CHAPTER 2

Configuring Cisco Unified Communications Manager for CTMS

Initial Release: February 25, 2009, OL-12906-03

Contents

Overview

Before installing the CTMS Administration software on your Cisco MCS-7845 Media Convergence Server, you need to perform the following configuration tasks in Cisco Unified Communications Manager (Cisco Unified CM):

- Create a SIP security profile. This security profile will be used on the SIP trunk between CTMS and Cisco Unified CM.
- Create a Session Initiation Protocol (SIP) trunk. The SIP trunk is used for communication between Cisco 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 conferences numbers to the CTMS.

Prerequisites

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

- Cisco Unified CM is running and using Release 6.1.3 or 7.0.2; If you decide to deploy the new CTS Release 1.5 Enhanced Phone User Interface (MIDlets), you must install Cisco Unified CM Release 7.0.2.
- Cisco TelePresence System is running Release 1.4x or later software.

For additional information about configuring Cisco Unified CM for Cisco TelePresence System, refer to the *Cisco Unified Communications Manager Installation Guide for the Cisco TelePresence System*.

For compatibility information, refer to *Compatibility Information for Cisco TelePresence System Release 1.5*.

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 Cisco 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 Profile**, 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 2-1 to configure the SIP trunk security profile. Leave default settings for fields not included in Table 2-1.

.

Table 2-1 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string identifying this SIP trunk security profile.
Description	—	Enter a text string describing this SIP trunk security profile.
Device Security Mode	Yes	If you are running in non-secure mode, select ***Non Secure***. If you are running SIP security, select ***Encrypted***.
Incoming Transport Type	Yes	Select ***TCP+UDP***. If Encrypted is selected, TLS will be entered automatically.
Outgoing Transport Type	Yes	Select ***TCP***.
Incoming Port	Yes	Enter ***5060*** for non-secure trunk. 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.

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 2-2 to configure the SIP trunk. Leave default settings for fields not included in Table 2-2.

.

Table 2-2 SIP Trunk Settings

Field	Required	Setting
Device Information		
Device Name	Yes	Enter a text string identifying this SIP trunk.
Description	—	Enter a text string describing this SIP trunk.
Device Pool	Yes	Select ***Default***.
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 Cisco 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 Video Conferencing (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 2-3 to configure the SIP trunk. Leave default settings for fields not included in Table 2-3.

.

Table 2-3 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.
Description	—	Enter a text string describing this route pattern.
Gateway/Route List	Yes	Select the SIP trunk that you created for CTMS.
Call Classification	Yes	Select ***OnNet***.

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