AVAYA

Avaya Agile Communication Environment Cisco Unified Communications Manager Integration

Release: 2.2

Document Revision: 05.01

Number: NN10850-024

While the information in this document is believed to be accurate and reliable, iexcept as otherwise expresslyagreed to in writing AYAYA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OFANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are Subject to change without notice.

Contents

Introduction....3
  Purpose....3
  Prerequisites....4
Solution overview....9
  Introduction....9
  Standards and protocols....10
  Administration....12
  Cisco IP Phones....13
  Security....15
  How ACE and the Cisco Unified CM interact....16
Basic Cisco Unified CM configuration....17
  Introduction....17
  Cisco Unified CM base configuration....18
Standard SIP solutions....21
  Introduction....21
  Configure SIP trunk for ACE....23
JTAPI solutions....29
  Introduction....29
  Configure CTI services for ACE....30

Introduction

Purpose

Description

Agile Communication Environment - Cisco Unified Communications Manager (NN10850-024) highlights the minimum Cisco Unified CM parameters that must be verified or addressed prior to integration with ACE. It assumes that the Cisco Unified CM is installed and fully operational. It also assumes that personnel have a basic understanding of Cisco Unified CM system architecture and programming methodology.

Important: This product does not replace ACE training or documentation. It is designed to augment training and documentation by providing focused topics related to ACE and Cisco Unified CM deployments. Refer to the Cisco documentation for more comprehensive information about programming a Cisco Unified CM system. Refer to the standard ACE documentation for tasks performed using the ACE GUI.

Resources

The resources for this product are:

- *Agile Communication Environment Planning and Installation* (NN10850-004)
- *Agile Communication Environment Administration* (NN10850-005)
- *Agile Communication Environment Web Services* (NN10850-007)

For information about Cisco products and documentation, see the Cisco website.

Prerequisites

ACE knowledge requirements

The following knowledge and skills are required.

- Working knowledge of the ACE solution, including purpose, design model, and benefits
- Working knowledge of ACE services and features
- Working knowledge of the basic purpose and characteristics of Service-Oriented Architecture (SOA) and Web Services and how they apply to an ACE solution
- Working knowledge of the key elements in the ACE reference architecture
- Working knowledge of platform operating requirements and supported configurations
- Working knowledge of supported operating systems
- Working knowledge of ACE platform software installation, upgrade, and uninstall procedures
- Working knowledge of the ACE operations, administration, management , and performance framework
- Working knowledge of the ACE security framework
- Ability to identify and use supported interfaces to perform procedures related to ACE configuration, administration, and management

Tip

It is strongly recommended that you complete product-specific training before you begin integrating ACE with the CS 1000 system. Recommended training includes Course 8674AX, *Agile Communication Environment Installation and Administration*.

Cisco Unified CM knowledge requirements

- Working knowledge of voice and data communications
- Working knowledge of Internet Protocol and Voice over IP concepts and terminology, including standards and protocols, such as Media Gateway Control Protocol (MGCP), H.323, Session Initiation Protocol (SIP), Computer Telephony Integration (CTI), and Java Telephony Application Programming Interface (JTAPI)
- Working knowledge of Cisco Unified Communications solution hardware, software, and architecture
- Working knowledge of Cisco Unified Communications solution programming and provisioning
- Working knowledge of call routing and dialing plan requirements for a Cisco Unified Communications solution

Deployment plan

Research and document deployment requirements; for example:

- Scope of work:
  - Project contacts
  - Local safety requirements
  - Deployment plan
  - Defined roles and responsibilities.
  - Milestones
  - Verification plan
- Description of existing network infrastructure; for example:
  - Type of network (campus, centralized, distributed, etc.)
  - System types and software release
  - Number and location of sites
  - Number of users (per site)
  - Number of users for various services (Click-to-Call, etc.)
  - Configured end points and terminal devices
  - Connectivity between network elements (standards and protocols used; trunk and route parameters, etc.)
  - Products, services, and features used in the existing environment
  - Dialing plans, IP addressing
- ACE core configuration requirements:
  - Deployment type (Linux or Windows)
  - Standalone or High Availability (HA)
  - Number and placement of nodes
  - Power fence (Linux HA only)
  - Reliability/resiliency requirements
- ACE applications requirements:
  - Applications to be deployed
  - ACE requirements (users, groups, service providers)
  - Hardware requirements
  - Software requirements

Integration checklist

Prior to the integration, document key solution parameters. Not all of the information applies to every solution being deployed; however, it is a best practice to document these parameters to reduce future rework.

Parameter	Assignment/Setting
Name of host server for Cisco Unified CM	
Cisco Unified CM login information Identify: - Host server IP address - User ID and password for the Cisco Unified CM	
Name of Cisco Unified CM Group - If there are multiple Cisco Unified CMs in the group, identify which is the primary Cisco Unified CM.	
Any devices that ACE will be configured to control - Type - IP address	

Solution overview

Introduction

Purpose

It is important to have a working knowledge of Cisco Unified Communications Manager (CM) operations and functiionality prior to integration with the Agile Communication Environment (ACE).This module provides an overview of the Cisco Unified CM solution, including standards and protocols, administration, IP Phone portfolio, and security. It also highlights how ACE and the Cisco Unified CM system interact.

Resources

Recommended resources are listed below.

- *Agile Communication Environment Overview (8672W)*
- *Agile Communication Environment Planning and Installation* (NN10850-004)
- *Agile Communication Environment Administration* (NN10850-005)
- *Agile Communication Environment Web Services* (NN10850-007)

Cisco Unified CM fundamentals

Cisco Unified Communications Manager is the software call-processing component of a Cisco Unified Communications solution. The Cisco Unified CM is hosted on a supported server and provides signaling and call-control services to Cisco and third-party applications. Cisco gateways enable communications with non-IP telecommunications devices.

The Cisco network can include one or more Cisco Unified CMs. The Cisco Unified CMs are organized logically by **groups**. A group can contain from one to three Cisco Unified CM systems, which are prioritized in a list. The first system is designated as primary, the second is secondary, and the third is backup.

IP Phones **register** to the primary Cisco Unified CM, which is configured to provide the call processing and signaling functions. In a multi-Cisco Unified CM network, if registration is not successful the IP Phones attempt to register to the next Cisco Unified CM in the group (secondary), and so on, until registration is successful.

IP Phones and other devices with common characteristics are organized logically into **device pools** for programming convenience. For example, IP Phones might be organized in device pools by bandwidth requirements. Intranet IP Phones might be assigned to a device pool configured for the G.711 CODEC, while extranet IP Phones might be assigned to a device pool configured for the G.729 CODEC.

Standards and protocols

Session Initiation Protocol

Session Initiation Protocol (SIP) allows IP-capable end points to create media sessions, such as phone calls, with each other. In a SIP environment, the signaling protocol is a peer-to-peer signaling protocol that creates, modifies, and terminates sessions over an IP network. SIP uses a media-description language and has a HyperText Transfer Protocol (HTTP)-like structure, which makes it easy to read and comprehend.

SIP clients traditionally use TCP and UDP port 5060 to connect to SIP endpoints, including SIP servers. Telephony systems use SIP in setting up and tearing down voice or video calls. However, SIP also offers session initiation for applications such as Event Subscription and Notification and Terminal mobility.

SIP is defined by the Engineering Task Force (IETF). For more information, go to www.ietf.org.

