Configuration Manager

You perform most Packaged CCE configuration with the Unified CCE Web Administration gadgets. Limited configuration is done in the legacy Configuration Manager toolset. This section explains the tools in Configuration Manager, how to access them, and why you might need them for Packaged CCE.

- Access Configuration Manager, page 1
- Configuration Manager Tools for Call Flow, page 2
- Configuration Manager Tools for Global Values and Actions, page 5
- Configuration Manager Tools for Multichannel, page 7
- Configuration Manager Tools for Scripting, page 10
- Configuration Manager Tools to Control User Access, page 11

Access Configuration Manager

Configuration Manager is a suite of tools installed with both CCE Data Server Virtual Machines and opened from a desktop icon on those VM consoles.

Although most configuration is accomplished with the Packaged CCE administration tools, you must use Configuration Manager for some configuration.

How to Access Configuration Manager

1. Open the VM Console for Packaged CCE. Select the Virtual Machine for either of the CCE Data Servers that are installed for your Packaged CCE deployment.

2. Click the Console tab.

3. Log in to the Data Server if necessary.

4. Select All Programs -> Cisco Unified CCE Tools -> Administration Tools -> Configuration Manager.

5. Select the type of tool indicated in the procedure you need to perform. This example shows the selection of Media Class List.
Configuration Manager Tools for Call Flow

Access these tools in Configuration Manager to facilitate or troubleshoot call flow.

Related Topics

PG Explorer, on page 2
Agent Targeting Rule, on page 4

PG Explorer

PG Explorer is listed in Unified CCE Configuration Manager under the Explorer Tools.

Open the tool and click Retrieve to see the two peripheral gateways that are configured for Packaged CCE: the Generic_PG and the MR_PG. The Generic_PG has five Peripheral Interface Managers (PIMs)—one for Unified Communications Manager and four for the Voice Response Units (VRUs).
To retain the Packaged CCE: CCE-PAC-M1 deployment type, do not delete either PG and do not add other PGs. The MR-PG is required, even if your contact center does not used multichannel (email and web)

**Note**

Reasons to access the Peripheral Gateway Explorer are to identify and change the default Desk Settings, to set the Primary and Secondary CTI addresses, and to enable agent reporting for an external HDS.

**Related Topics**

- Change Default Desk Settings, on page 3
- Enable Agent Reporting

**Change Default Desk Settings**

Follow these steps to locate and change the default desk settings configuration that appears in Unified CCE Web Administration tools.
**Procedure**

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

**Step 2** Select the GenericPG.

**Step 3** Select CUCM_PG_1.

**Step 4** On the Peripheral tab, locate the Default desk settings field. The first selection on the drop-down shows the option for the current default agent desk settings.

**Step 5** Select a different agent desk settings from the drop-down. Your selection moves to the top of the drop-down and becomes the new default desk settings.

**Step 6** Click **Save**.

**Related Topics**

Desk Settings

**Agent Targeting Rule**

To configure call routing in Packaged CCE, you must create one or more Agent Targeting Rules to specify the range of agent extension ranges. Based on agent targeting rules, if an agent attempts to log in to an extension to which the router cannot target a call, the peripheral gateway rejects the login request and returns an error that includes why the login request failed.

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.

**Procedure**

**Step 1** From either CCE Data Server, navigate to **Unified CCE Administration Manager > Configuration Manager**.

**Step 2** Select **Tools > List Tools > Agent Targeting Rule**.

**Step 3** Click **Retrieve**. Then click **Add**.

**Step 4** In the Attributes dialog box:

a) Name the rule

b) For Peripheral, select CUCM_PG_1.

c) For Rule type, select Agent Extension.

d) In the Routing client panel, select all four CVP clients—the two CVP_PGs on Side A and the two CVP_PGs on Side B.

e) In the Extension Ranges panel, click Add to enter the Low and High extensions for the agents. Then click **OK**.

**Step 5** Click **Save**.
What to Do Next

The CCE Call Server can only use an Agent Targeting Rule if **Agent targeting mode: Rule Preferred** is configured for the CUCM_PG_1 in PG Explorer (Advanced tab). This is set by default. If your Agent Targeting Rule does not work, verify that the configuration is still Rule Preferred.

