. The Routing window appears.

Step 2 Choose the type of application you want to set up (Pre-Routing or Post-Routing) and click **Next** to continue. The Routing Client and Dialed Number window appears, displaying information about all the configured routing clients of the type you selected.

Figure 25: Application Wizard—Routing Client and Dialed Number
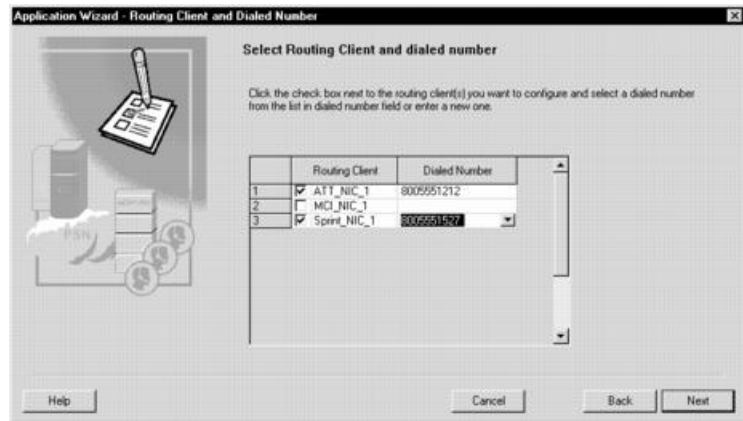
Step 3   Specify the following:

- **Routing Client**. Click to select one or more routing clients for the application. (A check mark to the left of the routing client indicates it is selected.)

- **Dialed Number**. Click the row and select a number from the drop-down list or enter a new dialed number value.

Note   You must specify a dialed number for each routing client selected.

Step 4   Click **Next**. The Peripheral window appears.

Figure 26: Application Wizard—Peripheral
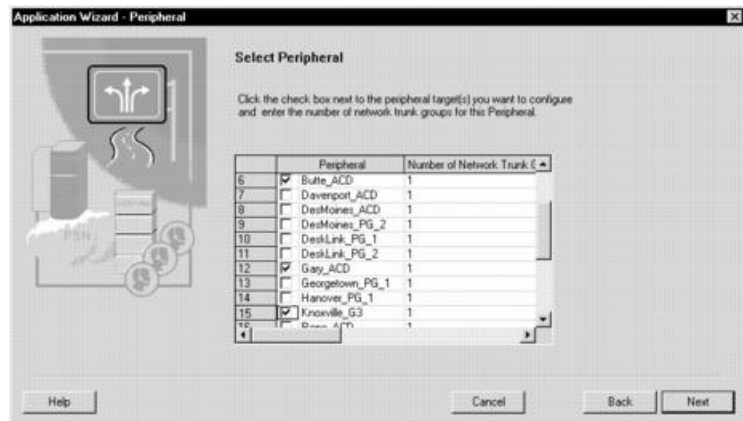
Step 5   Specify the following:

- **Peripheral**. Click to select one or more peripherals to which you want the application to deliver calls.

- **Number of Network Trunks**. The number of network trunk groups to be targeted at each peripheral.

Step 6   Click **Next**. The Network Trunk Group window appears, displaying the peripherals and routing clients you have previously selected.

Figure 27: Application Wizard—Network Trunk Group
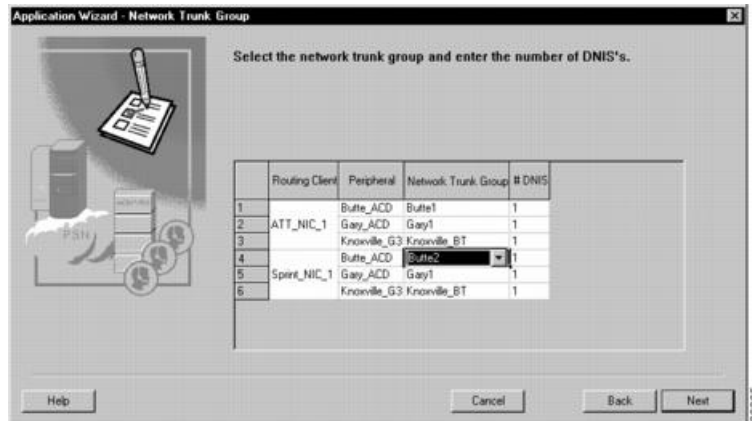
Step 7 For each row, specify the following:

  • **Network Trunk Group**. Click the row and select from the drop-down list.

  • **# DNIS**. The number of peripheral targets (DNIS values) to define for each network trunk group.

Step 8 Click **Next**. The Route DNIS and Label window appears.

Figure 28: Application Wizard—Service, Route, DNIS, and Label
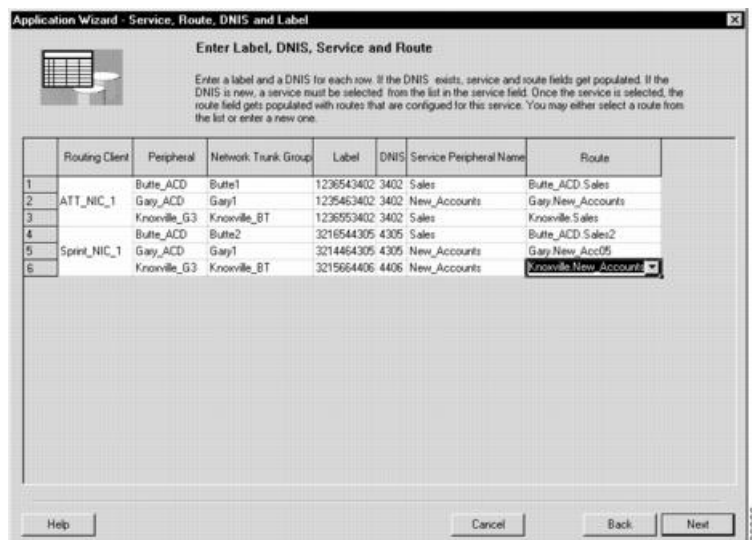
Step 9 For each network trunk group, specify the following:

  • **Label**. (This value does not have to be defined in the Unified ICM database.) The value the system software returns to the routing client to indicate the destination of the call.

  • **DNIS**. (This value does not have to be defined in the Unified ICM database.) The value the routing client sends to the network trunk group to indicate the destination of the call.

  • **Service Peripheral Name**. Click the row and select a predefined service at the peripheral from the drop-down list.

> • **Route**. Name of the route to be associated with the service. Select from the drop-down list or enter a new route name.

Step 10   Click **Next**. The Application Wizard displays a dialog listing the changes that will be made to the Unified ICM database.

Step 11   Click **Finish** to save the changes and exit the Application Wizard.

Translation Routes

A *translation route* is a special destination for a call that allows you to deliver other information along with the call. You do this by delivering the call first to the translation route. While the routing client is processing the call, the system software delivers the final destination for the call to the Peripheral Gateway along with any other necessary information. The peripheral then works with the PG to reroute the call to the ultimate target and ensure that the appropriate information is also delivered.

A single translation route can be used to send information to any number of different targets. However, because the PG must uniquely identify the call, you cannot perform translation routing on two calls to the same peripheral target simultaneously. To avoid this, you typically define a set of peripheral targets and routes, for each translation route.

Translation Route Wizard

You can define translation routes within the Configuration Manager. However, defining the correct associations with peripheral targets, labels, and routes is complicated. To automate much of the process, use the translation route wizard.

Note   You can also use the translation route wizard to view configuration or integrity reports on translation routes, update existing translation routes, and delete translation routes and their associated entities.

Create a Translation Route

To create a translation route, follow these steps:

Step 1   In the Configuration Manager, select **Tools** > **Wizards** > **Translation Route Wizard**. The Translation Route Wizard introductory dialog opens.

Step 2   Click **Next**. The Select Configuration Task dialog appears.

Step 3   To create a translation route, choose **Create New** and click **Next**. The Define translation route dialog appears.

Figure 29: Define Translation Route
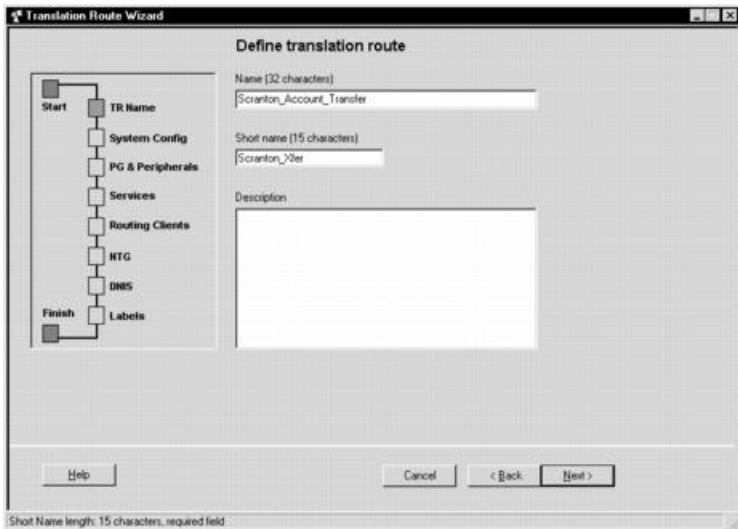
Note The graphic on the left of the dialog shows the entities you will be defining while using the translation route wizard.

Step 4 Enter a long and short name for the translation route and, optionally, a description — the short name is used in forming target names — and click **Next**. The Select configuration dialog appears.

Figure 30: Select Configuration
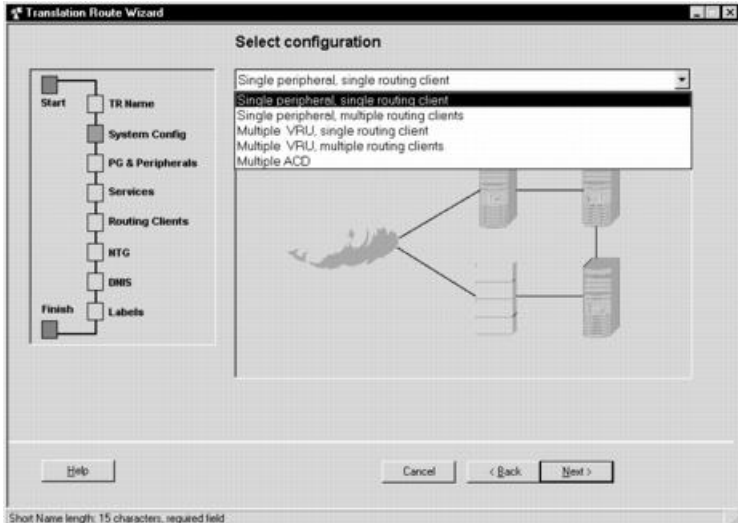
Step 5 Use the drop-down list to choose the configuration. The graphic changes to show the configuration you select.

Note A translation route can be associated with a single peripheral or with multiple VRUs associated with a single PG. It can handle calls originating from a single routing client or from multiple routing clients. (The Multiple ACD type is not currently supported.)

Step 6 Click **Next**. The Select peripheral gateway, peripherals, and services dialog appears.