SIP core signaling services

SIP does exactly what its name implies: it allows two (or more) end points to initiate a media session, such as a phone call or video conference. To allow IP end points to create media sessions, SIP provides five core signaling services:

1 SIP allows end points to locate other end points. Those other end points can be on the same LAN, across the WAN, or they can be stationary or mobile. However, if you are placing a call on your IP Phone, SIP's job is to locate the person you are trying to reach.
2 SIP invites end points into sessions. Once SIP has located the other end point, it contacts that end point to determine whether that end point is willing to enter a session. If you are placing an IP phone call to another IP phone, SIP will make the phone at the other end ring. If the user picks up, he or she has accepted the session.
3 Once both end points have accepted the session, SIP allows those end points to exchange media information in order to establish the session. For a VoIP call this information includes messages about the CODECs the end points are going to use, and whether or not they use encryption and authentication. All this happens in a split-second: the end points connect to each other to figure out whether they can talk to each other before you hear the “Hello?” from the other end of the line.
4 SIP also allows you to modify existing sessions, such as allowing you to conference in a third person in the middle of your call.
5 SIP tears down existing sessions at the appropriate time. When you are in an IP-based call and you hang up, SIP sends a BYE message that ends the session.

CTI

Computer telephony integration (CTI) enables you to leverage computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database on the basis of information that caller ID provides. CTI applications can also enable you to use information that an interactive voice response (IVR) system captures, so the call can be routed to the appropriate customer service representative so the information is provided to the individual who is receiving the call.

JTAPI

Java Telephony Application Programming Interface (JTAPI) is a Java-based programming interface for computer telephony applications.

As defined by SearchNetworking.com: “JTAPI consists of a set of language packages. The core package provides the basic framework for simple Telephony processes such as placing a call, answering a call, and dropping a call. Several extension packages provide additional telephony features. JTAPI is interoperable across various computer platforms. JTAPI is similar to Microsoft and Intel's Telephony Application Programming Interface (TAPI). JTAPI was developed in 1996 by a working group of computer and telecommunications companies including Intel, Lucent, Nortel Networks, Novell, and Sun Microsystems.”

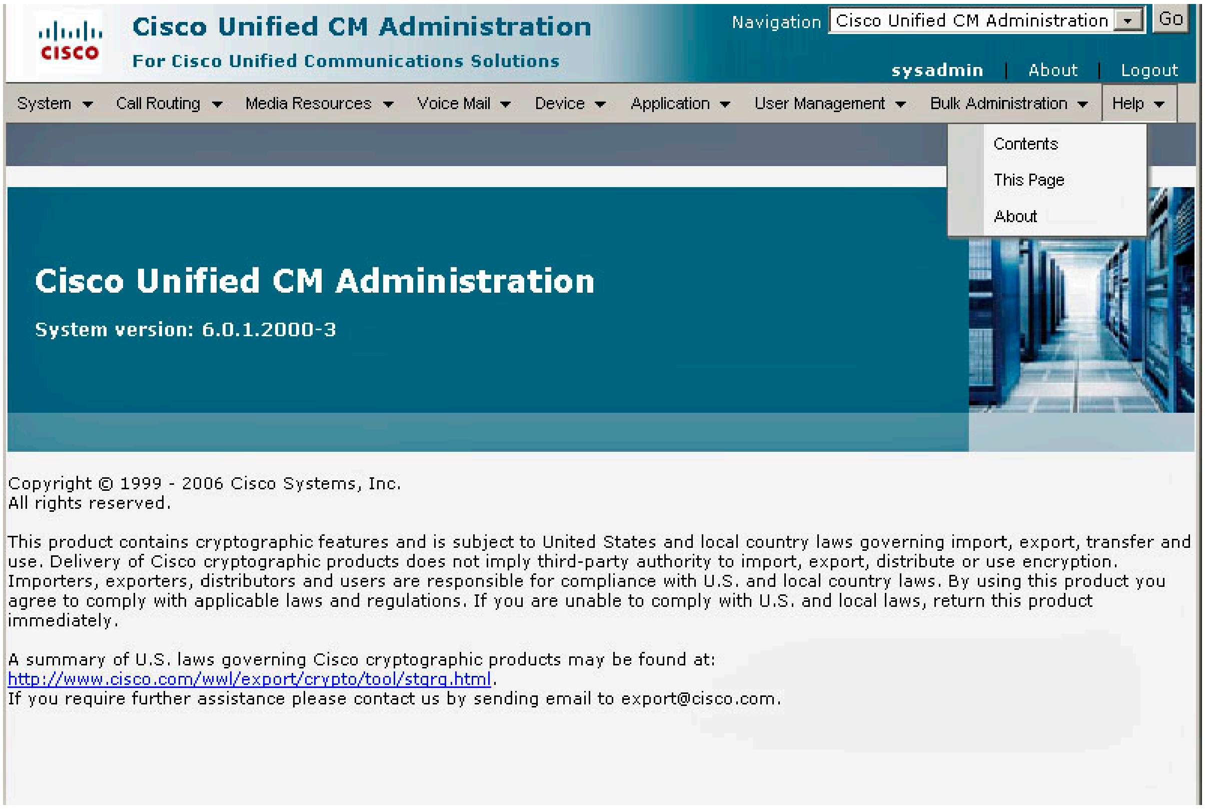
JTAPI is leveraged for selected web service because it is a more robust technology than SIP alone.

Administration

Description

The Cisco Unified Communications Manager (CM) software is installed on a supported server, which acts as the database server. The Cisco Unified Communications CM Administration web-based graphical user interface (GUI) is used for Operations, Administration, and Management (OAM) functions. Comprehensive online help is accessible from each page.

Important: Cisco Unified Communications CM Administration GUI is not accessed from the host server. It is accessed from a separate PC that is running a supported web browser.



Cisco Unified CM Administration

System version: 6.0.1.2000-3

Copyright © 1999 - 2006 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.
If you require further assistance please contact us by sending email to export@cisco.com.

Cisco IP Phones

Description

It is assumed that the IP Phones that ACE will control are already configured and operational. It is important, however, to have a basic understanding of the Cisco Unified IP Phone types, operation, and administration. This section provides a brief overview.

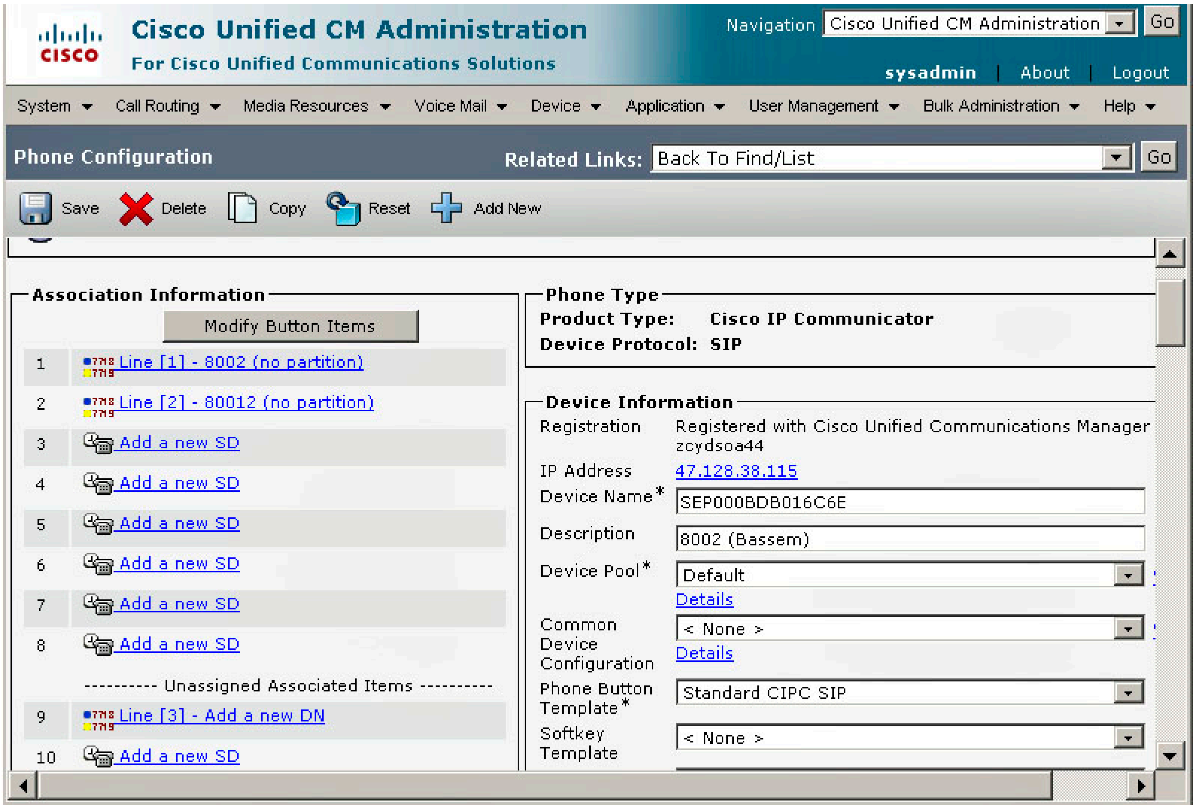
Cisco Unified IP Phones use the customer IP data network to communicate with the Cisco Unified CM. These devices are added to the Cisco Unified CM database manually or automatically using the auto-registration function. Note that the auto-registration is recommended only in small configurations or testing lab.

