Configure External Call Control

- External Call Control Overview, on page 1
- External Call Control Prerequisites, on page 2
- External Call Control Configuration Task Flow, on page 2
- External Call Control Interactions, on page 8
- External Call Control Restrictions, on page 10

External Call Control Overview

External call control lets an adjunct route server make call routing decisions for Unified Communications Manager by using the Cisco Unified Routing Rules Interface. When you configure external call control, Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. That server receives the request, applies appropriate business logic, and returns a route response that instructs your system on how to route the call and any additional call treatment to apply.

The adjunct router influences how your system allows, diverts, or denies calls; modifies calling and called party information; plays announcements to callers; resets call history so that adjunct voicemail and IVR servers can properly interpret calling and called party information; and logs reason codes that indicate why calls were diverted or denied.

External call control provides the following functions:

- Best Quality Voice Routing—The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure that calls are routed through voice gateways that deliver the best voice quality to all call participants.
- Least Cost Routing—The adjunct route server is configured with carrier contract information such as local access and transport area (LATA) and inter-LATA rate plans, trunking costs, and burst utilization costs to ensure that calls are routed over the most cost effective links.
- Ethical Wall—The adjunct route server is configured with corporate policies that determine reachability, for example, whether user 1 is allowed to call user 2.

External Call Control Prerequisites

This feature requires the Cisco Unified Routing Rules XML Interface, which directs your system on how to handle calls.

For more information, see the *Cisco Unified Routing Rules Interface Developers Guide* (CURRI documentation) at https://developer.cisco.com.

External Call Control Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Calling Search Space for External Call Control, on page 3	Configure a calling search space for your system to use when the route server sends a divert obligation. A calling search space comprises an ordered list of route partitions that you assign to devices. Calling search spaces determine the partitions that calling devices search when they attempt to complete a call.
Step 2	Configure an External Call Control Profile, on page 4	Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.
Step 3	Assign a Profile to a Translation Pattern, on page 4	For the translated patterns that you want to use with external call control, assign an external call control profile to the pattern. When a call occurs that matches the translation pattern, your system immediately sends a call routing query to an adjunct route server, and the adjunct route server directs your system on how to handle the call.
Step 4	(Optional) Import the Route Server Certificate into the Trusted Store, on page 5	If the route server uses HTTPS, import the certificate for the route server into the trusted store on your system node. You must perform this task on each node in the cluster that can send routing queries to the route server. If you use HTTPS for the primary or secondary web service URIs in the external call control profile, your system uses certificates to mutually authenticate through a TLS connection to the configured adjunct route servers.

	Command or Action	Purpose
Step 5	(Optional) Export the Self-Signed Certificate to the Route Server, on page 5	If the route server uses HTTPS, export the Cisco Unified Communications Manager self-signed certificate to the route server. You must perform this task for each node in the cluster that can send routing queries to the route server. To ensure that the primary and redundant route servers can authenticate with Cisco Unified Communications Manager through HTTPS, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to your system. Perform this procedure for each node in the cluster that can contact the primary and redundant adjunct route server.
Step 6	(Optional) Configure the Chaperone Function, on page 6	Configure chaperone functionality if your routing rules from the route server state that a chaperone must monitor or record a call. A chaperone is a designated phone user who can announce company policies in the call, monitor the call, and record the call.
Step 7	(Optional) Configure Customized Announcements, on page 7	Follow this procedure if your routing rules require that an announcement is played for some calls and you do not want to use the Cisco-provided announcements.

Configure a Calling Search Space for External Call Control

Configure a calling search space for your system to use when the route server sends a divert obligation. A calling search space comprises an ordered list of route partitions that you assign to devices. Calling search spaces determine the partitions that calling devices search when they attempt to complete a call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure an External Call Control Profile

Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **External Call Control Profile**.

Step 2 Perform one of the following tasks:

- Click **Find** and then choose an existing external call control profile from the resulting list to modify the settings for an an existing external call control profile, enter search criteria.
- Click **Add New** to add a new external call control profile.

Step 3 Configure the fields on the **External Call Control Profile Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Assign a Profile to a Translation Pattern

Configure an external call control profile to provide the URIs for the adjunct route server, a calling search space that is used for diverting calls, a timer that indicates how long your system waits for a response from the adjunct route server, and so on.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Perform one of the following tasks:

- Click **Find** and then choose an existing translated pattern from the resulting list to modify the settings for an existing translated pattern, enter search criteria, .
- Click **Add New** to add a new translated pattern.

Step 3 From the **External Call Control Profile** drop-down list, choose the external call control profile that you want to assign to the pattern.