Figure 31: Select Peripheral Gateway, Peripherals, and Services
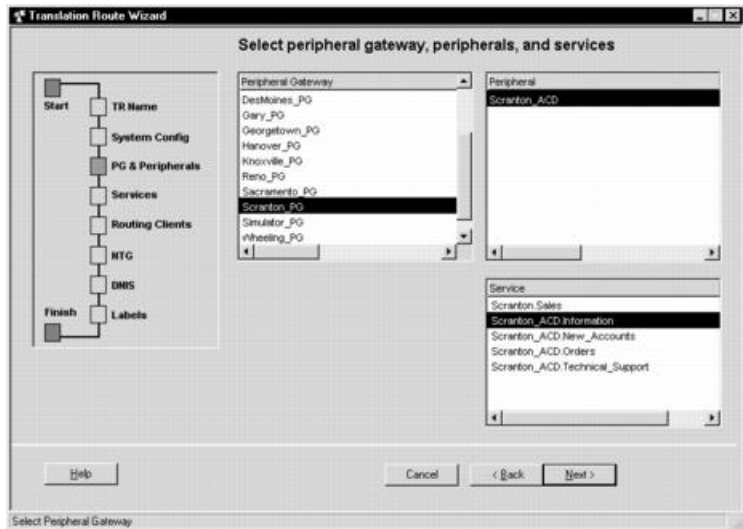
Step 7   Specify the following:

- **Peripheral gateway**. (scrolling list) The gateway target for the translation route.

- **Peripheral**. (scrolling list) The single peripheral or the peripheral to route calls to.

- **Service/Service array**. (scrolling list) If the translation route is associated with a single peripheral, then select the service associated with the translation route. If the translation route is associated with multiple VRUs, then select a service array.

Step 8   Click **Next**. The Select routing clients and dialed numbers appears.

Figure 32: Select Routing Clients and Dialed Numbers
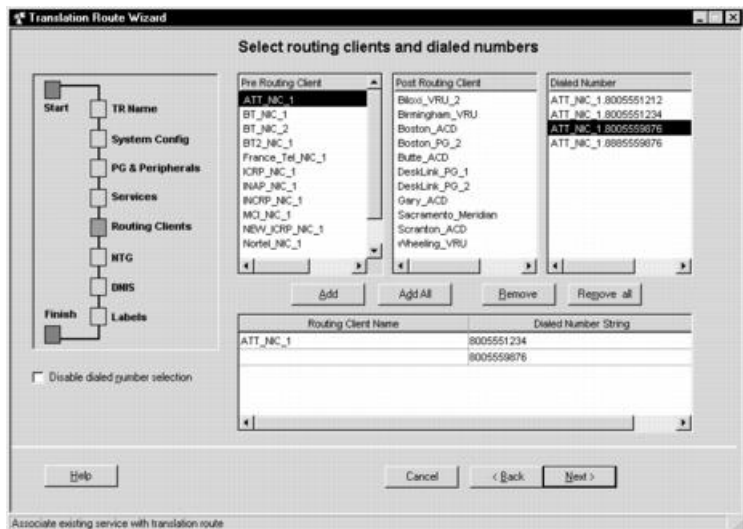
Use this dialog to specify the routing client or routing clients from which translation routed calls originate. For each routing client, you can also specify which specific dialed numbers are used for translation routed calls.

Step 9   Select a routing client from the Pre-Routing Client list or the Post-Routing Client list. The Dialed Number list updates to show the dialed numbers associated with the selected routing client.

Step 10   Select a dialed number you want to use with the translation route and click the **Add** button. The number appears in the list at the bottom of the dialog. The translation route wizard maps the translation route's labels to each of these dialed numbers.

> **Note**   Some routing clients do not require mappings of labels to specific dialed numbers. The dialed number list is automatically disabled for such routing clients. You need only select the routing client and click the **Add** button to add it to the list. You can also use the Disable Dialed Number Selection option to manually disable the dialed number list. The translation route wizard then does not create mappings of dialed numbers to labels for the routing client.

Step 11   Click **Next**. The Select network trunk groups for routing clients dialog appears.

Figure 33: Select Network Trunk Groups for Routing Clients
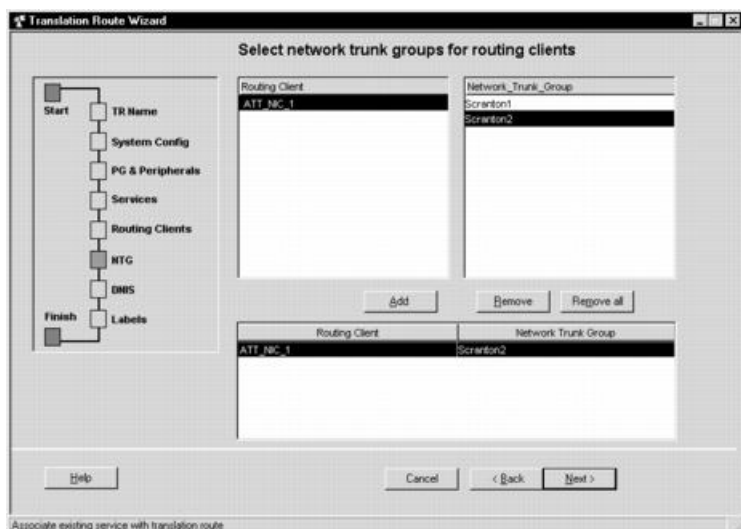
For each routing client you have selected, you must select at least one network trunk group to be used in peripheral targets associated with the translation route.

Step 12   Select a routing client, select a network trunk group value for it, and click **Add**. The network trunk group appears in the list at the bottom of the dialog.

Step 13   Click **Next**. The Configure DNIS dialog appears.

Figure 34: Configure DNIS
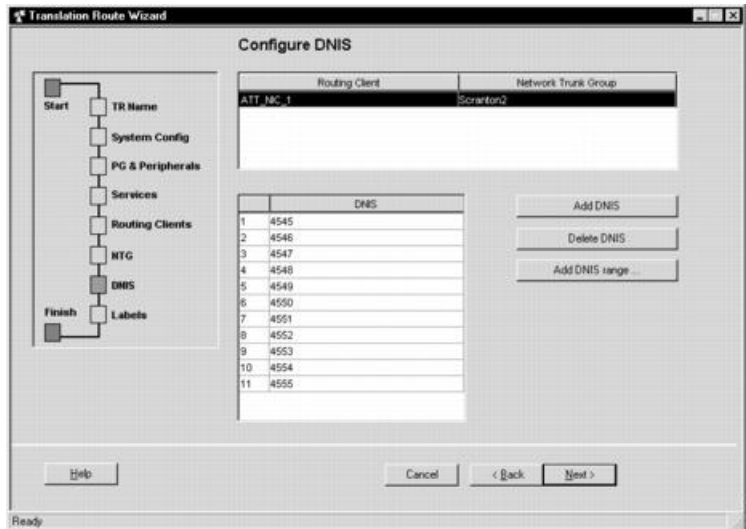
Use this dialog to specify the DNIS values to be used in peripheral targets associated with the translation route.

Step 14 Do one of the following:

- To enter a specific DNIS value, click **Add DNIS** and enter the value.

- To add a range of DNIS values, typically required by a translation route, click **Add DNIS Range**. A dialog prompts you to enter a starting and ending DNIS value. The translation route wizard automatically generates the DNIS values in the range.

Note DNIS values with leading zeroes, while valid, are different from DNIS values without leading zeroes. For example, 400, 0400, and 00400 are three different and unique DNIS values.

Step 15 Click **Next**. The Configure label dialog appears.

Figure 35: Configure Label
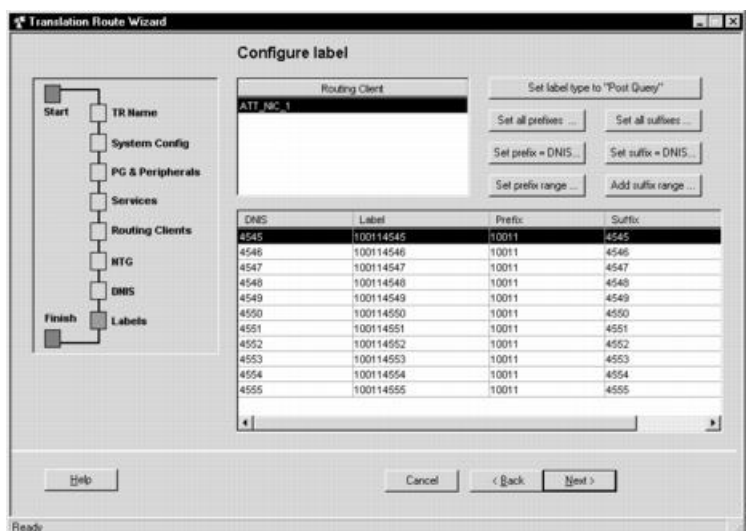
Use this dialog to define a label for each peripheral target. A label consists of a prefix and a suffix. Each DNIS value requires a unique label.

Step 16   Do one of the following:

> • Enter prefixes and suffixes individually.
>
> • Use the buttons in this dialog to set a range of values or base the prefix or suffix values on the DNIS values.

Step 17   Click **Next**. The Wizard complete dialog appears.

Figure 36: Wizard Complete Initial View
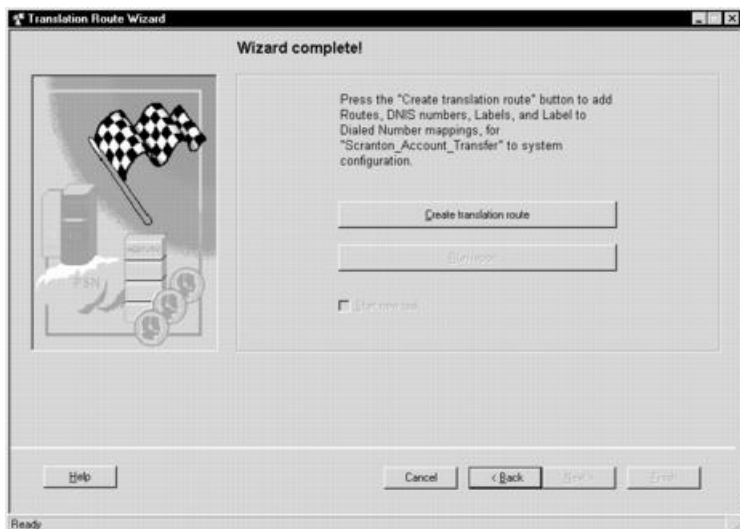
Step 18   Click **Create translation route** to create the translation route and its associated entities. First, the translation route wizard displays a success message and then the dialog appears as follows.