The Cisco Unified IP Phone portfolio includes a wide range of devices, including third-party SIP phones, H.323 clients, and CTI ports used for Cisco virtual devices (such as the Cisco SoftPhone and Cisco Unified Auto-Attendant), the Cisco ATA 186 telephone adapter, and the Cisco IP Communicator.

Cisco Unified IP Phones register to the primary Cisco Unified CM, which is configured to provide the call processing and signaling functions. In a multi-Cisco Unified CM network, if registration is not successful the IP Phones attempt to register to the next Cisco Unified CM in the group (secondary), and so on, until registration is successful.

Cisco phone administration

Cisco phones are configured using the Cisco Unified CM interface. Many fields are preconfigured with common settings that can be changed, as needed.



Phone Configuration

Related Links: Back To Find/List

Association Information

Modify Button Items

1 Line [1] - 8002 (no partition)
2 Line [2] - 80012 (no partition)
3 Add a new SD
4 Add a new SD
5 Add a new SD
6 Add a new SD
7 Add a new SD
8 Add a new SD

---------- Unassigned Associated Items ----------

9 Line [3] - Add a new DN
10 Add a new SD

Phone Type

Product Type: Cisco IP Communicator
Device Protocol: SIP

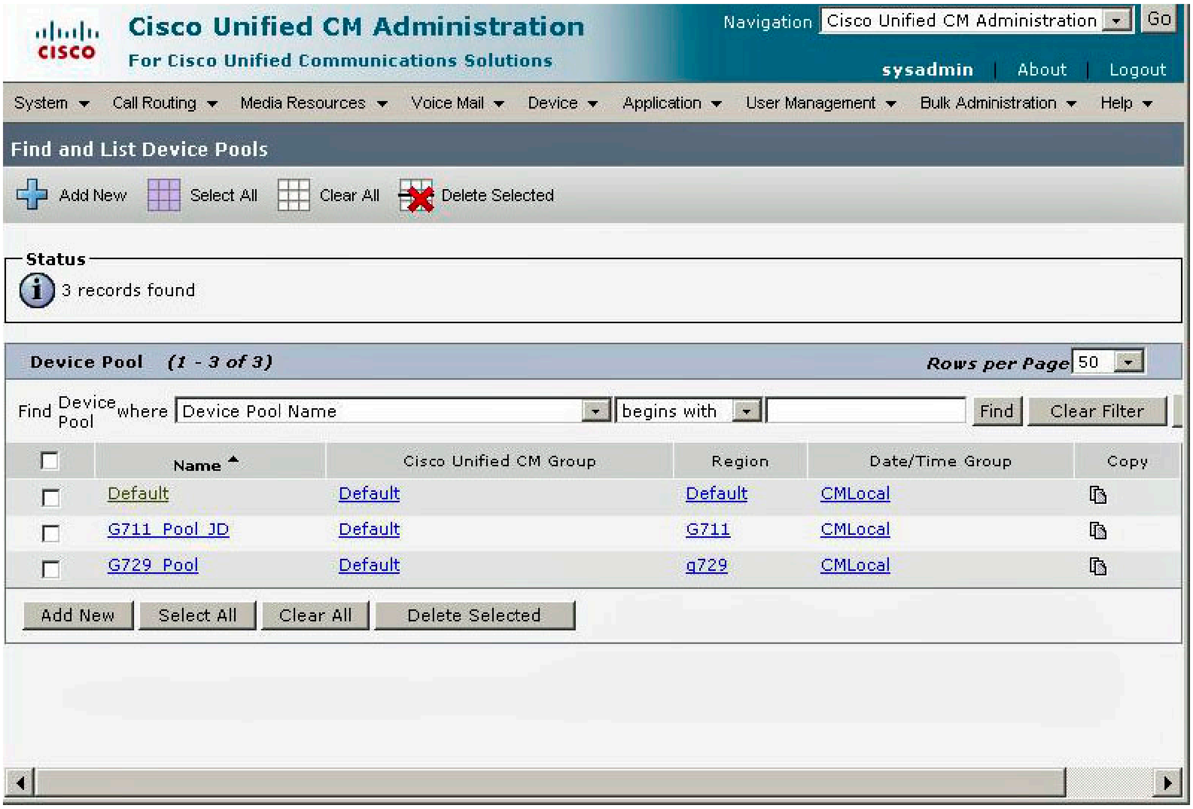
Device Information

Registration	Registered with Cisco Unified Communications Manager zcydsoa44
IP Address	47.128.38.115
Device Name*	SEP000BDB016C6E
Description	8002 (Bassem)
Device Pool*	Default Details
Common Device Configuration	< None > Details
Phone Button Template*	Standard CIPC SIP
Softkey Template	< None >

Cisco Unified CM device pools

IP Phones and other devices with common characteristics are organized logically into device pools for programming convenience. In the example, there are three device pools:

- **G711_Pool_JD**: Configured for devices that use the G711 CODEC, which is typically used for intranetwork calls
- **G729**: Configured for devices that use the G729 CODEC, which is typically used for internetwork calls
- **Default**: Configured for all remaining devices



Find and List Device Pools

Status
3 records found

Device Pool (1 - 3 of 3)   Rows per Page 50

Find Device Pool where Device Pool Name begins with

□	Name	Cisco Unified CM Group	Region	Date/Time Group	Copy
□	Default	Default	Default	CMLocal	⧉
□	G711_Pool_JD	Default	G711	CMLocal	⧉
□	G729_Pool	Default	g729	CMLocal	⧉

Security

Description

The ACE solution deployed in a private internal network that is protected through the web server in the demilitarized zone (DMZ). An HTTPS interface is supported between ACE and the web servers connected through the Web Services interface. Data is encrypted and ACE server authentication is provided to the clients over this interface.

The Service Provider interfaces do not need to be secured, as long as the enterprise internal network is considered a trusted network. The network servers on the Service Provider interface are also located in the internal network and isolated though firewalls/network address translation (NAT) and/or Session Border Controllers (SBCs).

