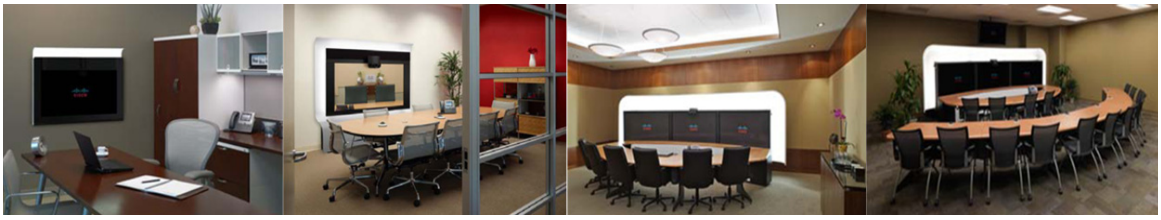

CHAPTER 4

Configuring Cisco Unified Communications Manager for CTMS

November 2011

Contents

Overview

Before installing the CTMS Administration software on the server, you need to perform the following configuration tasks in Unified CM:

- Determine if security is required on multipoint calls. If security is required, manually download certificates from Unified CM. Then upload these certificates to CTMS.
- Create a Session Initiation Protocol (SIP) security profile. This security profile will be applied to the SIP trunk between CTMS and Unified CM. Each secure SIP trunk has a unique X.509 subject name and therefore requires its own SIP security profile. Unsecure SIP trunks can share a SIP security profile.
- Create a SIP trunk. The SIP trunk is used for communication between Unified CM and CTMS.
- Create route patterns. A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns are used for routing calls that match CTMS conference numbers to the corresponding CTMS.

Prerequisites

Before starting the tasks in this chapter, make sure that the following conditions are met or that you understand the following information:

- The Unified CM version is one of the following, which are compatible with CTMS 1.8:
  - To support interop meetings with Cisco TelePresence TC version 5.0 endpoints: version 8.6.1
  - To support non-interop meetings without Cisco TelePresence TC version 5.0 endpoints: versions 7.1.5, 8.5.1, and 8.6.1
- Cisco TelePresence endpoints are running the compatible software releases outlined in the *Cisco TelePresence System Software Compatibility - CTS 1.8 Release*, which you can access at this location:

  http://www.cisco.com/en/US/products/ps8332/products_device_support_tables_list.html

For additional information about configuring Unified CM for Cisco TelePresence System, see the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* at this location:

http://www.cisco.com/en/US/partner/docs/telepresence/cucm_cts/cucm_cts_admin_book/guide/cucm_cts_admin.html

Limitations

Be aware of the following Unified CM configuration limitation:

- Do not enable duplex streaming mode in Unified CM. Enabling this mode causes issues with certain CTMS functionality, such as audio add-in and calls on hold.

Logging into the Cisco Unified CM Administration Application

To log into the Cisco Unified CM Administration application:

Step 1 Open a web browser.

Step 2 Access a web browser that is supported by the Cisco Unified CM Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

```
https://CUCM-server-name
```

where *CUCM-server-name* is the name or IP address of the server.

Note You may need to specify the address of the server where Unified CM is installed. If your network uses DNS services, you can specify the hostname of the server. If your network does not use DNS services, you must specify the IP address of the server.

Step 3 Log in with your assigned administrative privileges.

Step 4 Select ***Cisco Unified Communications Manager Administration*** in the **Navigation** field at the upper right corner of the page and click ***Go*** to return to the Cisco Unified Communications Manager Administration home page.

Creating a SIP Trunk Security Profile

To create a SIP trunk security profile:

Step 1 Click ***System***. Under **Security**, click ***SIP Trunk Security Profile***.

Step 2 Click the ***Add New*** button at the bottom of the page or click the ***+ sign*** at the top of the page.

Step 3 Enter the settings as indicated in Table 4-1 to configure the SIP trunk security profile. Leave default settings for fields not included in Table 4-1.

Table 4-1 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string identifying this SIP trunk security profile.
Description	No	Enter a text string describing this SIP trunk security profile.
Device Security Mode	Yes	For information about Device Security Mode, see the following documentation: http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/security/7_0_1/secugd/secutrnk.html#wp1071125
Incoming Transport Type	Yes	Select ***TCP+UDP***. If Encrypted is selected, TLS will be entered automatically.
Outgoing Transport Type	Yes	Select ***TCP***.
X.509 Subject Name	Yes (for secure signaling)	Inspect the downloaded LSC to find the X.509 subject name. See the "Security" section on page 3-11 for information about locating the LSC and subject name.
Incoming Port	Yes	Enter ***5060*** for non-secure trunk. Enter ***5061*** for authenticated or encrypted. If running SIP security, then enter a different unused port, for example 5275.

Step 4 Click the ***Save*** button at the bottom of the page.

Note For more information about security options, see the following documentation: http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/security/7_0_1/secugd/secutrnk.html#wp1071125

Creating a SIP Trunk

To create a SIP trunk:

Step 1 Click ***Device***. Click ***Trunk***.

Step 2 Click the ***Add New*** button at the bottom or click the ***+ sign*** at the top of the Trunk Configuration page.

Step 3 Select ***SIP Trunk*** from the **Trunk Type** pull-down menu, then click ***Next***.

Step 4 Enter the settings as indicated in Table 4-2 to configure the SIP trunk. Leave default settings for fields not included in Table 4-2.

Table 4-2 SIP Trunk Settings

Field	Required	Setting
Device Information		
Device Name	Yes	Enter a text string identifying this SIP trunk.
Description	No	Enter a text string describing this SIP trunk.
Device Pool	Yes	Select ***Default***.
Call Classification	Yes	Choose ***OnNet***. If this parameter is set to OffNet, CTS endpoints do not answer ad hoc calls from the CTMS. Any SIP trunk set to OffNet disables the auto-answer feature.
SIP Information		
Destination Address	Yes	Enter the IP address of the CTMS.
SIP Trunk Security Profile	Yes	Select the SIP trunk security profile that you created for CTMS.
SIP Profile	Yes	Select ***Standard SIP Profile***.

Step 5 Click the ***Save*** button at the bottom of the page.

Configuring a Route Pattern

A route pattern allows a Unified CM-managed device to access another device by dialing its number. Such devices may include gateways, Cisco TelePresence Multipoint Switch (CTMS) systems, or Cisco Unified Videoconferencing 5230 (CUVC) MCUs. Each device requires its own unique route pattern.

To configure a route pattern:

Step 1 Click ***Call Routing***. Under **Route/Hunt**, click ***Route Pattern***.

Step 2 Click the ***Add New*** button at the bottom or click the ***+ sign*** at the top of the Route Pattern Configuration page.

Step 3 Enter the settings as indicated in Table 4-3 to configure the SIP trunk. Leave default settings for fields not included in Table 4-3.

Table 4-3 Route Pattern Configuration Settings

Field	Required	Setting
Pattern Definition		
Route Pattern	Yes	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. The uppercase characters A, B, C, and D are valid characters. **Note** See the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco CallManager System Guide* for more information about wildcards. **Note** The route pattern that is configured must match the access settings numbers that are configured in the CTMS.
Description	No	Enter a text string describing this route pattern.
Gateway/Route List	Yes	Select the SIP trunk that you created for CTMS.
Call Classification	Yes	Choose ***OnNet***.

Step 4 Click the ***Save*** button at the bottom of the page.