Figure 37: Wizard Complete Success View
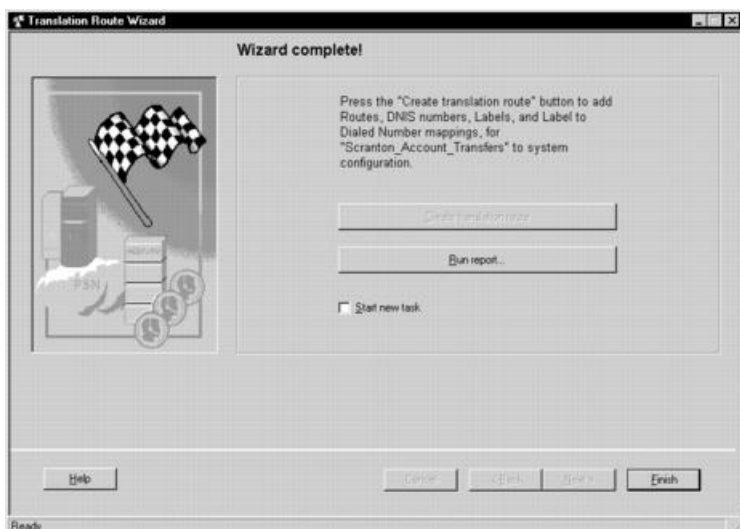
Step 19   Do one of the following:

- To see details about the translation route you just created, click **Run Report**.

- To return to the beginning of the translation route wizard and perform a new task, select **Start New Task** and click **Finish**.

- To exit the translation route wizard, click **Finish**.

Software Configuration for Integrated Applications

Software Configuration for Task Routing

This chapter provides configuration instructions for integrations with Cisco Enterprise Chat and Email only. You also can also use third-party multichannel applications with the Task Routing APIs.

For all 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

Software Requirements

☞

Important Do not install the system software and the integrated applications on the same machine.

Before you begin configuring the system software for the integrated applications, you must upgrade the system software.

For complete and current information on software requirements, see *Contact Center Enterprise Compatibility Matrix*.

Refer to the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* for specific upgrade and installation requirements.

Install the Application Interface

☞

| **Important** | You must install the application interface before beginning the Unified ICM configuration. |

If you want your Administration & Data Server to be the point of contact for the integrated applications configuration (to host the CMS Server), you need to perform this installation.

Refer to the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* for detailed information about the Administration & Data Server setup.

To install the application interface:

Step 1 Run the Web Setup tool (accessed from the Unified Contact Center Enterprise [Unified CCE] Tools folder).

Step 2 Select **Component Management** > **Administration & Data Servers**.

Step 3 Edit the Administration & Data Server on which the Distributor Service is running.

Step 4 On the Database and Options page, check **Configuration Management Service (CMS) Node**.

Step 5 Finish the installation process by completing the rest of the pages, then click **Finish** to save your edits.

After installing the application interface, you need to run the CMS Control tool on the installed Administration & Data Server to set up, from the Unified ICM side, the connections that allow the integrated applications to talk to that Administration & Data Server. You must also configure each application's end of the connection.

To improve performance, if no debugging is being performed using that console, keep the CMS node console minimized. If the console is not minimized, considerable CPU resources are tied up displaying numerous messages from the system I/O.

See Application Connections for more information about using the CMS Control tool to set up the connections between the system software and the integrated applications.

Pre-integration Configuration Verification

Verify the configuration by doing the following:

- Verify that all processes, including all PIMs and CTI servers, are active (that is, all processes start, duplexed routers load the configuration and synchronize, and all PIMs and CTI servers are active).

- Verify that the MSSQL server has started. Submit sample calls through all routing clients and all call types. Use the Call Tracer tool in the Script Editor to test router call handling functionality.

✎

| **Note** | This test must be finished both prior to the Unified ICM upgrade and after the Unified ICM upgrade. Address failures prior to integration. |

Software Configuration for Integration

Note

This chapter discusses integrations with Enterprise Chat and Email. You also can also use third-party multichannel applications. For all information about configuring Task Routing for third-party multichannel applications, see the *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

To configure Enterprise Chat and Email, you need to configure/install the following:

- Media routing domains (MRDs) for appropriate media classes within the system software
- Media routing peripheral gateways (MR PGs) and peripherals
- Voice Response Unit peripheral gateways (VRU PGs)
- ECC (Expanded Call Context) variables
- Application instances, and define them in the system software
- Agents (you can create agents either in the system software or in the applications)
- Connections to the CMS server using the Application tab of the CMS Control tool in the Administration Tools folder
- Configuration work on the integrated applications
- Skill group configuration using Script Editor
- Information to push to waiting Enterprise Chat and Email callers

The following sections describe each of the preceding actions, their configuration and installation instructions, and indicate the configuration tool you need for each configuration. Refer to a configuration tool's online help if you have any questions.

Note

Before using the configuration tools to perform each configuration process, if you have more than one Unified ICM instance you want to configure, open the Select Administration Instance tool in the Administration & Data Server or Administration Client and select the Unified ICM instance with which you want to work.

Media Routing Domains

To create and then assign a media routing domain (MRD) to a media class (physical media that the system software treats as a single concept), use the Configuration Manager's Media Routing Domain List tool.

The system software uses MRDs to organize how requests from different media are routed. An MRD is a collection of skill groups and services that are associated with a common communication medium. The system software uses an MRD to route a task to an agent who is associated with a skill group and a particular medium.

Before you can configure your application (for example, the Enterprise Chat and Email) to use the system software as a routing engine, MRDs must be established in the system software. These MRDs have unique

IDs across the enterprise. Then, on the application, you must enable those Unified ICM MRDs that you need to use.

☞

| Important | The MRD IDs *must* be created in the system software first, and then passed on to the person configuring the application to perform a successful configuration. In Enterprise Chat and Email you need only the MRD name; you do not need the MRD ID. |

A media class describes the type of requests you want to set up for routing on the system software.

Create the following media classes to enable the Enterprise Chat and Email feature:

The media class for voice already exists (Cisco_Voice).

Configure the Media Routing Domain

To configure the MRD:

Step 1 Start the Configuration Manager and select **Tools** > **List Tools** > **Media Routing Domain List**. The Media Routing Domain List window displays. Click the **Retrieve** button and then the **Add** button to display the Attributes tab.

Step 2 Enter the following information:

- Name. Enter the enterprise name of the MRD.

- Media Class. Use the drop-down list to select the media class for the integrated application.

- The Media routing domain ID is a required read-only field. (An ID number will be automatically created when you save your entry.)

Step 3 After entering the required fields, save the configuration and close the window.

| Note | Refer to the Configuration Manager's online help for detailed information about the Media Routing Domain List tool. |

Media Routing Peripheral Gateway

To create a media routing peripheral gateway (MR PG), use the Configuration Manager's Network VRU Explorer and the PG Explorer tools.

A media routing peripheral gateway is capable of routing media requests of different kinds (for example, email, Web callback, and so on). MR PGs support multiple media routing applications by placing multiple, independent peripheral interface managers (PIMs) on a PG platform. (There is a limit of 4 MR PIMs on a MR PG in Unified CCE Reference Design-compliant deployments.) A single MR PIM is required for each application server to be connected to the Unified ICM system. In addition to an MR PG, you also need at least one Agent PG, a legacy ACD PG, or a NonVoiceAgent PG.

For example, the diagram below provides an overview of the interfaces that need to be configured for Unified ICM integration with Enterprise Chat and Email.

Figure 38: Interfacing with Enterprise Chat and Email
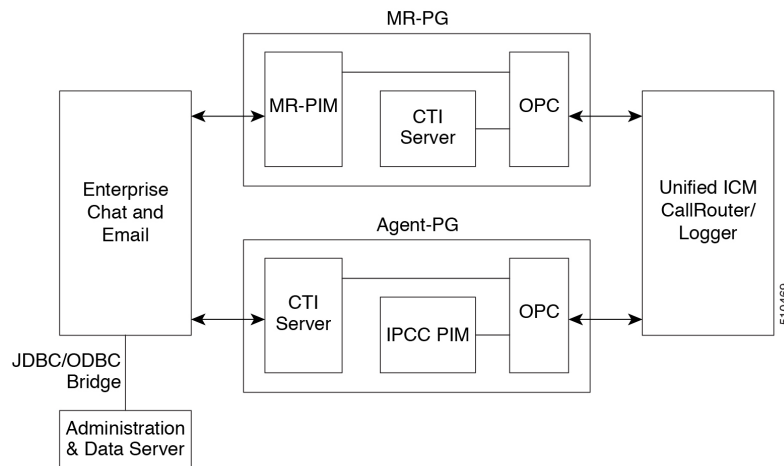
Configuring the MR PG

The MR PG interface provides routing instructions to the integrated applications, while the Agent PG configuration is used to report agent state and status to the system software.

> ✎
> **Note** No agents are configured on MR PGs. Agents are configured on NonVoice Agent PGs or other agent PGs.

The system software media routing mechanism leverages and takes advantage of the existing Unified ICM Network VRU operational infrastructures. To set up for media routing, you must configure a Network VRU in the Unified ICM configuration. This Network VRU configuration has no relationship with any actual Network VRU in your environment.

Configure MR PG

To configure the MR PG:

Step 1 Start the Configuration Manager. From the Configuration Manager menu, select **Configure ICM** > **Targets** > **Network VRU** > **Network VRU Explorer**. The Network VRU Explorer window displays.

Step 2 Click the **Retrieve** button and then click the **Add Network VRU** button. The Network VRU dialog displays.

Step 3 Do the following:

- Enter a name for the Network VRU (for example, Cust_MR_VRU).

- Select **Type 2** from Type drop-down list.

- Optionally, enter a description (that is, "Media Routing").

- Select *Default* in the **ECC Payload** drop down list.

- Save and close the window.

Step 4 From the Configuration Manager menu, select **Configure ICM** > **Peripherals** > **Peripheral** > **PG Explorer**. The PG Explorer window displays.

Step 5 Click **Retrieve** and then click the **Add PG button**. The Logical controller dialog displays.

Step 6 Do the following:

- Enter a name for the PG (for example, Cust_MR_PG1).

- Select **MediaRouting** as the Client Type.

Step 7 In the tree section of the window, expand the tree and click the **Add Peripheral** button. The Peripheral configuration dialog displays.

Step 8 Do the following:

- Select the Peripheral tab and check the **Enable Post Routing** box.

- Select the Advanced tab and select the previously created Network VRU from the drop-down list.

- On the Routing Client tab, enter a routing client name (for example, Cust_MR_PG1_1.RC) and set the default timeouts to **2000, 1000,** and **10**, respectively.

- Save the configuration. After you save the configuration, the system assigns a Logical Controller ID and a Physical Controller ID.

Note Make a note of these values because you will need to provide them when you install the MR PG.

Step 9 Close the window.

Setting Up the MR PG

Customer contact applications use the MediaRouting interface to request instructions from the system software when they receive a contact request from a customer using one of the mediums, such as email, web collaboration, or voice. When the system software receives a new task request from the application, Unified ICM runs a pre-defined Unified ICM script to determine how to handle the task.

After the Unified ICM script runs Unified ICM sends an instruction to the application to do one of the following:

- While the application is executing an application script that is stored on the application server, Unified ICM is looking for a best available agent that has the matching skill within the enterprise, and assigns this agent to this task.

- Handle the new task with a Unified ICM–determined best available agent that has the matching skill within the enterprise or a label the application uses to determine the best available agent for the task.

Note When choosing where to set up the MR PG, be aware that you can only set up two PGs per server.