The port assignments that the customer can use to set up the firewall rules/NAT equipment are described in *Nortel Agile Communication Environment Planning and Installation* (NN10850-004).

SIP trunk security

Cisco Unified CM Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings. You apply the configured settings to the SIP trunk when you choose the security profile in the Trunk Configuration window.

Installing Cisco Unified Communications Manager provides a predefined, non secure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a non secure profile.

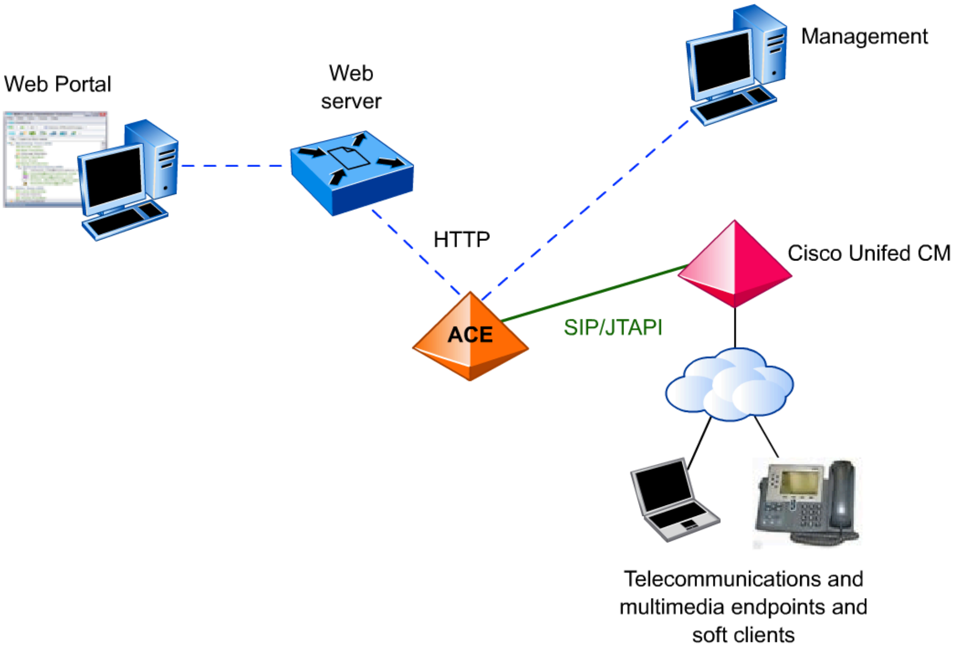
Only security features that the SIP trunk supports display in the security profile settings window.

Tip	It is assumed that the existing customer infrastructure has been engineered in accordance with established corporate security practices.

How ACE and the Cisco Unified CM interact

Example Cisco Unified CM deployment

The figure provides a simplified view of a Cisco Unified CM deployment.



Basic Cisco Unified CM configuration

Introduction

Purpose

Prior to integration with the Agile Communication Environment (ACE), the Cisco Unified Communications solution must be installed, configured correctly, and fully operational.

This module reviews baseline configuration requirements that must be met and provides information on how to confirm that the Cisco Unified Communications solution meets the baseline configuration requirements.

Cisco Unified CM baseline checklist

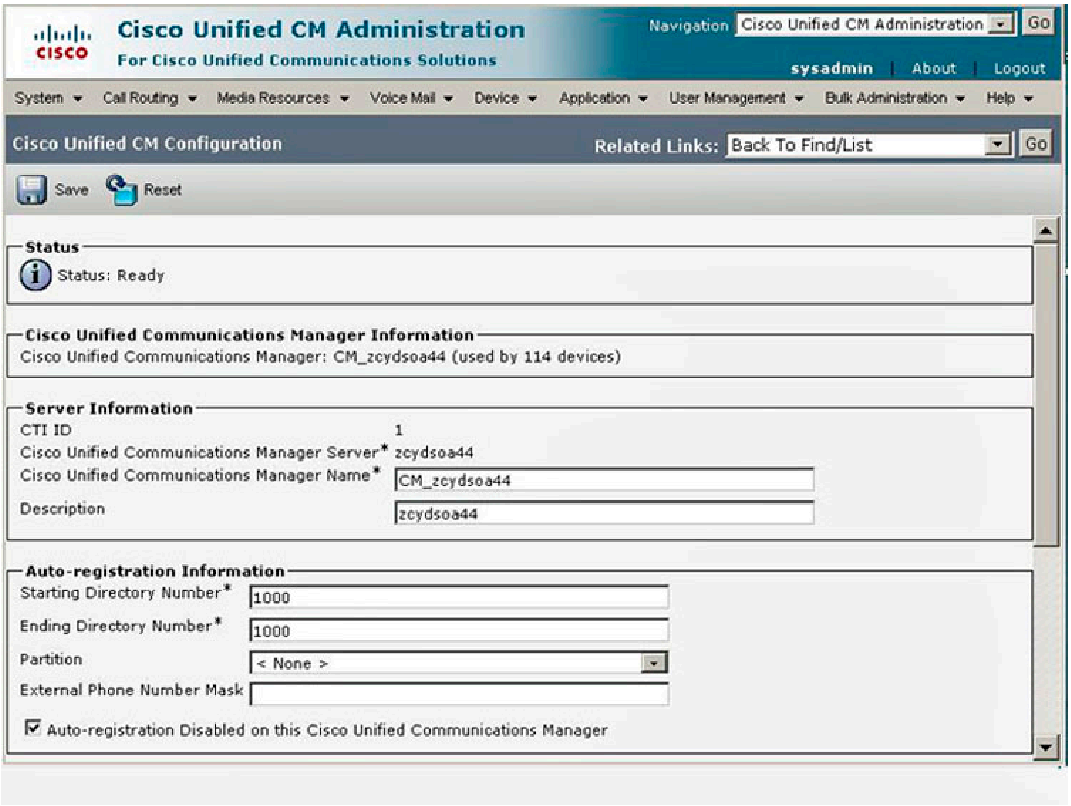
X	Requirement	Comments
	Identify Cisco Unified CM configuration parameters, such as server host.	From Cisco Unified CM interface, select **System - Cisco Unified CM - Server**.
	Identify the Cisco Unified CM Group to which Cisco IP Phones register.	From Cisco Unified CM interface, select **System - Cisco Unified CM**.
	Identify device pools to which any ACE controlled IP Phones belong.	From Cisco Unified CM interface, select **System -Device Pools**.
	Verify that Cisco Unified CM Release 6.0 or higher software is required.	From Cisco Unified CM interface, select **System - Licensing**.

Cisco Unified CM base configuration

Cisco Unified CM configuration

The Cisco Unified CM Configuration window displays basic confirmation parameters for a selected Cisco Unified CM.