Step 4 Configure other fields as needed in the **Translation Pattern Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 5 Click **Save**.

Import the Route Server Certificate into the Trusted Store

If the route server uses HTTPS, import the certificate for the route server into the trusted store on your system node. You must perform this task on each node in the cluster that can send routing queries to the route server. If you use HTTPS for the primary or secondary web service URIs in the external call control profile, your system uses certificates to mutually authenticate through a TLS connection to the configured adjunct route servers.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 In the **Upload Certificate** popup window, click **CallManager-trust** from the **Certificate Name** drop-down list, and browse to the certificate for the adjunct route server.

Step 4 After the certificate appears in the **Upload File** field, click **Upload**.

Step 5 (Optional) Perform this procedure again if your system can contact a redundant adjunct route server.

Export the Self-Signed Certificate to the Route Server

If the route server uses HTTPS, export the Unified Communications Manager self-signed certificate to the route server. You must perform this task for each node in the cluster that can send routing queries to the route server. To ensure that the primary and redundant route servers can authenticate with Unified Communications Manager through HTTPS, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to your system.

Perform this procedure for each node in the cluster that can contact the primary and redundant adjunct route server.

Procedure

Step 1 From Cisco Unified Operating Administration, choose **Security** > **Certificate Management**.

Step 2 In the **Certificate List** window, click **Generate New**.

Step 3 From the **Certificate Name** drop-down list, choose **CallManager**.

Step 4 Click **Generate New**.

Step 5 From the **Find and List Certificates** window, choose the **CallManager.pem** certificate that you just created.

Step 6 After the certificate file data appears, click **Download** to download the certificate to a location that you can use for exporting the certificate to the adjunct route server.

Step 7 Export the certificate to each adjunct route server that sends directives.

Configure the Chaperone Function

Configure chaperone functionality if your routing rules from the route server state that a chaperone must monitor or record a call. A chaperone is a designated phone user who can announce company policies in the call, monitor the call, and record the call.

Unified Communications Manager provides the following capabilities to support chaperone functionality, as directed by the adjunct route server:

- Redirect an incoming call to a chaperone, hunt group, or a list of chaperones.
- Provide a chaperone with the ability to record a call.

When the chaperone is connected to the caller or when the chaperoned conference is established, the **Record** softkey or programmable line key (PLK) (depending on the phone model) is active on the phone so that the chaperone can invoke call recording. Call recording occurs for only the current call, and call recording stops when the current call ends. Messages that indicate the status of recording may display on the phone when the chaperone presses the recording softkey or PLK.

Procedure

Step 1 For phones on which you want to enable recording, set the Built-in-Bridge to **On** in the **Phone Configuration** window.

Step 2 Create a recording profile:

a) Choose **Device** > **Device Settings** > **Recording Profile**.
b) Create a Call Recording Profile for the phones that can record chaperoned conferences.

Step 3 Apply the recording profile to the line appearance.

Step 4 Add a SIP trunk to point to the recorder.

Step 5 Create a route pattern that points to the SIP trunk.

Step 6 Configure the following service parameters:

a) Play Recording Notification Tone to Observed Target
b) Play Recording Notification Tone to Observed Connected Target

Step 7 Assign the Standard Chaperone Phone softkey template to the phone that the chaperone uses.

Step 8 Perform the following steps from **Call Routing** > **Directory Number** for a new phone or from **Device** > **Phone** if the phone is already configured:

a) Configure only one directory number (DN) for the chaperone phone.
b) For the DN on the chaperone phone, choose **Device Invoked Call Recording Enabled** from the **Recording Option** drop-down list.
c) For the DN on the chaperone phone, enter `2` for the **Maximum Number of Calls** setting, and enter `1` for the **Busy Trigger** setting.

Step 9 For Cisco Unified IP Phones that support the **Record** softkey, configure the Standard Chaperone Phone softkey template so that only the **Conference**, **Record**, and **End Call** softkeys display on the phone in a connected state.

Step 10 For Cisco Unified IP Phones that support the record programmable line key (PLK), configure the PLK in the **Phone Button Template Configuration** window.

Step 11 (Optional) If you have more than one chaperone in your cluster, add the chaperone DN to the chaperone line group that you plan to assign to the chaperone hunt list.

This step ensures that an available chaperone monitors the call.

Configure Customized Announcements

Follow this procedure if your routing rules require that an announcement is played for some calls and you do not want to use the Cisco-provided announcements.

Tip Do not use embedded spaces for the announcement identifier.

If other language locales are installed, you can upload other .wav files for this announcement to use with those locales.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Announcement**.

