Software Configuration for Integrated Applications

- Software Configuration for Task Routing, on page 1
- Software Requirements, on page 1
- Software Configuration for Integration, on page 3
- Application Object Filter, on page 21

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:

Procedure

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:

Procedure

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.

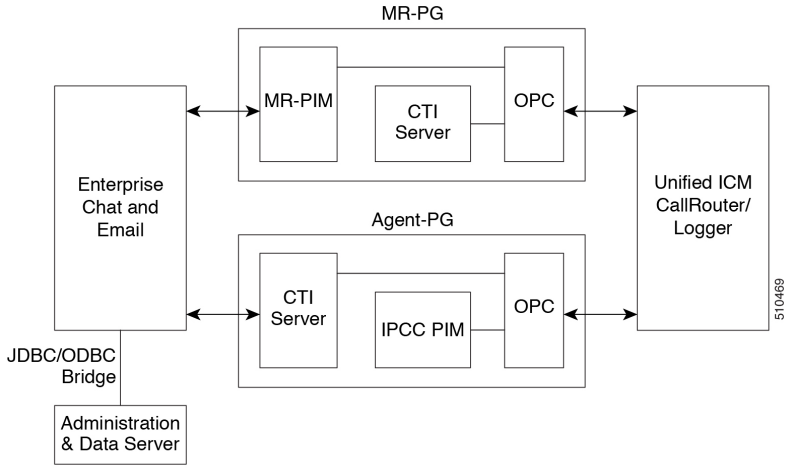
Media Routing Peripheral Gateway

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 1: 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:

Procedure

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:

Procedure

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 5. 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:

Procedure

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:

Procedure

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:

Procedure

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

Create an Agent

Configure VRU Peripheral Gateway

- Add VRU PG, on page 12
- Add VRU PIM, on page 13

Add VRU PG

Procedure

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.

Procedure

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:

Procedure

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:

Procedure

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 1: 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.

Fault Tolerance Strategy	Description
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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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.