Related Topics

- PG Explorer, on page 2

Configuration Manager Tools for Global Values and Actions

This section explains Configuration Manager tools you can use to perform for system-wide actions.

- System Information, on page 5
- Permanent Deletion, on page 7

System Information

The System Information tool in Configuration Manager allows you to define global values.

Minimum Password Length

To configure a minimum password length for agents:
1. Launch Configuration Manager
2. Select **Miscellaneous Tools > System Information**.
3. Locate the Minimum password length field in the Person Security panel. Enter a value from 0 to 32.
4. Click **Save**. The length you configure becomes the required password length for agents.

**Service Threshold Length**

This field in the Call Types tool defaults to the value that is currently configured in System Information. It is the number of seconds that a caller spends in a queue before being connected to an agent. To change it:

1. Launch Configuration Manager.
2. Select **Miscellaneous Tools > System Information**.
3. Locate the Service level threshold field in the Call Type panel. It is a number. To change it, enter a different number.
4. Click **Save**. The value you enter becomes the system default target number of seconds that a caller spends in a queue before being connected to an agent.

**Service Level Type**

This field in the Call Types tool defaults to the setting that is currently configured in System Information. One of three options is set here to determine how the system software calculates the service level for the service for abandoned calls.

- Are they ignored, which means they have no impact on service level calculation?
- Do they have negative impact, which means only calls that are answered within the Service level threshold time are counted as treated calls?
- Do they have positive impact, which means abandoned calls will have a positive impact on the Service Level?

1. Launch Configuration Manager.
2. Select **Miscellaneous Tools > System Information**.
3. Locate the Service level type drop-down in the Call Type panel. The drop-down has three options, and the option that appears at the top is the current default. To change it, select another option.
4. Click **Save**. The option you chose becomes the new system default service level type.

**System Bucket Interval**

This field in the Call Type panel establishes which set of time ranges ("buckets") is used to capture call-handling activity.

The software is installed with one system bucket interval, but once you create custom bucket intervals, you can make one of them the default.

To do this:

1. Launch Configuration Manager.
2. Select **Miscellaneous Tools > System Information**.
3 Locate the Bucket intervals drop-down in the Call Type panel. The first option on the list is the current default. This option also appears in the Bucket Intervals gadget in Unified CCE Web Administration and serves as the system default until you change it here.

4 To change it, use the drop-down to select a different bucket interval.

5 Click Save. The bucket interval you selected becomes the first option in the drop-down and is now the new system default bucket interval.

Related Topics
   Bucket Intervals
   Add and Maintain Agents
   Add and Maintain Call Types

Permanent Deletion

Some objects are only "marked for deletion" in Unified CCE Administration. They remain in the system for reporting and record-keeping purposes. To delete them permanently:

Procedure

1. Launch Configuration Manager.
2. Select Using the Configuration Manager > Deleted Objects.
3. Click the table name for the object you want to delete. This opens a panel showing all records for that table that have been marked for deletion.
4. Select one, several, or all records.
5. Click Delete Permanently.

Configuration Manager Tools for Multichannel

This section explains the Configuration Manager tools applicable to multichannel. Multichannel refers to the routing of calls to non-voice applications: email or web chat, also known as Email Interaction Manager (EIM) and Web Interaction Manager (WIM).

   Media Class List, on page 8
   Application Instance List, on page 9
   Application Path List, on page 10
   Media Routing Domain List, on page 8

Related Topics
   Overview of Multichannel Services
Media Class List

The Media Class List shows these Media Classes. The first four are not supported for Packaged CCE:

- Cisco_Blended_Collaboration
- Cisco_Email
- Cisco_Multi_Session_Chat
- Cisco_Single_Session_Chat
- Cisco_Voice
- CIM_BC
- CIM_EIM
- CIM_OUTBOUND
- CIM_WIM

You cannot delete or edit the attributes for Cisco_Voice.
You can delete and edit attributes for CIM_BC, CIM_EIM, CIM_OUTBOUND, and CIM_WIM.
You can add Media Classes.