The windows shows the configuration for the Cisco Unified CM that is hosted on the server **zcydsoa44**. From this example, you can see that 114 devices register to Cisco Unified CM. The Computer Telephony Integration (CTI) is configured, and that autoregistration of new phones (automatic assignment of Directory Number) is disabled.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Related Links: Back To Find/List Go
Save Reset

Cisco Unified CM Configuration

Status

Status: Ready

Cisco Unified Communications Manager Information

Cisco Unified Communications Manager: CM_zcydsoa44 (used by 114 devices)

Server Information

CTI ID 1
Cisco Unified Communications Manager Server* zcydsoa44
Cisco Unified Communications Manager Name* CM_zcydsoa44
Description zcydsoa44

Auto-registration Information

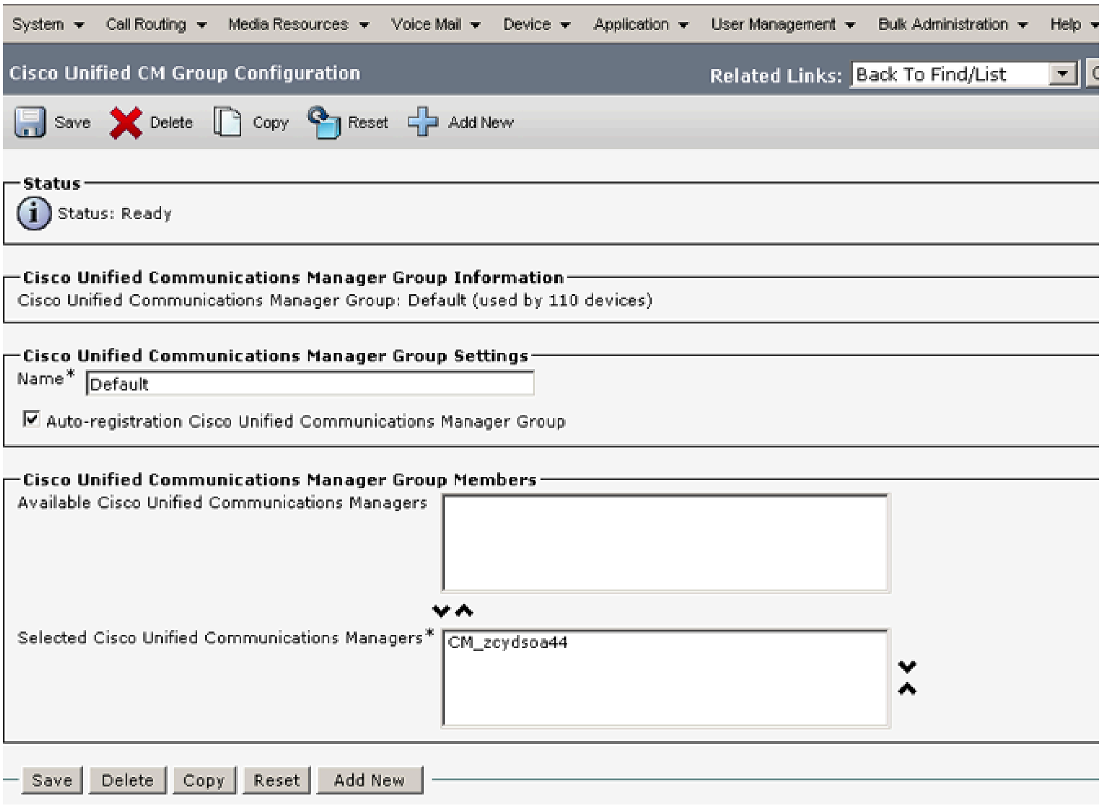
Starting Directory Number* 1000
Ending Directory Number* 1000
Partition < None >
External Phone Number Mask

☑ Auto-registration Disabled on this Cisco Unified Communications Manager

Cisco Unified CM group configuration

The Cisco network can include one or more Cisco Unified CMs. The Cisco Unified CMs are organized logically by groups. A group can contain from one to three Cisco Unified CM systems, which are prioritized in a list. The first system is designated as primary, the second is secondary, and the third is backup.

In the example, the group has one Cisco Unified CM. Assigned devices register to this Cisco Unified CM.



Cisco Unified CM Group Configuration

Status

Status: Ready

Cisco Unified Communications Manager Group Information

Cisco Unified Communications Manager Group: Default (used by 110 devices)

Cisco Unified Communications Manager Group Settings

Name* Default

☑ Auto-registration Cisco Unified Communications Manager Group

Cisco Unified Communications Manager Group Members

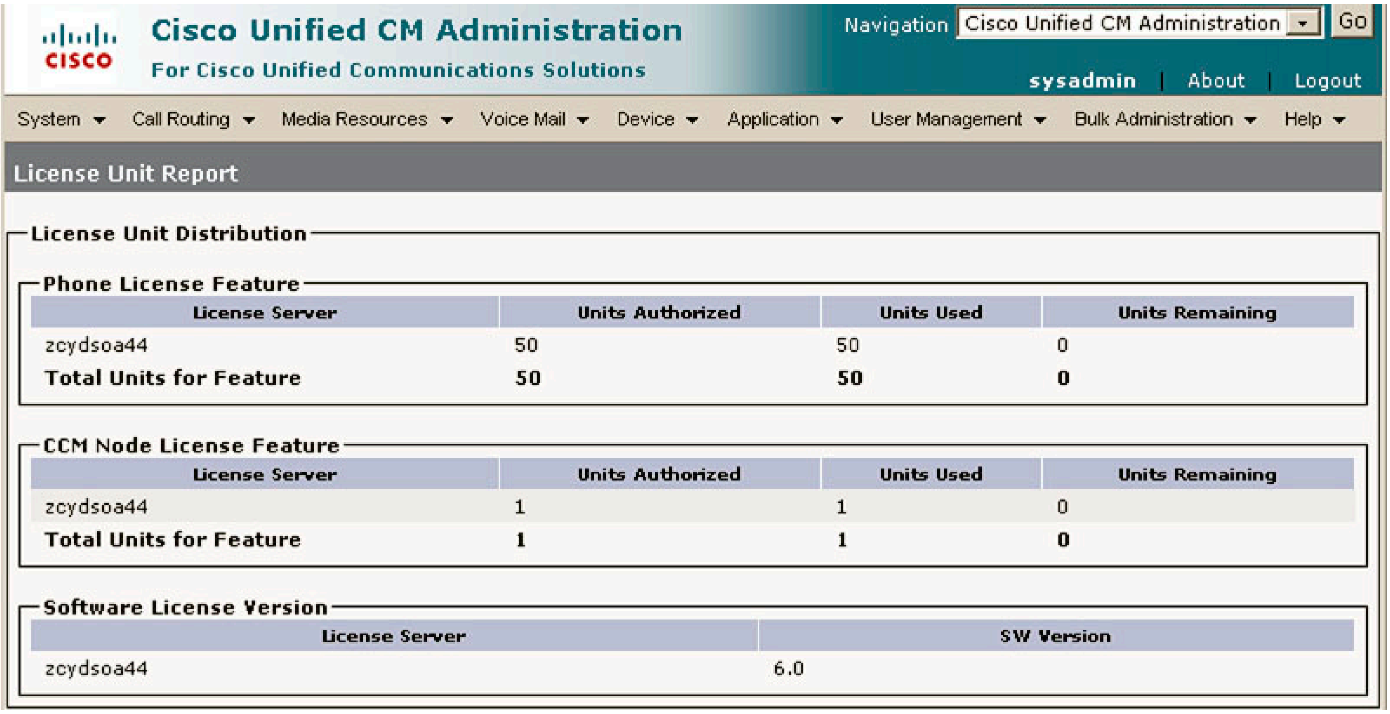
Available Cisco Unified Communications Managers

Selected Cisco Unified Communications Managers* CM_zcydsoa44

Cisco Unified CM License Unit Report

When deploying a solution, it is important to make sure that the system software issue and release meets the minimum requirement for the solution. The Cisco Unified CM License Unit Report window displays the number of equipped software release. It also displays the authorized, used and remaining number of phone and node licenses.

The following Cisco Unified CM License Unit Report shows that the Release 6.0 software is installed, which ACE requires at a minimum. The other parameters are for Cisco engineering purposes and are relevant for ACE integration planning.