Set Up MR PG

To set up the MR PG, follow these steps:

Step 1 Access the Peripheral Gateway Setup tool on the machine that you want to make an MR PG. Add the customer if you have not already done so.

Step 2 Click **Add** in the Instance Components section and choose **Peripheral Gateway** from the Unified ICM Component Selection window. The Peripheral Gateway Properties window displays.

Step 3 Do the following:

- Choose Production Mode.

  | **Note** | The Auto Start at System Startup option ensures that the PG can restart itself automatically if necessary. Set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied. |

- Specify whether the PG is part of a duplexed pair.

- In the ID field, choose the PG's device identifier as enabled in the CallRouter's Device Management Protocol (DMP) configuration dialog (part of setting up the CallRouter portion; enables the connection between the Router and the PG). Each logical PG must have a unique device assignment at the CallRouter. (If a PG is duplexed, both physical machines use the same device assignment.) To add another logical PG, you must enable another PG device for the CallRouter.

- If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplexed, select **Side A**.

- Use the Client Type Selection section of the window to select **MediaRouting** and click the **Add** button.

- Select the drive and language as appropriate and click the **Next** button.

Step 4 The Peripheral Gateway Component Properties window displays.

Enter the Logical Controller ID generated when you configured the PG with the PG Explorer in Step 8 of Configure MR PG, on page 159. Click the **Add** button and select **PIM 1** from the list.

Step 5 The MediaRouting Configuration box displays.

Step 6 Do the following:

- To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

- Enter the peripheral name in the Peripheral name field. In most cases, you must use the enterprise name from the associated Peripheral record.

  | **Note** | When creating peripheral names, use short descriptive names and keep the length to a minimum. |

- Enter the Peripheral ID from the Peripheral record.

- For Application Hostname (1), enter the host name or the IP address of the application server machine (Enterprise Chat and Email). If using the host name, the name must be in the host's file.

- For Application Connection Port (1), enter the port number on the application server machine that the PIM will use to communicate with the application.

- Leave Application Hostname (2) blank.

- Leave Application Connection Port (2) blank.

- For Heartbeat Interval (seconds), specify how often the PG will check its connection to the application server. (Use the default value) .

- For Reconnect Interval (seconds), specify how often the PG will try to re-establish a lost connection to the application server. Use the default value

- Check the **Enable Secure Connection** check box to enable secure connection for the PG.

- Click **OK**.

Step 7   From the Peripheral Gateway Component Properties window, click the **Next** button. The Device Management Protocol Properties window displays. Enter the appropriate settings and click the **Next** button.

Step 8   The Peripheral Gateway Network Interfaces window displays. Enter the appropriate settings and click the **Next**button.

Step 9   The Check Setup Information window displays. Verify the setup information and click the **Next**button. The system software sets up the PG.

Step 10   When the Setup Complete window displays, click the **Finish** button to exit from the setup program.

Configure and Install Unified Communications Manager PG

When agents and skill groups are created in the system software, they reside on a peripheral. A peripheral can be associated with a CUCM ACD for agents doing any work on the phone. If the agents on the peripheral will never be doing phone work, one or more NonVoice peripherals can be used.

Configure Unified Communications Manager PG

To configure the Unified Communications Manager PG, follow these steps:

Step 1   Start the Configuration Manager. From the Configuration Manager menu, select **Configure ICM** > **Peripherals** > **Peripheral** > **PG Explorer**. The PG Explorer window displays.

Step 2   Click **Retrieve** and then click the **Add PG** button. The Logical controller dialog displays.

Step 3   Do the following:

- Enter a name for the PG (for example, Cust_NVA_PG1).

- Select **CUCM** as the Client Type.

- Enter the address for the Primary CTI server and the Secondary CTI server in the following form:

  <IP address of the CTI server>:<Client Connection Port Number>

  that is, 192.168.1.101:42027

  This entry is necessary for Enterprise Chat and Email to gather CTI connection data.

Step 4   In the tree section of the window, expand the tree and click on the peripheral. The Peripheral configuration dialog displays.

Step 5   Do the following:

- Use the default name or change the name.

  Note   This name is used in composite names which are limited to a 32-character length, for example, an agent enterprise name. Therefore, keep the name short.

          • Because Unified CCE uses post routing, do not un-select the **Enable Post Routing** checkbox.

Step 6   Select the **Agent Distribution** tab and check the **Enable agent reporting** checkbox.

Step 7   Save the configuration. After you save the configuration, the system assigns a Logical Controller ID and a Physical Controller ID. Make a note of these values because you will need to provide them when you install the Unified Communications Manager PG.

Step 8   Close the window.

Install Unified Communications Manager PG

To install the Unified Communications Manager PG, follow these steps:

Step 1   Run the PG Setup tool (accessed from the Unified CCE Tools folder) on the machine that will be the Agent PG. Add the customer if you have not already done so.

Step 2   Click **Add** in the Instance Components section and select **Peripheral Gateway** from the ICM Component Selection window. The Peripheral Gateway Properties window displays.

Step 3   Do the following:

          • Choose **Production Mode**.

           Note   The **Auto Start at System Startup** option ensures that the PG can restart itself automatically if necessary. Set the Auto Start feature after installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes and/or databases are applied.

          • Specify whether the PG is part of a duplexed pair.

          • In the ID field, choose the PG's device identifier as enabled in the CallRouter's DMP configuration dialog. Each logical PG must have a unique device assignment at the CallRouter. (If a PG is duplexed, both physical machines use the same device assignment.) To add another logical PG, you must enable another PG device for the CallRouter.

          • If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplexed, select **Side A**.

          • Use the Client Type Selection section of the window to select the PG and click the **Add** button.

          • Select the drive and language as appropriate and click the **Next** button.

Step 4   The Peripheral Gateway Component Properties window displays.

Enter the Logical Controller ID generated when you configured the Agent PG with the PG Explorer. Click the **Add** button.

Step 5   Do the following:

          • To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

          • Enter the peripheral name in the Peripheral Name field. In most cases, you must use the enterprise name from the associated Peripheral record.

           Note   When creating peripheral names, use short descriptive names and keep the length to a minimum.

          • Enter the Peripheral ID from the Peripheral record.

• Specify the maximum length for an agent extension in the Agent Extension Length field.

• Enter the Unified CM host/IP that this peripheral will connect to in the **Service** field.

• Specify the User ID and User password created on the Unified Communications Manager (Unified CM) you are connecting to.

Step 6   Click **OK**.

Install CTI Server

You need to install a CTI Server for each Agent PG (the steps are basically the same as those for a Media Routing PG). Each PG uses a CTI Server to provide the interface between the integrated application and the system software.

Note

• It is important that when you install a CTI Server, you pick the Custom Gateway (CG) that corresponds to the Agent PG that you just installed. For example, if you just installed a MR PG as PG1 and an IPCC Agent PG as PG2, you must install the CTI Server for PG2 as CG2, not CG1.

• You do not need to install a CTI server on the Agent PG if one is already installed.

Install a CTI Server

To install a CTI Server, follow these steps:

Step 1   Run the PG Setup tool (accessed from the Unified CCE Tools folder) on the same machine as the Agent PG. Add the customer if you have not already done so.

Step 2   Click **Add** in the Instance Components section and select **CTI Server** from the ICM Component Selection window. The CTI Server Properties window displays.

Step 3   Do the following:

• Choose **Production Mode**.

Note   The **Auto Start at System Startup** option ensures that the PG can restart itself automatically if necessary. Set the Auto Start feature *after* installation is complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before hotfixes or databases are applied.

• Specify whether the CTI Server is part of a duplexed pair.

• In the ID field, specify the number of the CTI Server node (CG1 through CG80).

• In the ICM System ID field, enter the DMP device number of the Agent PG that you want associated with the CTI Server.

Note   The DMP device number is the check box you checked for the PG (that is, if you checked box 1, the device number is 1; box 2, the device number is 2; and so on).

• If the CTI Server is duplex, specify whether you are installing Side A or Side B. If the CTI Server is simplex, select Side **A**.

Step 4   The CTI Server Component Properties window displays.

Enter the appropriate Connection Port Number. For more information about setting up CTI Server Component Properties, see *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.

Check the **Enable Secure-Only Mode** check box to enable secure connection. When you check the **Enable Secure-Only Mode** check box, the **Non-Secured Connection Port** field is disabled.

> **Note**   Before you enable secured connection between the components, ensure to complete the security certificate management process.
>
> For more information, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
>
> .

Step 5   Click the **Next** button. The CTI Server Network Interface Properties window displays. Enter the appropriate interface information.

Step 6   Click the **Next** button to view the setup information window. If the information is correct, click the **Next** button and finish the installation.

Agents

You can create *persons* (records that contain personal information about an agent) and *agents* (person who handles customer contact) in the system software. Creating them in Unified ICMs does not make them immediately available to Unified ICM; the application must enable the agent.

> **Note**   When you create an Agent record, you can associate it with an existing Person record (clicking the **Select Person** button). 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.

Configuring an agent for multi-media means assigning that agent to at least two skill groups (one for each media). For example, the agent might handle both email and phones, chat and phones, or blended collaboration and email.

> **Note**   Use the integrated applications to assign an agent an application-specific skill group. Application-specific skill groups must be created and maintained in the application, not in the system software.

If you want to configure phone agents in the system software, you must first create Person records for them in the Configuration Manager's Person List tool.

Every agent is associated with a Person record. This is primarily a person's first and last name and login password. This record must exist before you can create an agent in the system software.

The purpose of the Person record is so that, in a multi-channel contact center, one person can be assigned as an agent on different peripherals since the system software defines an agent as belonging to only one peripheral.

> **Note** The preceding is also true for non-integrated Unified ICM systems.

The second step in creating an agent in the system software is to use the Configuration Manager's Agent Explorer tool to create the agent. When you do so, the agent is associated with a person.

Related Topics

Configure VRU Peripheral Gateway

Add VRU PG

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.

b) Check the **Auto start at system startup** check box.

c) Check the **Duplexed Peripheral Gateway** check box.

d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select **PG3**.

e) Select the appropriate side (**Side A** or **Side B**).

f) In the **Client Type Selection** pane, add **VRU** to the **Selected types**.

g) Click **Next**.

Add VRU PIM

> ⚠️ **Caution** Before you enable secured connection between the components, ensure to complete the security certificate management process.
>
> For more information, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **VRU**.

Step 3 Select the appropriate PIM from the **Available PIMS** list, then click **OK**.

Step 4   In the **Configuration** dialog box, check the **Enabled** check box.

Step 5   In the **Peripheral name** field, enter the CVP server name.

Step 6   In the **Peripheral ID** field, enter the logical controller ID of CVP server.

Step 7   In the **VRU Hostname** field, enter the hostname of the CVP server.

Step 8   In the **VRU Connect port** field, enter **5000**.

Step 9   In the **Reconnect interval (sec)** field, enter **10**.

Step 10   In the **Heartbeat interval (sec)** field, enter **5**.

Step 11   From the **DSCP** drop-down list, select **CS3(24)**.

Step 12   Check the **Enable Secured Connection** option to enable secured connection.

This establishes a secured connection between VRU PIM and CVP.