Procedure

Step 1 Launch Configuration Manager and navigate to Tools > List Tools > Media Class List.
Step 2 Click Retrieve.
Step 3 Select a Media Class to review or edit its attributes.
Step 4 Add or delete Media Classes as appropriate.
Step 5 Save the configuration.

Media Routing Domain List

If you plan to use multichannel routing, you must configure one or more Media Routing Domains (MRDs) for them. The system uses MRDs to organize how requests from different media are routed to agents. After you add them in Configuration Manager, these MRDs will populate the Select Media Routing Domain popup window in the Dialed Number tool. If MRDs have already been configured, you might need to access this tool to change settings such as Max time in queue or Service Level Threshold.
Procedure

Step 1 Launch Configuration Manager and navigate to **Tools > List Tools > Media Routing Domain List**.

Step 2 Click **Retrieve**. Cisco_Voice is configured by default.

Step 3 Click **Add**.

Step 4 Enter the name of the MRD.

Step 5 From the Media Class drop-down menu, select any of the CIM_BC, CIM_WIM, or CIM_EIM media classes (or a custom media class if you have added one) depending on the purpose of the MRD. Typically you would have at least one MRD for each media class.

Step 6 The MRDomainID is a required read-only field. (An ID number is automatically created when you save your entry.)

Step 7 The Service Level Threshold value is the system-default that is used when configuring a skill group. See **Add and Maintain Skill Groups**.

Step 8 Enter required fields. Refer to the online help for field explanations.

Step 9 Save the configuration.

Application Instance List

If you plan to use multichannel routing, you must configure an application instance in Configuration Manager to allow the Email and Web applications to access Unified CCE. In adding an application instance, define an application ID and application key (password) that identifies the application. You need to enter the same information on the Email and Web application.

Procedure

Step 1 Launch Configuration Manager and navigate to **Tools > List Tools > Application Instance List**.

Step 2 Click **Retrieve**. Then click **Add**.

Step 3 Enter a name for the Application Instance.

Step 4 Enter and confirm the Application key.

Step 5 Select Other from the Application type drop-down menu.

Step 6 Select Full read/write from the Permission level drop-down menu.

Step 7 Save the configuration.

What to Do Next

Configure the Application Path for the Application Instance

Related Topics

- Application Path List, on page 10
Application Path List

If you plan to use multichannel routing, you must configure an application path to associate the Application Instance with peripheral gateway (PG). For Packaged CCE, the PG for the multichannel application instance is CUCM_PG in the Generic_PG.

Procedure

1. Launch Configuration Manager and navigate to Tools > List Tools > Application Path List.
2. Click Retrieve. Then click Add.
3. From the Application instance drop-down menu, select the Application Instance you have created for multichannel.
4. From the Peripheral gateway drop-down menu, select Generic_PG. The Name field populates with Generic_PG.YourApplicationInstanceName. You can change it.
5. Enter an optional Description.
6. Click Add. This adds a row to the Application Path Members table that defaults to the first peripheral and the first MRD. Add a record for each multichannel MRD associated to the CUCM_PG_1 peripheral.
   To change the MRD selection in the row, click on the MRD column and then click on the arrow that appears to the right of the row, which displays a drop-down list of all possible MRDs. Click on the one you want to select.
7. Save the configuration.

Configuration Manager Tools for Scripting

This section explains the Configuration Manager tool applicable to scripting:

- Script Reference, on page 10
- User Variable List, on page 11

Related Topics

Scripting with Packaged CCE

Script Reference

The Script Reference tool is an interface for identifying which scripts reference which objects. Not all target types are applicable to Packaged CCE.
To access this tool, navigate to Configuration Manager > Miscellaneous Tools > Script Reference. Select a Target type to see the scripts where that target is referenced.
User Variable List

User Variables are used in scripting for routing calls. 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.

