Configure Call Control Discovery

Call Control Discovery Overview

Use Call Control Discovery (CCD) to advertise Unified Communications Manager information along with other key attributes, such as directory number patterns. Other call control entities that use the Service Advertisement Framework (SAF) network can use the advertised information to dynamically configure and adapt their routing operations. All entities that use SAF advertise their directory number patterns along with other key information. Other remote call control entities can learn the information from this broadcast and adapt the routing operations of the call.

Call Control Discovery Prerequisites

- SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks
- Remote call control entities that support and use the SAF network; for example, other Unified Communications Manager or Cisco Unified Communications Manager Express servers
- Cisco IOS routers that are configured as SAF forwarders

Call Control Discovery Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	See the documentation that supports your Cisco IOS router. Cisco Feature Navigator (http://www.cisco.com/go/cfn) allows you to	Configure a Cisco IOS router as the SAF forwarder.

	Command or Action	Purpose
	determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform.	
Step 2	Configure SAF Security Profile, on page 3	Configure the SAF security profile for the SAF forwarder to provide a secure connection between the SAF forwarder and Unified Communications Manager.
Step 3	Configure SAF Forwarders, on page 4	Configure the SAF forwarders, which are Cisco IOS routers configured for SAF. They notify the local cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local cluster for each configured and registered trunk that is configured; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.
Step 4	Configure SIP or H.323 Intercluster Trunks, on page 4	Configure SIP or H.323 intercluster (non-gatekeeper controlled) trunks for SAF support. The local cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network.
Step 5	Configure Hosted DN Groups, on page 5	Configure hosted DN groups, which are collections of hosted DN patterns. After you assign a hosted DN group to the CCD advertising service, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD advertising service.
Step 6	Configure Hosted DN Patterns, on page 5	Configure hosted DN patterns, which are directory number patterns that belong to Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns with hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.

	Command or Action	Purpose
Step 7	Configure the Advertising Service, on page 6	Configure the call control discovery advertising service, which allows Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network.
Step 8	Configure the Partition for Call Control Discovery, on page 6	Configure a call control discovery partition to ensure that the learned patterns are inserted into digit analysis under this partition.
Step 9	Configure the Requesting Service, on page 6	To ensure that your local cluster can detect advertisements from the SAF network, configure one call control discovery requesting service to listen for advertisements from remote call control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns are inserted into the digit analysis.
Step 10	Block Learned Patterns, on page 7	Block learned patterns that remote call control entities send to the local Unified Communications Manager. Perform this procedure on learned patterns that you no longer want to use.

Configure SAF Security Profile

Configure the SAF security profile for the SAF forwarder to provide a secure connection between the SAF forwarder and Unified Communications Manager.

Tip Use the same username and password that you entered on the router (SAF forwarder).

Before you begin

Configure a Cisco IOS router as the SAF forwarder. (See the Cisco Feature Navigator at http://www.cisco.com/%20go/cfn.)

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **SAF** > **SAF Security Profile**.

Step 2 Configure the fields on the **SAF Security Profile Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure SAF Forwarders

Configure the SAF forwarders, which are Cisco IOS routers configured for SAF. They notify the local cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local cluster for each configured and registered trunk that is configured; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.

Tip If more than one node appears in the **Selected Cisco Unified Communications Managers** pane, append @ to the client label value; otherwise, errors can occur if each node uses the same client label to register with the SAF forwarder.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **SAF** > **SAF Forwarder**.

Step 2 Configure the fields on the **SAF Forwarder Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure SIP or H.323 Intercluster Trunks

Configure SIP or H.323 intercluster (non-gatekeeper controlled) trunks for SAF support. The local cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 Perform one of the following tasks:

- For SIP trunks:
  - **a.** From the **Trunk Service Type** Type drop-down list, choose **Call Control Discovery**. You cannot change the trunk service type after you select it from the drop-down list.
  - **b.** Click **Next**.

c. Configure the fields on the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

- For intercluster (non-gatekeeper controlled) trunks:

a. Click **Next**.

b. Check the **Enable SAF** check box.

c. Configure the other fields on the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure Hosted DN Groups

Configure hosted DN groups, which are collections of hosted DN patterns. After you assign a hosted DN group to the CCD advertising service, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD advertising service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Hosted DN Group**.