Step 13   Click **OK**.

Step 14   Repeat these steps to configure the remaining PIMs.

Application Instance

> **Important**   Application instances must be configured before you configure the multi-media application.

Use the Configuration Manager's Application Instance List tool to configure application instances, external to Unified ICM, to allow identification and access to the Configuration Management System (CMS). This enters an application ID and application key (password) that identifies the application. You need to enter the same information in the application.

> **Important**   Share the system software configuration information you noted during the previous procedures with the person performing the integrated applications configuration.

Configure an Application Instance

To configure the application instance, follow these steps:

Step 1   Start the Configuration Manager and select **Tools** > **List Tools** > **Application Instance List**. The Application Instance List window displays. Click the **Retrieve** button and then the **Add** button to display the Attributes tab.

Step 2   Enter the following information:

- Name. The enterprise name for the application instance.

- Application key. This is the password that the integrated application will use to be identified by the system software. The password is restricted to the 7-bit printable ASCII characters (any of the 94 characters with the numeric values from 32 to 126). Control characters (for example, "tab") and international characters are not allowed. This means passwords cannot be entered in a non-Western alphabet, such as Kanji.

- Application type. Available option is **<Other>**.

Note Select **<Other>** when using Enterprise Chat and Email.

• Permission Level. Select the permission level from the drop-down list.

Step 3 After entering the required fields, save the configuration and close the window.

Note Refer to the Configuration Manager's online help for detailed information about the Application Instance List tool.

Application Connections

In order for the application to communicate with the Unified ICM system for configuration purposes, a communications path between the system software and the application must be established.

You can define the communications path from the system software (CMS Server) to the application using the Application tab in the CMS Control tool, which resides on the Administration & Data Server in the icm\bin directory. A similar user interface on the application side is used to define the communications path from the application to the CMS Server.

Within the Application tab, the Application Connections table lists the current application connections, where you can add, edit, and delete application connections.

Note The Application link and Unified ICM Administration & Data Server link must match on the application side.

Configure CMS Server Connections

To configure CMS Server connections, follow these steps:

Step 1 From the **Start** menu, select **Run** and enter `C:\icm\bin\cmscontrol.exe` to access CMS Control.

Step 2 Select the Application tab.

Step 3 Click **Add**. The Application Connection Details dialog displays.

Step 4 Enter the application connection properties:

• **Administration & Data Server link**. The Unified ICM RMI Driver connection end point identity.

• **Administration & Data Server RMI Registry Port**. The port number for the Unified ICM Administration & Data Server RMI registry.

• **Application link**. The application RMI Driver connection end point identity.

• **Application RMI registry port**. The port number for the Application RMI registry.

• **Application host name**. The computer address where the application interface client resides. This name can be either an IP address or a name resolved by DNS or WINS.

Step 5 Click **OK** twice. This restarts the Cms_Jserver on the Administration & Data Server or Administration Client.

Note   When you click **OK** the second time to save your changes and close the CMS Control window, a message box may appear that states:

```
The CmsJServer process is about to be cycled. Click OK to proceed or
Cancel to quit.
```

Step 6   Click **OK** to proceed.

Note   Refer to the application-specific instructions for specific field information. Refer to the CMS Control tool's online help for specific information about the field descriptions.

Additional Configuration Setups

After configuring the system software, you need to perform the following configurations in the Enterprise Chat and Email application:

- After you configure the system software and Enterprise Chat and Email, more configuration must occur on the Cisco Media Blender server.

Note   Refer to the *Cisco Media Blender Administration Guide, Release 7.1*, for details.

- Unified ICM and ACD queues:

    If the Enterprise Chat and Email will be used to send requests submitted to it to the system software, you must create one Unified ICM queue. When a request is submitted to a Unified ICM queue, the system software routes the request to the Enterprise Chat and Email and agent most appropriate to handle the request.

    If you use legacy ACDs for blended collaboration you must create ACD queues on the Enterprise Chat and Email. ACD queues are used to communicate with Cisco Media Blender.

Refer to the Enterprise Chat and Email installation CD for documentation on performing these configurations.

Application Gateways

An application gateway is an optional Unified ICM feature that allows you to invoke an external application from within a script (using a Gateway node). You can pass data to the application and receive data in return, which you can then examine and use for routing decisions.

Before you can use these nodes in a script, you must first configure the gateways.

The application gateway requires connection information to communicate with the external application. You perform this task using the Configuration Manager.

Configuring Application Gateways

Configure a application gateway for an application you want to access, from within the scripts.

Configuration information includes data such as:

- Type of application the gateway interacts with-a non-Unified ICM application or an application on another Unified ICM system

- Form of connection the gateway uses-duplex or simplex

- Fault tolerance strategy for the gateway-described in the following table.

Table 22: Application Gateway Fault Tolerance Strategies

Fault Tolerance Strategy	Description
Duplicate Request	In ICM, both side A and B, connects to separate application gateway hosts. They send simultaneous requests. Each request is sent to both the sides of the gateway. The response that comes back first, is used by both the sides of A and B of ICM.
Alternate Request	In ICM, Side A and Side B connects to separate application gateway hosts. All requests are sent alternatively to A and B.
Hot Standby	Each router manages a connection to a different host. All requests are directed to the designated primary host. If either host (or connection) fails then all requests are directed to the backup host. This results in the loss of some requests on failures.
None	The application gateway is not duplexed.

Once you specify the configuration information, you can define the connection information for the gateway. For example, the network address of the port, through which the system software communicates with the application.

If your Central Controller is duplexed, you can define separate connection information for each side of the Central Controller. This allows each side to communicate with a local copy of the external application.

Note　For a remote Unified ICM, the address must be, as that specified for the INCRP NIC on the targeted system. Alternatively you may use the hostname in place of the address. There is a colon, an instance, or customer number. This value denotes which Unified ICM is accessed on the remote system, followed by another colon, and a letter. This letter indicates which side of the NAM system prefers to use this connection. The preference letters are as given:

- A - side A of the NAM prefers this connection

- B - side B of the NAM prefers this connection

- N - neither side of the NAM prefers this connection

- R - both sides of the NAM prefer this connection

An example of an address is,199.97.123.45:1:A.

Configure an Application Gateway

To configure an application gateway, follow these steps:

Step 1   Within the Configuration Manager, select **Tools** > **List Tools** > **Application Gateway List**. The Application Gateway List window appears.

Step 2   To enable Add, click **Retrieve**.

Step 3   Click **Add**. The Attributes property tab appears.

Step 4   Complete the Attributes property tab.

     Note   Select TLS in the **Encryption** field to secure the application gateway connection.

                 For additional information, see the online help.

Step 5   Click **Save** to create the application gateway.

           Next, configure the connection information for the application gateway.

Configure an Application Gateway Connection and Set Default Connection Parameters

           To configure an application gateway connection and set the default connection parameters, follow these steps:

Step 1   Within the Application Gateway List window, click **Retrieve** and select the desired Application Gateway.

Step 2   Complete the Connection property tabs.

     Note   For additional information refer to the online Help.

Step 3   Click **Save** to apply your changes.

Application Gateway: Fault Tolerance

           The Fault Tolerance field in the Application Gateway Table takes the following values:

- 0 = None,

    This is applicable for a simplex system with a single application gateway host.

- 1 = Duplicate Request

    Each router manages to connect to specific hosts. Each time a scripts initiates a request, both routers will ask their corresponding host. Both routers will accept the first response. This method is the most reliable, but has the added expense of requiring two interface hosts. Even if a host or a connection fails, all requests will be satisfied.

- 2 = Alternate Request

    Each router manages to connect to a specific hosts. The routers will take turns, sending half the requests to the host connected to side A, and the other half to the host connected to side B. If either hosts fails, the entire load will be directed to the surviving host. In such events some requests may be lost. This is due to the fact that there is a time gap between, the router figuring out a host failure and requesting routing of calls, within the deadline imposed by the network.

- 3 = Hot Standby

Each router connects to a different host. All requests are directed to the designated primary host. If the host (or connection) fails, all requests will be directed to the backup host. This option may also lose some requests on failures.

Skill Group Configuration with Script Editor

Universal Queue is the ability of the system software to route requests from voice, web, chat, and email channels from a single queue point directly to appropriately skilled agents. With Universal Queue, the system software treats requests from different media channels as a part of a single queue. Routing scripts send queued requests to agents based on business rules regardless of the media channel. For example, the routing of asynchronous channels such as email, and synchronous channels such as voice and chat, allows the system software to deliver the right contact to the right resource the first time, regardless of the channel it came through. The Queue to Agent node allows the targeting of a task (the work performed by an agent) to a script-specified agent.

The Queue to Agent node enables an agent to receive and operate on more than one task at a time. As a result, Universal Queue coordinates an agent's ability to work on multiple tasks on various media. It supports a simple control model where an agent's ability to handle an additional task depends on what task that agent is currently handling. For this level of control, the system software must have exclusive access to task assignment.

Note For Universal Queue to work, the agent must be assigned to skill groups that "ICM picks the agent", that is for which the system software does the routing.

The CallRouter can move tasks out of the present script execution and resubmit them into the system as a new invocation.

Routing Script Configuration

Due to the introduction of a media routing domain relationship, skill groups are medium specific. When an agent logs into the system software via a phone, or via Enterprise Chat and Email, the agent actually logs into an MRD. This automatically logs the agent into skill groups associated with that agent within that MRD. Then, as a task request for a specific MRD begins script execution, the call router considers only the skill groups associated with that specific MRD. This allows one script to be written to handle many MRDs.

When upgrading from an earlier version of the system software, setup upgrades all existing skill group definitions to the voice media routing domain. (MRDs for chat, email, or blended collaboration media classes must be added using the Configuration Manager's Media Routing Domain List tool.)

The associated MRD applies to most related objects. Service member objects map skill groups only to services of the same media routing domain.

Skill groups are created as follows:

- Skill groups for integrated email, chat, and blended collaboration are created, modified, and deleted using the system software.

- Skill groups for standalone email and chat are created, modified, and deleted using the application.

- Legacy ACD skill groups are configured on the ACD and on the system software.

Queue to Specific Agent

To assign a task to a specific agent, the CallRouter needs to do four things:

1. Pick an agent to receive the task.

2. Pick the MRD.

3. Pick a skill group from the list provided by the MRD selection.

4. Pick a route from the list provided by the skill group selection.

Using this style of queue to agent node, you select a specific agent at script design time.

In this case, where it is obvious who the agent is, the node property sheet displays a choice of routes for the peripheral that the agent is assigned to.

Note   Routes, agents, skill groups, and services are all associated with a peripheral.

Select Multiple Skill Groups and Routes by Agent

To select multiple skill groups and routes for different media by agent, follow these steps:

Step 1   In Script Editor, open the appropriate script in Edit mode.

Step 2   Select the **Queue to Agent** node.

Step 3   Right-click and select **Properties** to open the Queue to Agent Properties dialog.

Step 4   Ensure the Queue to Agent type is set to **Select using direct references**. If not:
   a) Select **Change** to open the Queue Agent Type dialog.
   b) Select **Explicit agent references**.
   c) Click **OK** to return to the Queue to Agent Properties dialog.