User variables can be:
- Associated with object types, such as Call Types or Skill Groups. This enables the system software to maintain an instance of that variable for each object of that type in the system.
- Identified as persistent (retain value across CallRouter restarts)
- Identified as non-persistent (do not retain value across CallRouter restarts)

Procedure

1. Launch the Configuration Manager and select Tools > List Tools > User Variable List.
2. Click Retrieve. Then click Add.
3. Complete the Attributes property tab.
   Variable name, Object type, and Data type fields are required. All other fields are optional.
4. Click Save.

Configuration Manager Tools to Control User Access

There are two tools used to limit access Packaged CCE and to Unified CCE Configuration Manager, and you must use both of them.

Related Topics
- Feature Control Set List, on page 11
- User List Tool, on page 12

Feature Control Set List

Use this tool to create a Feature Control set. Once you create a feature control set, you can access the User List Tool to associate that set with users to determine which tools they can access.

Procedure

1. Launch Configuration Manager > List Tools > Feature Control Set List.
2. Click Retrieve; then click Add.
3. Enter a name and a description for the new Feature Control Set.
4. Establish access to tools by marking checkboxes for the application names on the feature set. Deny access by leaving the boxes unchecked.
Note that most application names on the Feature Control Set List do not correspond to Packaged CCE tools. This table calls out the ones that apply.

<table>
<thead>
<tr>
<th>To enable this Packaged CCE tool:</th>
<th>Check this application name in the Feature Control Set List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents (UI and API)</td>
<td>Agent Explorer</td>
</tr>
<tr>
<td>Attributes (UI and API)</td>
<td>Attribute</td>
</tr>
<tr>
<td>Desk Settings (UI and API)</td>
<td>Agent Desk Settings List</td>
</tr>
<tr>
<td>Precision Queues (UI and API)</td>
<td>Precision Queue</td>
</tr>
<tr>
<td>Skill Groups (UI and API)</td>
<td>Skill Group Explorer</td>
</tr>
<tr>
<td>Teams (UI and API)</td>
<td>List Agent team</td>
</tr>
<tr>
<td>Reason Codes (UI and API)</td>
<td>Reason Code List</td>
</tr>
<tr>
<td>Bucket Intervals (UI and API)</td>
<td>Bucket Intervals List</td>
</tr>
<tr>
<td>Call Types (UI and API)</td>
<td>Call Type List</td>
</tr>
<tr>
<td>Dialed Numbers (UI and API)</td>
<td>Dialed Number/Script Selector List</td>
</tr>
<tr>
<td>Expanded Call Variables (UI and API)</td>
<td>Expanded Call Variable List</td>
</tr>
<tr>
<td>Network VRU Scripts (UI and API)</td>
<td>Network VRU Script List</td>
</tr>
<tr>
<td>Bulk Jobs (UI and API)</td>
<td>Dialed Number Bulk Edit AND Agent Bulk Edit</td>
</tr>
<tr>
<td>Deployment , Configure Deployment, and Agent Trace (UI)</td>
<td>System Information</td>
</tr>
<tr>
<td>Congestion Control, Deployment Type Info, and Agent Trace (API)</td>
<td></td>
</tr>
</tbody>
</table>

**User List Tool**

With this tool, you can associate Feature Control Set with a user and/or limit access to "read-only." These are independent options.
Procedure

Step 1 To assign a feature control set:
   a) Launch **Configuration Manager > List Tools > User List**.
   b) Click **Retrieve**.
   c) Select the user you want to limit, or add the user to the list.
   d) Select the feature control set from the drop-down list. The user will be able to access the applications you checked for that feature control list. The user will not be able to access the unchecked applications.

Step 2 To limit access to "read-only":
   a) Launch **Configuration Manager > List Tools > User List**.
   b) Click **Retrieve**.
   c) Select the user you want to limit, or add the user to the list.
   d) Check Read only.

Note
Users who have no feature control set limitations but have "read-only" checked can access all tools but have no permissions to make changes in tools.

Users who have feature control set limitations and have "read only" checked cannot see the tools the feature control set excludes. They can see the other tool but cannot make changes in those tools.

Users who try to access a tool for which they do not have permissions are redirected to the first tool for which they have permissions.