License Unit Report

License Unit Distribution

Phone License Feature

License Server	Units Authorized	Units Used	Units Remaining
zcydsoa44	50	50	0
Total Units for Feature	**50**	**50**	**0**

CCM Node License Feature

License Server	Units Authorized	Units Used	Units Remaining
zcydsoa44	1	1	0
Total Units for Feature	**1**	**1**	**0**

Software License Version

License Server	SW Version
zcydsoa44	6.0

Standard SIP solutions

Introduction

Purpose

This module reviews Cisco Unified CM configuration guidelines for the following ACE services, which require the CCM SIP service provider. For detailed support requirements, see *Agile Communication Environment Administration* (NN10850-005).

CCM SIP service provider fundamentals

The ACE CCM SIP service provider is used for services where the ACE acts as the Back-to-Back User Agent (B2BUA) for both ends of a Session Initiation Protocol (SIP) call. The CCM SIP service provider enables ACE to facilitate calls between endpoints, from call establishment to termination. B2BUA is defined in Request for Comments (RFC) 3261, SIP: Session Initiation Protocol. For more information, see the Internet Engineering Task Force website, www.ietf.org.

Third Party Call Control (v3) requires a media terminal to provide call treatment, such as announcements used for ringback tone and recorded announcements. The supported media terminal is the Interactive Communications Portal (ICP). ICP is a software solution that supports SIP for call processing and signaling, as well as multimedia conferencing for audio and video streams in large and small conferences. For more information, see *Media Application Server and Interactive Communications Portal Fundamentals* (NN44471-101).

SIP checklist

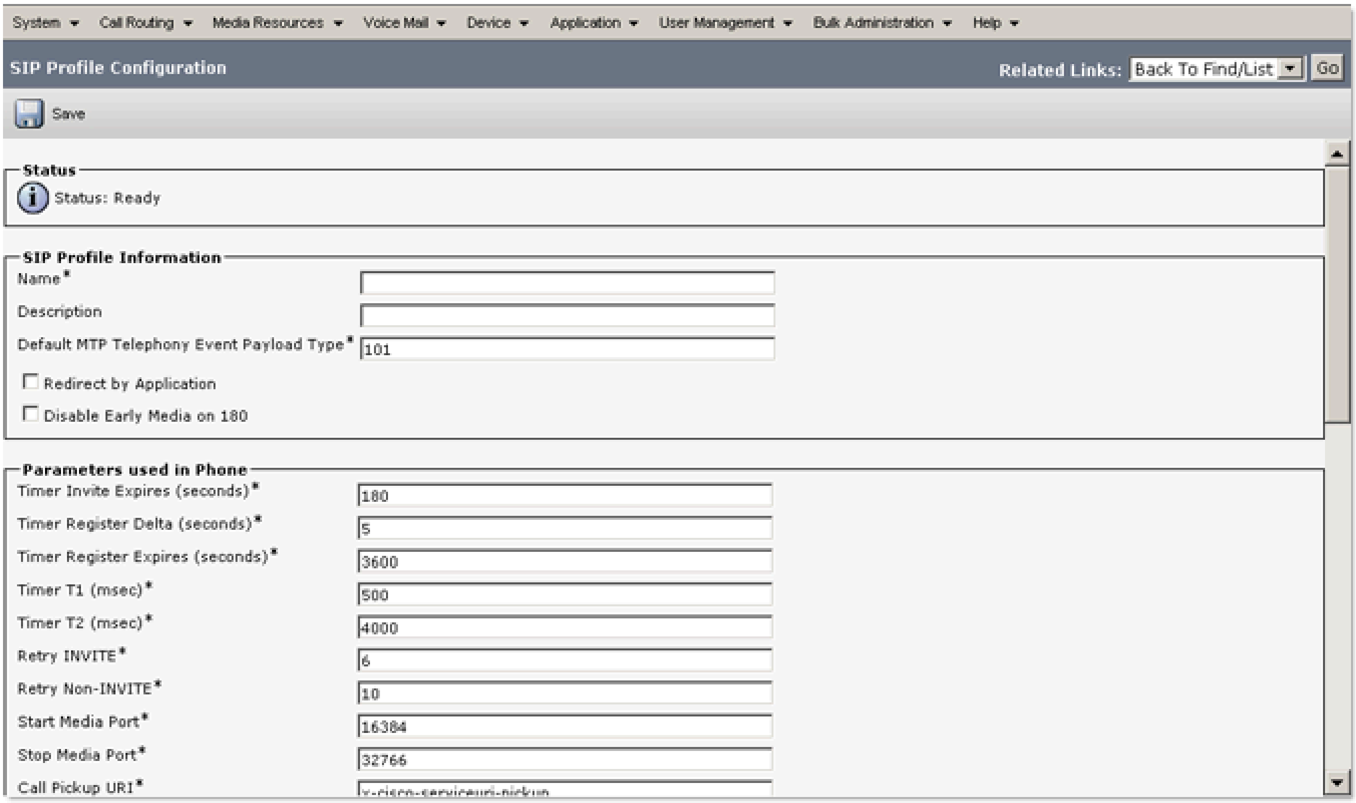
X	Parameter	Comments
	Create a SIP Profile.	A SIP profile is a programming convenience. Rather than assign SIP attributes to each SIP trunk, you can create a SIP profile that defines common SIP attributes and assigns the profile to applicable SIP trunks. From the Cisco Unified CM interface, select **Device - Device Settings - SIP Profile**.
	Create a SIP trunk security profile.	Each SIP trunk is assigned a SIP trunk security profile during the configuration process. This profile defines security attributes, such as transport type, security mode, and authentication and authorization settings for incoming SIP messages. From the Cisco Unified CM interface, select **System - Security Profile - SIP Trunk Security Profile**.
	Create a SIP trunk for ACE.	With a standard SIP solution, ACE connects to the Cisco Unified CM network via SIP trunk. Note that ACE does not connect directly to Cisco Unified CM. The SIP trunk connects to a SIP proxy server, which is connected to the Cisco Unified CM. When configuring a SIP trunk, pay special attention to Information. Make sure **Media Termination Point** is **disabled** (no check mark). ACE is not actually sending media, so the injection of media points does not apply. From the Cisco Unified CM interface, select **Device - Trunk**.
	Configure SIP route pattern.	SIP Route Patterns determine call routing and blocking. Assign domain/IP address and SIP Trunk, and transformational rules that are appropriate for your ACE solution. From the Cisco Unified CM interface, select **Call Routing - SIP Route Pattern**.

Configure SIP trunk for ACE

SIP profile

SIP profiles are a programming convenience that enable you to assign common SIP attributes to devices; for example, timers, Universal Resource Indicators (URI) for call features (Call Pickup, Meet Me, Call Forward, Abbreviated Dial, etc.), Start and Stop Media Ports.

SIP profiles are created from the Cisco Unified CM interface (**Device - Device Settings - SIP Profile** - **Add New**). Many fields are pre-populated with default settings suitable for many SIP solutions. The SIP profile contains some standard entries that cannot be deleted or changed.