Step 5   Select an agent from the drop-down list in the **Agent** column. This enables the rest of the columns.

Step 6   In the **Domain** column, select the appropriate MRD.

Step 7   In the appropriate column, select a skill group and a Route valid for the selected agent and MRD.

You can specify the agent multiple times, each with a different MRD selection.

Queue to Agent Expression

In this mode of the queue to agent node, the agent identity is determined by the queue to agent expression at runtime.

Since the agent and MRD are not known until script execution time, you need some way of selecting an appropriate skill group and route. To accomplish this, pick an enterprise skill group. Ensure the enterprise skill group includes appropriate skill groups to cover all MRD cases for that agent. To select the route, use an enterprise route. Again, ensure that the enterprise route includes an appropriate collection of routes.

Select Multiple Skill Groups and Routes by Agent Expression

To select multiple skill groups and routes for different media by agent expression, follow these steps:

Step 1   In Script Editor, open the appropriate script in Edit mode.

Step 2   Select the Queue to Agent node.

Step 3   Right-click and select **Properties** to open the Queue to Agent Properties dialog.

Step 4   Ensure the Queue to Agent type is set to **Select using indirect references**. If not:

     a.   Select **Change** to open the Queue Agent Type dialog.

     b.   Select **Lookup agent references by expression**.

     c.   Click **OK** to return to the Queue to Agent Properties dialog.

Step 5   Enter an agent expression (typically, task.PreferredAgentID) into the **Agent Expression** column. **Formula Editor** is enabled when the **Agent Expression column** is selected.

Step 6   In the appropriate column, select an appropriate **Enterprise Skill Group** and an **Enterprise Route** valid for the entered agent expression.

You can specify the agent expression multiple times, each with a different enterprise skill group and enterprise route selection.

Refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* for more information about using Script Editor.

Information to Waiting Web Collaboration/Chat Users

On the Central Controller, you can create a Network VRU script list, which lists scripts set up to play to callers waiting for an agent.

With Unified ICM routing, you can display information, such as advertisements or informational URLs to a caller who is waiting to join a session with an agent. You can also populate these ads or URLs so that they display caller information originating in the callform. This way, you can personalize ads or messages seen by the waiting caller.

You can set up a VRU script list to point to URLs or text messages to display on the browsers of callers waiting for a Collaboration agent. Refer to the *Cisco Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html for detailed instructions on setting up this information.

Application Object Filter

The application object filter restricts access to application-specific data that is not owned by the running application. Application owned data includes skill groups, services, application paths, and routes. The application object filter is not applicable if there are no multimedia applications.

Access to the application object filter is restricted. You must use a super user password (case sensitive) to enable or disable the application object filter. This password is set as "password" during installation.

Generally enabled, the application object filter prevents administrators from creating or editing application-specific skill groups, services, application paths, or routes in the Configuration Manager. You would want this enabled since creating or editing the preceding application-specific data using Unified ICM could cause the application to become out of sync with Unified ICM. These items must be created and updated in the application requiring them, and not in the system software.

Disabling the application object filter allows administrators to create, delete, or edit application-specific skill groups, services, application paths, and routes from the Configuration Manager tools. You might want to do this if, for example, an application is dead (you cannot access the application) and application-specific data needs to be removed from the Unified ICM database. Another example of when you would want to disable the application object filter would be you need clean up after removing an application.

Disable Application Object Filter

To disable an application object filter, follow these steps:

Step 1   Click **Options** > **Application Object Filter**.

Step 2   Enter the Password when prompted.

Step 3   Select Disable.

Step 4   The tool opens and the status line indicates the application object filter is disabled.

- Open tools are not affected by the change in the application object filter status. The status change affects tools opened only after the application object filter status has been changed.

- Each time the Configuration Manager opens, the application object filter reverts to its default status – enabled.

Unified CCE User Integration for Unified Intelligence Center

User Authentication

Any user who is imported with the Unified CCE User Integration feature can log in. After they are integrated, Unified CCE supervisors can log into Unified Intelligence Center with their Active Directory user ID and password.

Unified CCE User Integration

The Unified CCE user integration feature imports supervisors and their teams from Unified ICM/Unified CCE from the Unified ICM Configuration Manager and database into Unified Intelligence Center.

Supervisors are automatically given Unified Intelligence Center user roles and can log in to Unified Intelligence Center to access collections and run reports for their agent teams.

Note
- You cannot run User Integration until you upload the license for Unified Intelligence Center.
- There are five tasks in the initial setup for Unified CCE User Integration. Some are performed in the Administration interface. Some are performed in the Reporting interface. As the System Application User has access to both interfaces, it is efficient for that user to set up Unified CCE User Integration.

The tasks are to:

- Enable Unified CCE User Integration in the Administration interface.

- Complete the configuration of the Unified CCE Historical Data Source in the Reporting Interface.

- Synchronize Users in the Administration Interface.

- Validate Collections of Agents and Agent Teams in the Reporting Interface.

- Set up a synchronization schedule in the Administration Interface.

Results of Unified CCE User Integration:

- Integrated Supervisors can sign in to Unified Intelligence Center Reporting (provided their Active Directory authentication is configured).

- Integrated Supervisors are added to the Unified Intelligence Center Reporting User List with the roles of Report Designer and Dashboard Designer.

- The Unified Intelligence Center Value Lists page is updated with *Agents* and *Agent Teams* collections.

- I

  ntegrated Supervisors can view their *Agents* and *Agent Teams* collections (**Unified IC Reporting** > **Value Lists** drawer).

- Integrated Supervisors are granted permissions only to the *Agents* and *Agent Teams* collections that they own.

After you configure the Unified CCE User Integration schedule, Unified Intelligence Center updates with every synchronization the changes to supervisors and their teams.

Enable Unified CCE User Integration

Users who you configure as agent supervisors in Unified CCE Configuration manager and save in the Unified ICM database can be integrated into Unified Intelligence Center.

To enable Unified CCE user integration:

Step 1   Log in to CUIC OAMP.

Step 2   From the Administration application, click **Cluster Configuration** > **UCCE User Integration**.

Step 3   Click **Enable UCCE User Integration**.

Step 4   Optionally, set the schedule for time of day and days of the week when you want to user integration. (You can return to this page and set the schedule later, after you configure the Unified CCE Historical Data Source.)

Step 5   Click **Save**.

Step 6   *Do not click* **Synchronize Now**. (You must first configure the Unified CCE Historical data source.)

What to do next

Set up security for remote database.

Set Up User Roles, Permissions, and Groups

Unified Intelligence Center users who correspond to Unified CCE supervisors are created by Unified CCE User Integration and have the Report Designer and Dashboard Designer roles.

Data Collections

When you implement the Unified CCE User Integration feature, the Unified Intelligence Center Value List page is updated with collection values for Agent and Agent Teams value lists.

Collections

When you use the Unified CCE User Synchronization feature, the Agent and Agent Team Value Lists are populated with collections for all agents and agent teams that were imported for all Unified ICM supervisors

All Collections Panel

The **All Collections** panel displays when you select a Value List and click **Collections**. Doing this extends the Value List page so that it displays any All Collections for that Value List. The collections are presented in two panels: Collection Name and Collection Type.

> **Note** Collections imported by Unified CCE User Integration are called System collections. You cannot delete or modify these collections as they are pulled from Unified ICM configuration data.

Actions for Collections

- **Create**—click this to open the Create/Edit Collection Page.

- **Edit**—select a collection name and click this to open the Create/Edit Collection Page. This button is disabled for System collections imported by Unified CCE User Integration.

- **Delete**—select a collection and click this to confirm the deletion. If you delete a Collection, it does not appear as a filtering option for a report. This button is disabled for System collections imported by UCCE User Integration.

- **Populate Values**—This button is enabled only for Collections of Type Identifier and Wildcard. This button is disabled for System collections imported by Unified CCE User Integration.

- **Show Values**—select a collection and click this to see all the values in that collection; for example, to see all agents in an Agent Team collection.

Collections from Unified CCE User Integration

If you implement Unified CCE User Integration, the stock Agent and Agent Teams Value Lists are updated with collections of agents and agent teams that are automatically created from the synchronization.

The collections that are imported from the synchronization are identified as *system* collections and do not affect any *custom* collections you might have created for the Agent or Agent Teams Value Lists.

Supervisors who are imported with Unified CCE User Integration become Unified Intelligence Center Dashboard Designer and Report Designer Users. As Report Designer Users, they have execute access for the Value List drawer and for the Agent and Agent Team collections for which they are supervisors.

All imported Supervisors have execute permission for *all* Value Lists. However, for the imported team collections under the Agents and Agent Teams Value Lists, only the Supervisors for *those teams* have execute permission to those Collections.

The *system* collections for Agent and Agent Team that are created by Unified CCE User Integration are distinguished from the *custom* Agent and Agent Team collections in that you cannot edit, delete, or modify the system collections.

User List Page

The first time the Super User administrator who installed the system opens this page, the list is populated with his or her name and with the names of all Supervisors who integrated from Unified CCE (if the initial User Integration has been run).

Unified CCE User Integration is configured and scheduled in the Unified Intelligence Center Operations Console (Cluster Configuration > ICM User Integration). It is documented in the online help for the Operations Console.

Configuring Variables

Expanded Call Context Variables

Expanded Call Context (ECC) variables are variables that you define and enable in the Configuration Manager to store values for a call. You can specify the variable name and data type. The name must begin with the string "user." ECC variables are in addition to the variables the system software defines for each call (PeripheralVariable1 through PeripheralVariable10, CallerEnteredDigits, CallingLineID, and so on).

An ECC variable name can be up to 33 bytes long (1–32 usable characters). Use the following naming convention when creating an ECC variable:

user.<CompanyName>.<VariableDescription>

In this syntax:

- **<CompanyName>** is the name of your company.

- **<VariableDescription>** is a descriptive tag for the variable.

For example:

```
user.Cisco.AcctNum
```

Using this naming convention prevents naming conflicts with any third-party applications that interface with the system software.

Note For a large corporation, you can break **<VariableDescription>** down to include the Business Unit, Division, or other organizational entities.

ECC variables follow these size rules:

- An ECC variable can be either a scalar variable or an array element, each with a maximum length of 210 bytes.

Note   Array types are not supported for an agent request.

- The maximum number of elements in an array is 255.

- The maximum buffer size for each scalar variable = 5 + the maximum variable length. The 5 bytes includes 4 bytes to tag the variable and 1 byte for the null terminator.

- The maximum buffer size for each array = 5 + (1 + the maximum length of an array element) * (the maximum elements in the array). There is a null terminator for each element, and a null terminator for the array as a whole.

- You pass ECC variables in an ECC payload which has a 2000-byte limit. The total sum of all the maximum buffer sizes for each variable and each array in one ECC payload cannot exceed 2000 bytes.

  For example, if you intended to use the following:

  - A scalar ECC variable with a maximum length of 100 bytes

  - A scalar ECC variable with a maximum length of 80 bytes

  - An ECC array with a maximum of 9 elements with each element having a maximum length of 200 bytes

  Totaled the buffer size is: (5+100) + (5+80) + (5 + (1+200)*9) = 2004. Because this size is too large, you must change the length of one of the scalar ECC variables or the length of the array ECC variables.