Step 2 Configure the fields on the **Hosted DN Groups Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure Hosted DN Patterns

Configure hosted DN patterns, which are directory number patterns that belong to Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns with hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**.

Step 2 Configure the fields on the **Hosted DN Patterns Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Advertising Service

Configure the call control discovery advertising service, which allows Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Advertising Service**.

Step 2 Configure the fields in the **Advertising Service Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Partition for Call Control Discovery

Configure a call control discovery partition to ensure that the learned patterns are inserted into digit analysis under this partition.

Note The CCD partition does not appear under **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager Administration.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Partition**.

Step 2 Configure the fields in the **Call Control Discovery Partition Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure the Requesting Service

Caution Updating the **Learned Pattern Prefix** or **Route Partition** fields can affect system performance. To avoid system performance issues, we recommend that you update these fields during off-peak hours.

To ensure that your local cluster can detect advertisements from the SAF network, configure one call control discovery requesting service to listen for advertisements from remote call control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns are inserted into the digit analysis.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Requesting Service**.

Step 2 Configure the fields in the **Requesting Service Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure your remote call control entity to use the SAF network. (See the documentation for your remote call control entity.)

Block Learned Patterns

Block learned patterns that remote call control entities send to the local Unified Communications Manager. Perform this procedure on learned patterns that you no longer want to use.

Before you begin

Configure your remote call control entity to use the SAF network. See the documentation that supports your remote call control entity.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Control Discovery** > **Block Learned Patterns**.

Step 2 Click **Add New**.

Step 3 Configure one of the following fields:

- In the **Learned Pattern** field, enter the exact learned pattern that you want to block. You must enter the exact pattern that you want Cisco Unified Communications Manager to block.
- In the **Learned Pattern Prefix** field, enter the prefix to block a learned pattern based on the prefix that is prepended to the pattern.

Example:

For **Learned Pattern**, enter 235XX to block 235XX patterns.

Example:

For **Learned Pattern Prefix**, enter +1 to block patterns that use +1.

Step 4 In the **Remote Call Control Entity** field, enter the name of the remote call control entity that advertises the pattern that you want to block.

Step 5 In the **Remote IP** field, enter the IP address for the remote call control entity where you want to block the learned pattern.

Step 6 Click **Save**.

Call Control Discovery Interactions

Table 1: Call Control Discovery Interactions

Feature	Interaction
Alarms	Cisco Unified Serviceability provides alarms to support the call control discovery feature. For information about how to configure alarms, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
BLF Subscriptions	For a user to subscribe BLF status of a SAF learned pattern, Unified Communications Manager sends a SIP subscribe message over a SIP trunk to the remote cluster. This functionality is supported with only SAF-enabled SIP trunks.
Bulk Administration Tool	In the Bulk Administration Tool, you can import and export the configuration for SAF security profiles, SAF forwarder, CCD advertising service, CCD requesting service, hosted DN groups, and hosted DN patterns.
Call Detail Records	Unified Communications Manager supports redirecting onBehalfOf as SAFCCDRequestingService with a redirection reason as SS_RFR_SAF_CCD_PSTNFAILOVER, which indicates that the call is redirected to a PSTN failover number.

Feature	Interaction
Incoming Called Party Settings	The H.323 protocol does not support the international escape character +. To ensure that the correct DN patterns are used with SAF and call control discovery for inbound calls over H.323 gateways or trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configure the incoming called party settings to ensure that when a inbound call comes from a H.323 gateway or trunk, Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk or gateway. For example, a caller places a call to +19721230000 to Unified Communications Manager A. Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type. For this inbound call from the trunk, Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.
Digest Authentication	Unified Communications Manager uses digest authentication (without TLS) to authenticate to the SAF forwarder. When Unified Communications Manager sends a message to the SAF forwarder, Unified Communications Manager computes the SHA1 checksum and includes it in the MESSAGE-INTEGRITY field in the message.
QSIG	The QSIG Variant and ASN.1 ROSE OID Encoding settings in the **H.323 Configuration** window are advertised by the CCD advertising service. These settings affect decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not affect outgoing calls. The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the **H.323 Configuration** window in Cisco Unified CM Administration indicates that QSIG support is not required.

Call Control Discovery Restrictions

All clusters are limited to advertised or learned routes within the same autonomous system (AS).