SIP Profile Configuration

Status

Status: Ready

SIP Profile Information

Name*	
Description	
Default MTP Telephony Event Payload Type*	101

☐ Redirect by Application

☐ Disable Early Media on 180

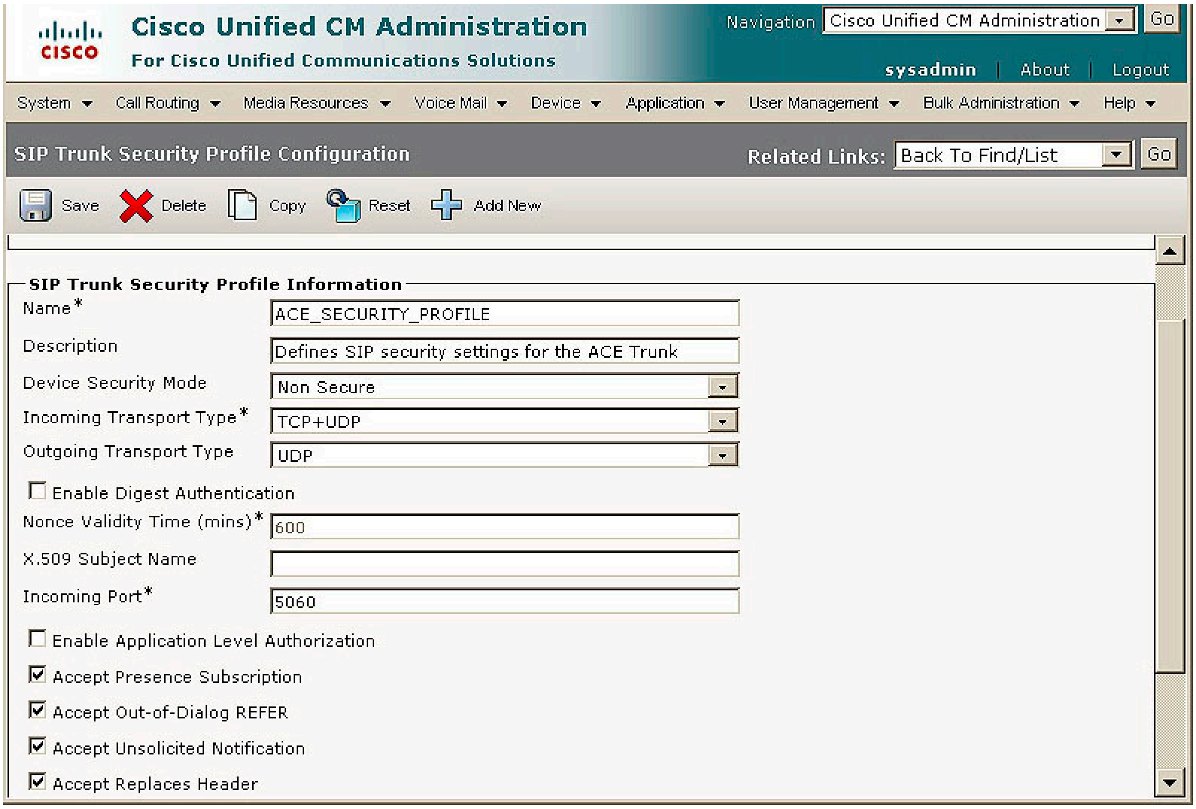
Parameters used in Phone

Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	5
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup

SIP trunk security profile

Each SIP trunk must be assigned a SIP trunk security profile, created previously using the Cisco Unified CM interface (**System - Security Profile - SIP Trunk Security Profile** - **Add New**).

By default, the window is pre-populated with settings that are suitable for many solutions. Commonly addressed fields are highlighted in the example. Pay special attention to the Device Security Mode field. Choose the setting appropriate for your environment.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System
Call Routing
Media Resources
Voice Mail
Device
Application
User Management
Bulk Administration
Help
Related Links: Back To Find/List Go
Save
Delete
Copy
Reset
Add New

SIP Trunk Security Profile Configuration

SIP Trunk Security Profile Information

Name* ACE_SECURITY_PROFILE

Description Defines SIP security settings for the ACE Trunk

Device Security Mode Non Secure

Incoming Transport Type* TCP+UDP

Outgoing Transport Type UDP

□ Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name

Incoming Port* 5060

□ Enable Application Level Authorization

☑ Accept Presence Subscription

☑ Accept Out-of-Dialog REFER

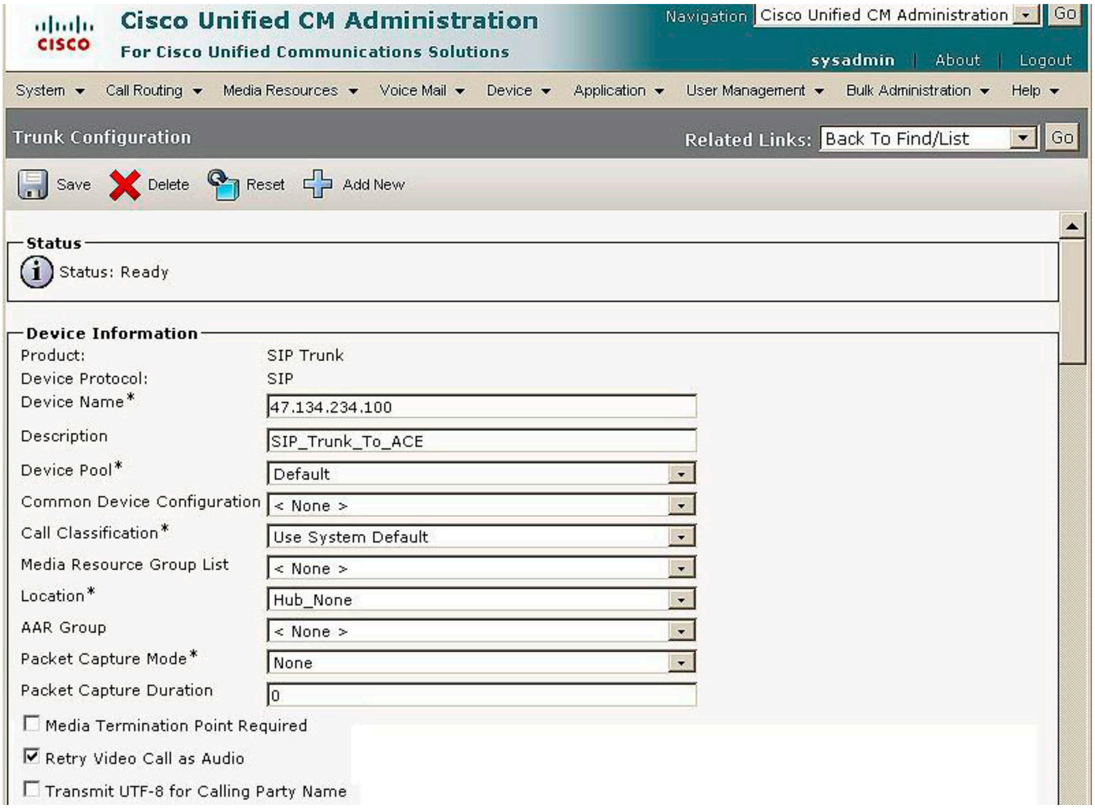
☑ Accept Unsolicited Notification

☑ Accept Replaces Header

SIP trunks

SIP trunks are created using the Cisco Unified CM interface (**Device - Trunk** - **Add New**). The window is divided into multiple sections. Many trunk configuration fields have pre-defined settings that are suitable for many SIP environments but can be changed, as needed.

Important: In the Device Information section (shown below), make sure **Media Termination Point** is **disabled** (no check mark). ACE is not actually sending media, so this the injection of media points does not apply.