ECC Payloads

You can define as many ECC variables as necessary. But, you can only pass 2000 bytes of ECC variables on a specific interface at any one time. To aid you in organizing ECC variables for specific purposes, the solution has *ECC payloads*.

An ECC payload is a defined set of ECC variables with a maximum size of 2000 bytes. You can create ECC payloads to suit the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads. The particular ECC variables in a given ECC payload are called its *members*.

Note   For ECC payloads to a CTI client, the size limit is 2000 bytes plus an extra 500 bytes for the ECC variable names. Unlike other interfaces, the CTI message includes ECC variable names.

In certain cases, mainly when using APIs, you might create an ECC payload that exceeds the CTI Server message size limit. If you use such an ECC payload in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, "CTI Server was unable to forward ECC variables due to an overflow condition."

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. TCDs and RCDs record the ID of the ECC payload that had scope during that leg of the call. The *Call.ECCPayloadID* variable contains the ID of the ECC payload which currently has scope.

In solutions that only use the default ECC payload, the system does not create an ECC variable that exceeds the 2000-byte limit for an ECC payload or the 2500-byte CTI Message Size limit. The system does this because it automatically adds all ECC variables to the default ECC payload if that is the only ECC payload.

If you create another ECC payload, the system no longer checks the 2000-byte limit when creating ECC variables. The system creates the ECC variables without assigning them to an ECC payload. Assign the new ECC variable to an appropriate ECC payload yourself through the ECC Payload Tool.

You can create and modify ECC payloads in the **Configuration Manager** > **List Tools** > **Expanded Call Variable Payload List** tool.

Default ECC Payload

The solution includes an ECC payload named "Default" for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

If your solution only has the Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Note   You cannot delete the Default payload. But, you can change its members.

Important   During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the **CTI Message Size** counter in the **Expanded Call Variable Payload List** tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

In a fresh install, the Default payload includes the predefined system ECC variables. In an upgrade, the Default payload's contents depend on whether the starting release supports ECC payloads:

- **ECC payloads not supported**—During the upgrade, a script adds your existing ECC variables to the Default payload.

- **ECC payloads are supported**—The upgrade brings forward the existing definition of your Default payload.

Note   If your solution includes PGs from a previous release that does not support ECC payloads, the Router always sends the Default payload to those PGs. Those PGs can properly handle the Default payload.

ECC Payload Node

The **ECC Payload** node is available from the **General** tab on the **Object Palette**:

Figure 39: Payload icon

Use this node to change the ECC payload that has scope for the following part of your script. Once you select an ECC payload, it has scope for all non-VRU operations until changed. You can select the ECC payload either statically or dynamically by the payload's EnterpriseName or ID.

ECC Payload Use by Interface

This table summarizes the use of ECC payloads in various operations:

Condition	ECC Payload That Is Used
Routing to VRU	Default payload If an ECC payload is specified in the configuration of that VRU, it overrides the Default payload.
Routing to Application Gateway	ECC payload that currently has scope in the script
Routing to Agent PG (including the Unified CM PG and Avaya PG)	ECC payload that currently has scope in the script
Routing to Media Routing PG	Default payload If an ECC payload is specified in the configuration of the VRU for that MR PG, it overrides the Default payload.
Routing to pre-12.0 PG	Always Default payload
Routing to System PG (Agent or VRU)	Always Default payload
Routing to Avaya Aura Symposium PG	Always Default payload
Routing to Aspect PG	Always Default payload
Contact Director to target Unified CCE	ECC payload that currently has scope in the script
Routing to INCRP NIC	ECC payload that currently has scope in the script
Pre-route to Gateway PG on Parent in Parent/Child	Always Default payload

Note If you do not create another ECC payload, the solution uses the Default payload for everything.

ECC Variables for Blended Collaboration or Voice MRDs with Collaboration

ECC variables must be configured in Configuration Manager's Expanded Call Variable List tool (for each integrated application) to route requests using the voice Media Routing Domain.

For Cisco Blended Collaboration or Voice MRDs with Collaboration, the ECC variables are:

 • user.cisco.cmb

 • user.cisco.cmb.callclass

 • user.ece.activity.id

 • user.ece.customer.name

☞

Important   While their default size is 40 characters, use the Expanded Call Variable List tool in the Configuration Manager to limit the user.cisco.cmb variable to 8 bytes and the user.cisco.cmb.callclass variable to 10 bytes to prevent ECC space limitation issues.

Expanded Call Context Variable Configuration

Expanded call context variable configuration consists of two steps:

 • Enable ECC variables

 • Define ECC variables

For Web Callback and Delayed Callback to work properly, an ECC variable (also known as a named variable) must be defined. The Cisco CTI driver supports the use of ECC variables in addition to the standard call variables associated with a call. Before an ECC variable can be used, it must be defined in the Unified ICM ECC variable database table.

✎

Note   For more information, refer to the *Database Schema Handbook for Cisco Unified Contact Center Enterprise*.

Enable ECC Variables

Step 1   Within the Configuration Manager, double-click **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

Step 2   Select the **Expanded call context enabled** check box.

For additional information, refer to the online Help.

Step 3   Click **Save** to apply your changes.

Define ECC Variables

Step 1   Within the Configuration Manager, double-click **Tools** > **List Tools** > **Expanded Call Variable List**.

The **Expanded Call Variable List** window appears.

Step 2 Click **Retrieve** to enable adding ECC variables.

Step 3 Click **Add**.

The **Attributes** property tab appears.

Step 4 Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

Step 5 Click **Save** to apply your changes.

What to do next

If you change the configuration of any ECC variable with the **Expanded Call Variable List** tool, restart the Unified CVP Call Server or VRU PIM to force a renegotiation of the ECC variables.

Before you can use the new ECC variable, you must add it to an ECC payload.

Note   If your solution only has a Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Define ECC Payloads

You can create and modify ECC payloads in the **Expanded Call Variable Payload List** tool.

Note   The tool checks that the ECC payload does not exceed the 2000-byte limit only when you save your changes. The counters on the **Members** tab only show what the current size is with all the selected members. They are only informational and do not enforce the limit. The limit is enforced when you attempt to save the changes.

To define an ECC payload, you create the ECC payload and then add its members.

Step 1 In the Configuration Manager, open **Tools** > **List Tools** > **Expanded Call Variable Payload List**.

The **ECC Payload List** window appears.

Step 2 Click **Retrieve** to enable adding ECC payloads.

Step 3 Click **Add**.

The **Attributes** property tab appears.

Step 4 Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

Step 5 On the **Members** tab, click **Add**.

A dialog box listing all the existing ECC variables appears.

Step 6 Select the members for your ECC payload and click **OK**.

Watch that the **ECC Variable Size** counter does not exceed 2000 bytes. For ECC payloads that go to CTI clients, watch that the **CTI Message Size** counter does not exceed 2500 bytes.

Step 7   Click **Save** to apply your changes.

Validate ECC Variable Size for CTI Server

Before configuring ECC variables, validate the total size of the ECC variables against the following rules and limits:

- Because the total size of the buffer used to store the variables in CTI Server internally is 2500 bytes, the total sum of all the maximum buffer sizes for each scalar variable and arrays must be no greater than 2500.

- The maximum buffer size for each scalar variable = 4 + length of the ECC name + the maximum length of the variable where the 4 bytes includes a 1 byte tag, 1 byte to define the length, and 2 terminating NULL characters.

- The maximum buffer size for each array = (5 + length of the ECC name + the maximum length of array element) * (the maximum number of elements in the array) where the 5 bytes includes a 1 byte tag, 1 byte to define the length, 1 byte for the array index, and 2 terminating NULL characters.

- For example, if you intend to use one scalar ECC variable with a maximum length of 100 bytes named *user.var*, one scalar ECC variable with a maximum length of 80 bytes named *user.vartwo*, and an ECC array named *user.varthree* with a maximum of 9 elements with each element having a maximum length of 200 bytes, the buffer size would be:

  (4+8+100) + (4+11+80) + ((5 + 13 + 200)*9)) = 2169

  where 8 is the length of *user.var*, 11 is the length of *user.vartwo* and 13 is the length of *user.varthree*.

User Variables

You can also create global user variables; for example, you can create a user variable called usertemp to serve as a temporary storage area for a string value used by an If node.

After you have defined a user variable, you can then use the Script Editor Formula Editor to access the variable and reference it in expressions, just as you would with a "built-in" variable.

Each user variable must:

- Have a name that begins with **user**.

  Note   This name cannot contain the dot/period (.) character.

- Be associated with an object type, for example, Service. (This enables the system software to maintain an instance of that variable for each object of that type in the system.)

- Be checked as persistent. A persistent variable maintians its value between script invocations. This allows you to set the variable in one script and reference later in another script.

Note Because these variables may be persisted, do not use User Variables to store sensitive information belonging to the customer or company. Using these variables to store confidential information could lead to violation of security standards, such as PCI, the Common Criteria, HIPAA, or FIPS 140-2.

A user variable can store a value up to 40 characters long.

Define User Variables

Step 1 Within the Configuration Manager, select **Tools** > **List Tools** > **User Variable List**.

The User Variable List window appears.

Step 2 In the User Variable List window, click **Retrieve** to enable Add.

Step 3 Click **Add**.

The Attributes property tab appears.

Step 4 Complete the Attributes property tab.

Note The **Variable name**, **Object type**, and **Data type** fields are required. All other fields are optional. For additional information refer to the online Help.

Step 5 Click **Save** to apply your changes.

Network IVRs/VRUs

VRU Configuration Tools

Network VRU Explorer Tool

This tool allows a network applications manager (NAM) to view, edit, or define network VRUs, labels, and their associations. The system software can send a customer call to a network VRU.

Note The Network VRU Explorer is not available on a limited (single Instance) Administration & Data Server.

To begin, select the filters you want and click **Retrieve**.

The changes you make in the Network VRU Explorer window are not applied to the database until you click **Save**.

Network VRU Script List Tool

This tool allows you to list the network VRU scripts currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones.

Network VRU scripts are created by VRU engineers for VRUs. This List tool defines these previously created scripts for the system software so it can interact with the scripts.

Note The Network VRU Script List tool is not available on a Limited (single Instance) Administration & Data Server.

VRU Currency List Tool

This tool allows you to list the VRU currencies currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones.

VRU Defaults List Tool

This tool allows you to list VRU defaults currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones.

VRU Locale List Tool

This tool allows you to list the VRU locales currently defined in the Unified ICM database, to define new ones, and to view, edit, or delete the records of existing ones.

Configuring Network VRUs and VRU Scripts

Before you start configuring a Network VRU, you must know its type. The VRU type determines what routing script nodes the system software needs to use to communicate with the VRU. For example, when interacting with a Type 3 VRU, the system software runs a routing script containing a Send to VRU node to successfully process a call.

The following table lists the VRU types that are currently available.