Step 2 Perform one of the following tasks:

- To add a new announcement:

a) Click **Add New**.
b) In the **Announcement Identifier** field, enter an announcement identifier.
c) In the **Description**, enter a description of the announcement.
d) From the **Default Announcement** drop-down list, choose a default Cisco-provided announcement if desired.
e) Click **Save**.

- To upload a custom .wav file for the announcement:

a) Click **Upload File**.
b) From the **Locale** drop-down list, choose the locale language for the announcement.
c) Click **Choose File**, and then choose a .wav file to upload.
d) Click **Upload File**.
e) When the upload finishes, click **Close** to refresh the window and show the uploaded announcement.

External Call Control Interactions

Table 1: External Call Control Interactions

Feature	Interaction
Best Call Quality Routing	You can set up routing rules on the adjunct route server that determine which gateway to use for a call, taking voice quality into consideration. For example, gateway A provides the best voice quality, so it is used for the call. In this case, the adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and mean opinion scores (MOS) to ensure that calls are routed through voice gateways that deliver the best voice quality to all call participants.
Call Detail Records	External Call Control functions can be displayed in call detail records; for example, the call detail record can indicate whether the adjunct route server permitted or rejected a call. In addition, the call detail record can indicate whether Unified Communications Manager blocked or allowed calls during which it did not receive a decision from the adjunct route server.
Call Forward	External Call Control intercepts calls at the translation pattern level, while Call Forward intercepts calls at the directory number level. External Call Control has a higher priority than Call Forward; for calls that invoke Call Forward, Unified Communications Manager sends a routing query to the adjunct route server if the translation pattern is assigned to an External Call Control profile. Call Forward is triggered only when the adjunct route server sends a Permit decision with a Continue obligation to the Cisco Unified Communications Manager. **Note** The **Call Diversion Hop Count** service parameter that supports External Call Control and the **Call Forward Call Hop Count** service parameter that supports Call Forward are independent of each other.
Call Pickup	When a phone user tries to pick up a call by using the Call Pickup feature, External Call Control is not invoked; Unified Communications Manager does not send a routing query to the adjunct route server for that portion of the call.
Chaperones	A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone.

Feature	Interaction
Cisco Unified Mobility	Unified Communications Manager allows the route decision from the adjunct route server for the following Cisco Unified Mobility features: • Mobile Voice Access • Enterprise Feature Access • Dial-via-Office Reverse Callback Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features: • Cell pickup • Desk pickup • Session handoff
Conferences	When a phone user creates a conference, External Call Control may be invoked for the primary call and consultative call.
Directory Numbers	When you configure directory numbers as four- or five-digit extensions (enterprise extensions), you need to configure two translation patterns if on-net dialing supports four or five digits. One translation pattern supports globalizing the calling and called numbers, and a second translation pattern supports localizing the calling and called numbers.
Do Not Disturb	By default, the DND setting for the user takes effect when the user rule on the adjunct route server indicates that the adjunct route server sent a continue obligation. For example, if the adjunct route server sends a continue obligation, and the user has DND-R enabled, Unified Communications Manager rejects the call.
Emergency Call Handling	**Caution** We strongly recommend that you configure a very explicit set of patterns for emergency calls (for example, 911 or 9.11) so that the calls route to their proper destination (for example, to Cisco Emergency Responder or a gateway) without having to contact the route server for instructions on how to handle the call.
Transfer	When a phone user transfers a call, External Call Control may be invoked for both the primary call and consultative call. However, Unified Communications Manager cannot enforce any routing rules from the adjunct route server between the party that transfers and the target of the transfer.

External Call Control Restrictions

Table 2: External Call Control Restrictions

Restriction	Description
Adding Parties	The chaperone cannot use the phone to add parties to a conference after the conference begins, because the call must be put on hold for the chaperone to add parties. The other parties on the conference may add additional parties to the conference. The configuration for the **Advanced Ad Hoc Conference Enabled** service parameter, which supports the Cisco CallManager service, determines whether other parties can add participants to the conference. If the service parameter is set to **True**, other parties can add participants to the conference.
Call Transfer	The chaperone cannot use the phone to transfer the conference call to another party.
Conference Log Out	When the chaperone leaves the conference, the entire conference ends.
Conference Softkey	After the chaperone creates a conference, the **Conference** softkey, if available, is disabled on the phone.
Hold	The chaperone cannot use the phone to put the conference call on hold.
Recording	If the chaperone starts recording before the feature makes a consultative call to the party that will join the conference, Unified Communications Manager suspends recording while the chaperone makes the consultative call; recording resumes after the conference is established.