Table 23: Voice Response Unit (VRU) Types

Type	Description	Nodes to use with this type
1	Normal label type and a correlation ID.	
2	Normal label type and a DNIS.	Required: Translation Route to VRU. Optional: Queue and Run VRU Script.
3	Resource label type and a correlation ID. The routing client can automatically take back the call from the VRU when the system software returns a destination label. **Note** Use this type (rather than Type 7) when the routing client can automatically take back the call from the VRU when the system software returns a destination.	Optional: Send to VRU, Queue, and Run VRU Script.

Type	Description	Nodes to use with this type
5	Resource label type and either a correlation ID or a DNIS. **Note** Use this type (rather than a Type 3 or Type 7) when the routing client itself takes care of mapping the call to requests from the system software.	Required: Send to VRU. Optional: Queue and Run VRU Script.
6	No label, no correlation ID, and no DNIS (call is already at the VRU).	The VRU for this type is programmed so that it can recognize such a request based on the call qualifiers, so you can assume the call is already at the VRU. Optional: Queue and Run VRU Script.
7	Similar to Type 3, but the system software automatically instructs the VRU to release the call when it sends a destination label to the routing client. **Note** Use this type (instead of Type 3) when the routing client cannot take back the call from the VRU. That is, the system software automatically instructs the VRU to release when it sends a route response to the routing client; for example, CWC Network VRUs.	Optional: Send to VRU, Queue, and Run VRU Script.
8	Similar to Type 2, but a Type 8 VRU is used when the NAM has a routing client that controls the call to the VRU.	Required: Translation Route to VRU. Optional: Queue and Run VRU Script.
9	Simplifies configuration requirements in Unified Customer Voice Portal(Unified CVP) Comprehensive Model deployments. Use this type for calls that originate from a TDM VRU or ACD and need to be transferred to Unified CVP for self service or queuing, and for calls that originate from an Unified CCE or Unified CM, and need to be transferred to Unified CVP for self service or queuing.	Required: All Unified CVP micro-application scripts

Type	Description	Nodes to use with this type
10	Type 10 was designed to simplify the configuration requirements in Unified CVP Comprehensive Model deployments. There is a Handoff of routing client responsibilities to the Unified CVP switch leg. There is an automatic transfer to the Unified CVP VRU leg, resulting in a second transfer in the case of calls originated by the VRU, ACD, or Cisco Unified Communications Manager. For calls originated by Cisco Unified Communications Manager, the Correlation ID transfer mechanism is used. The Correlation ID is automatically added to the end of the transfer label defined in the Type 10 Network VRU configuration. The final transfer to the Unified CVP VRU leg is similar to a Type 7 transfer, in that a RELEASE message is sent to the VRU prior to any transfer.	

It is not really necessary to include a Send to VRU node in a script referring to a Type 3 or Type 7 VRU, as the Queue and Run VRU Script nodes automatically send the call to the VRU if it is not already there when they run. However, including it in such scripts can act as a visual aid if you ever need to troubleshoot the script.

For Types 3 and 7 you must use the System Information dialog to configure a range of correlation IDs. These IDs allow the system software to match calls arriving at the VRU with calls sent there by the system software. (For Types 2 and 8, the system software uses the DNIS values associated with the translation route to match up the calls. For Type 6, no matching is required since the call is already at the VRU.)

VRU Port Map Data Descriptions

A VRU port map associates a VRU trunk with an ACD trunk or an ADC port. In cases where ACD and VRU PIMs are controlled by the same PG, each row in the VRU_Port_Map table specifies how a VRU port maps to an ACD trunk or port.

You can add or modify the VRU Port Map in bulk using the VRU Port Map Bulk Inster or Bulk Edit tools in **Configuration Manager** > **Bulk Configuration** > **.**

Table 24: VRU Port Map Data Descriptions

Field	Description
State	(display only) A symbol indicating whether a row's record is changed, not changed, to be deleted, or to be inserted.
VRU Trunk Group (required)	Indicates the VRU Trunk Group associated with this port map.

Field	Description
VRU Trunk Number (required)	Indicates the VRU Trunk associated with this port map.
Mapping Type (required)	Type of mapping associated with this port map. There are two mapping types: • VRU Trunk, which maps to ACD Trunk • VRU Port, which maps to ACD Port This selection determines which two of the next four fields are editable.
ACD Trunk Group	(optional) Indicates the ACD Trunk Group associated with this port map.
ACD Trunk Number	(optional) Indicates the ACD Trunk associated with this port map.
ACD Peripheral	(optional) Indicates the ACD Peripheral associated with this port map.
ACD Port	(optional) Indicates the ACD Port associated with this port map.

Network VRU Script Data Descriptions

Each row identifies a script used by a network VRU to handle a call. A VRU script is managed by the VRU itself. It is not stored in the Unified ICM database or directly managed by the system software. The system software can only direct the VRU to run the script.

Note The Network VRU Script Bulk tool is not available on a Limited (single Instance) Administration & Data Server.

Table 25: Network VRU Script Data Descriptions

Field	Description
State	(display only) A symbol indicating whether a row's record is changed, not changed, to be deleted, or to be inserted.
Network Target (required)	Identifies the network VRU associated with the script.
VRU Script Name (required)	The name of the script as known at the VRU.
Network VRU Script (required)	The enterprise name of the script.
Customer	(optional) The name of the customer associated with the script.
Interruptible (required)	Indicates whether the system software can interrupt the script (for example, if a routing target becomes available): Yes or No.
Overridable (required)	Indicates whether the script can override its own Interruptible attribute: Yes or No.

Field	Description
Configuration Parameter	(optional) A parameter string that is sent to the VRU to initialize the script.
Timeout	(optional) The number of seconds the system software will wait for a response after invoking the script. If the system software does not receive a response from the routing client within this time, it assumes the VRU script has failed.
Description	(optional) Additional information about the script.

Network VRUs

Define each logical VRU in the database before continuing to the following sections.

Create Network VRU Target

Step 1 Within the Configuration Manager, select **Tools** > **Explorer Tools** > **Network VRU Explorer**.

The Network VRU Explorer window appears.

Step 2 In the Network VRU Explorer window, click **Retrieve** to enable **Add Network VRU** .

Step 3 Click **Add Network VRU**.

The Network VRU property tab appears.

Step 4 Complete the Network VRU property tab.

The Name and Type fields are required. All other fields are optional.

The ECC Payload field provides the name of the ECC payload that has scope for interactions with this network VRU. For additional information refer to the Online Help.

Step 5 Click **Save** to apply your changes.

Define Network VRU Label

You must associate all VRU Types (except Type 6) with a Network VRU label.

Step 1 In the Network VRU Explorer window, click **Retrieve** and select the Network VRU you want to add the label to.

The Label property tab appears.

Step 2 Complete the Label property tab.

The **Routing client**, **Label**, and **Label type** fields are required. All other fields are optional. For additional information refer to the online Help.

Step 3   Click **Save** to apply your changes.

Set Default Network VRU and Range of Correlation Numbers

For Network VRUs, you must use the System Information dialog to define a range of correlation IDs so the system software can communicate with the VRU about the call.

Step 1   Within the Configuration Manager, select **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

Step 2   In the System Information window, select the **Default Network VRU**.

Step 3   Enter the **Minimum Correlation Number**.

Step 4   Enter the **Maximum Correlation Number**.

For additional information refer to the online help.

Step 5   Click **Save** to apply your changes.

Configure VRU Scripts

To allow a routing script to control the processing on the VRU, you must configure VRU-based scripts within the system software. A routing script can then direct the VRU to run a specific script.

> **Note**   VRU scripts are defined and maintained on the VRU. The system software maintains only a name for each VRU script. It does not maintain the scripts themselves.

Step 1   Within the Configuration Manager, select **Tools** > **Network VRU Script List**. The Network VRU Script List window appears.

Step 2   In the Network VRU Script List window, enable **Add** by clicking **Retrieve**.

Step 3   Click **Add**. The Attributes property tab appears.

Step 4   Complete the Attributes property tab.

> **Note**   The **Name**, **Network VRU**,**VRU script name**, and **Timeout** fields are required. All other fields are optional. For additional information refer to the online Help.

Step 5   Click **Save** to apply your changes. The system software database manager automatically generates a unique Network VRU Script ID.

Accessing VRUs in Scripts

After you configure Network VRU and VRU scripts, you can use the Script Editor (refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* for additional information) to write a routing script to send a call to the VRU and invoke a specific VRU script.

Calls Queued at VRUs

You can queue a call at a Network VRU until a specific resource becomes available. A call can be queued directly to an agent, to a precision queue, to one or more skill groups, to an enterprise skill group, or to one or more scheduled targets. As soon as an agent becomes available at one of the specified targets, the call is removed from the queue and sent to the target.

Peripheral Terminology

Mapping to ACD-Specific Terminology

The following table summarizes the mapping of Unified Intelligent Contact Management (Unified ICM) terminology to ACD-specific terminology.

Table 26: Unified ICM and Peripheral-Specific Terminology

Unified ICM term	Peripheral-specific equivalent
Agent	Agent
Peripheral target	Trunk group and **DNIS**
Service	**Aspect Contact Center**: Application **Avaya Communication Manager**: Vector Directory Number (VDN)
Skill group	**Aspect Contact Center:** Agent group **Avaya Communication Manager:** Skill group or hunt group 3 Trunk group and **DNIS**
Trunk	**Aspect Contact Center:** Instrument 4 Trunk
Trunk group	Trunk group

Note Multi-channel applications function as application instances.

In some cases the Unified ICM concept is very close to the corresponding ACD feature. For example, the Unified ICM concept of a service is very similar to the Aspect concept of an application. In other cases, the ACD does not have a feature that maps exactly to the Unified ICM feature. In these cases, you might choose

a different mapping than shown in the above table. For example, although it might make sense to associate each VDN on an Avaya Communication Manager with a Unified ICM service, you could also map each hunt group to a service.

On an Avaya Communication Manager running in EAS mode, each skill group has primary and secondary subgroups. The system software emulates this by automatically creating additional skill groups for these peripheral types. For example, when you configure the Sales skill group for an Avaya Communication Manager ACD, the system software automatically creates the Sales.pri and Sales.sec skill groups in addition to the base Sales group. In monitoring and scripts, you can reference the .pri and .sec skill groups directly or you can refer to the base skill group.

Some ACDs have limitations that prevent them from making full use of specific features of the system software.

Refer to the *Pre-installation Planning Guide for Cisco Unified ICM* for the current list of supported peripherals with any peripheral-specific limitations.

Peripheral Terminology

Different peripheral manufacturers use different terminology for agents, skill groups, and services. For example, a service might be called an application, split, or gate. A skill group might be called an agent group or hunt group.

For example, note the following about using peripherals with Unified ICM:

1. The Aspect contact center maps a trunk group and DNIS to a Call Control Table (CCT). The DEFINITY ECS uses the trunk group and DNIS for incoming calls.

2. Without customer controlled routing (CCR), one or more services map to an ACD DN. With CCR, one or more services map to an ACD CDN.

3. If an ECS is running in expert agent selection (EAS) mode, a skill group maps to an ECS skill group; otherwise, it maps to a hunt group.

4. A contact center instrument can be a trunk, a teleset, or a workstation.