Status

Status: Ready

Device Information

Product: SIP Trunk

Device Protocol: SIP

Device Name* 47.134.234.100

Description SIP_Trunk_To_ACE

Device Pool* Default

Common Device Configuration < None >

Call Classification* Use System Default

Media Resource Group List < None >

Location* Hub_None

AAR Group < None >

Packet Capture Mode* None

Packet Capture Duration 0

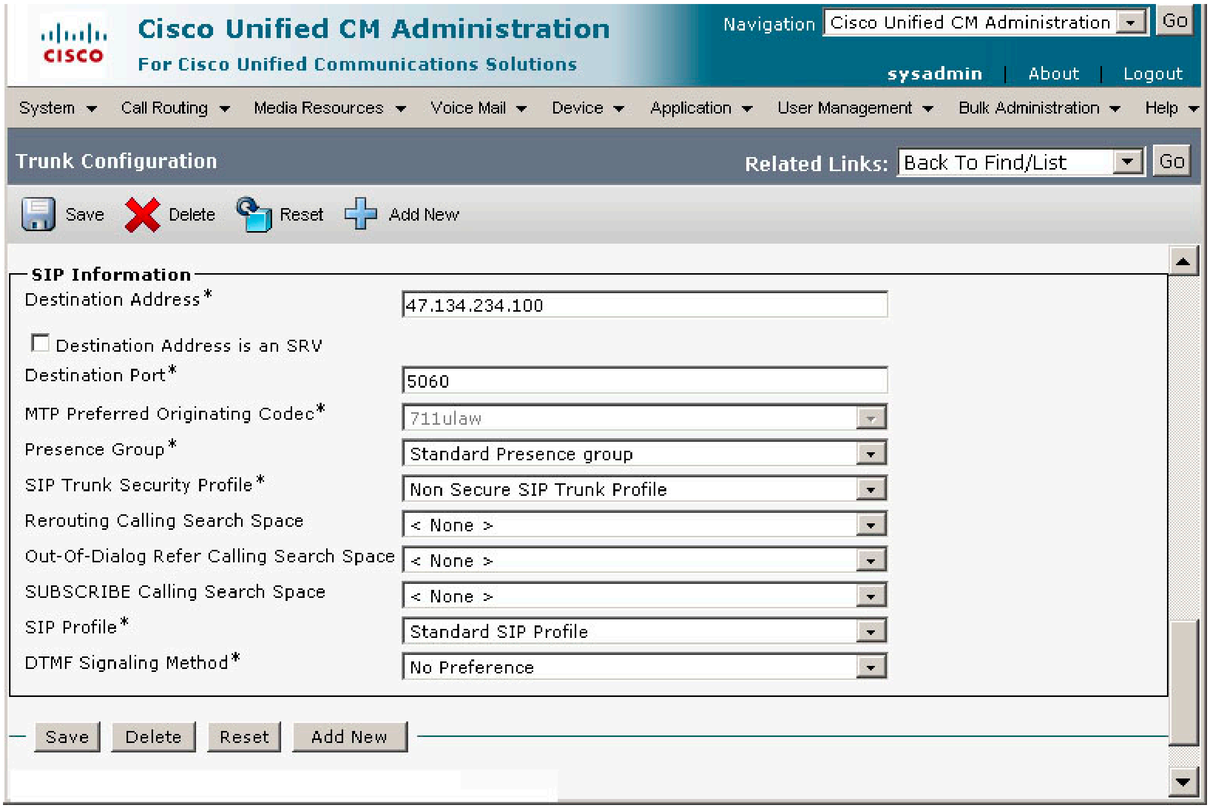
☐ Media Termination Point Required

☑ Retry Video Call as Audio

☐ Transmit UTF-8 for Calling Party Name

SIP trunks - continued

Within the SIP Information section, be sure to assign the appropriate SIP Profile and SIP Trunk Security Profile (defined previously).



Trunk Configuration

SIP Information

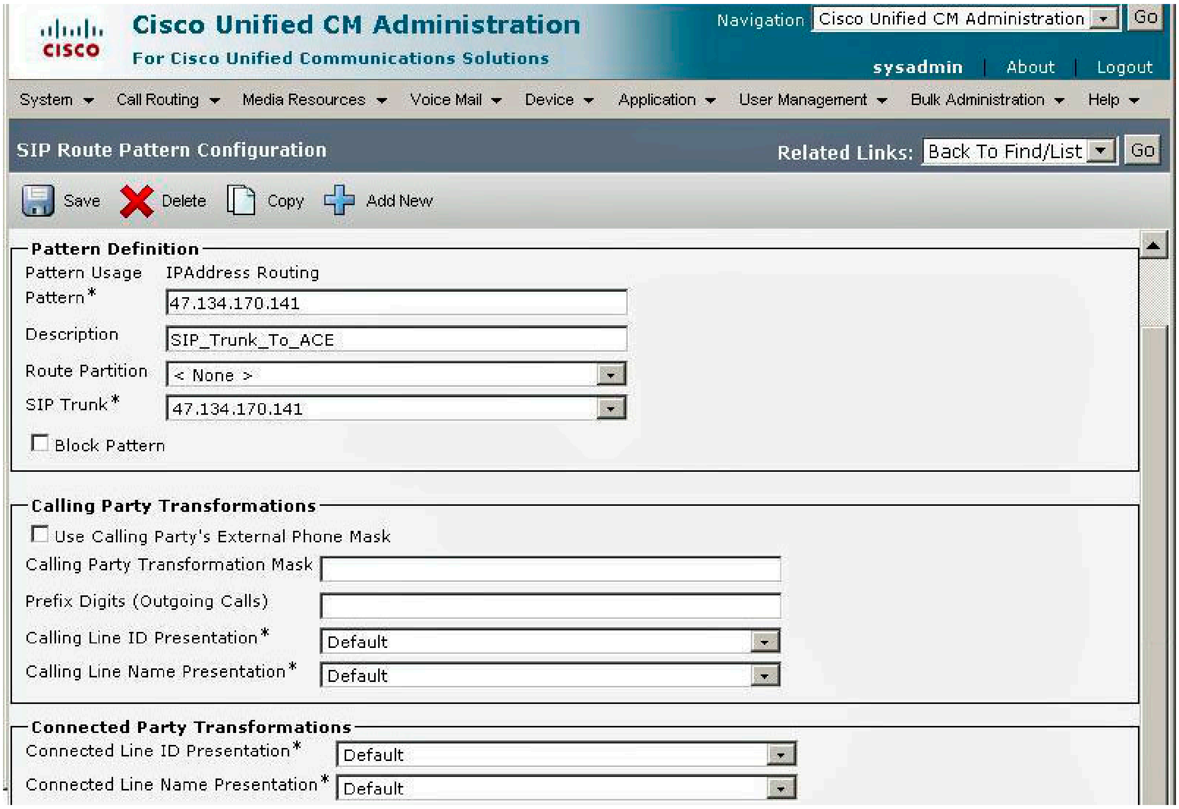
Destination Address*	47.134.234.100
□ Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

SIP Route Pattern

The SIP Cisco Unified CM refers to SIP Route Patterns to determine call routing and blocking. As part of the SIP Route Pattern configuration, a domain name/IP address is associated with a specific SIP trunk. Calls presented to this domain name/IP address are routed through the specified SIP trunk.

SIP Route Patterns are configured using the Cisco Unified CM Administration interface (**Call Routing - SIP Route Pattern - Add New**. Some commonly addressed SIP Route Pattern parameters are:

- **Pattern Usage**: Domain routing or IP Address routing (mandatory)
- **Pattern**: Domain, sub-domain, IP address, or IP subnetwork (mandatory)
- **Description**: Description of route pattern (optional)
- **SIP Trunk**: SIP trunk to which the SIP route pattern is associated (mandatory)
- **Important**: You must configure at least one SIP Profile and SIP Trunk before you can configure a SIP route pattern


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Related Links: Back To Find/List Go
Save Delete Copy Add New

SIP Route Pattern Configuration

Pattern Definition

Pattern Usage IPAddress Routing
Pattern* 47.134.170.141
Description SIP_Trunk_To_ACE
Route Partition < None >
SIP Trunk* 47.134.170.141
□ Block Pattern

Calling Party Transformations

□ Use Calling Party's External Phone Mask
Calling Party Transformation Mask
Prefix Digits (Outgoing Calls)
Calling Line ID Presentation* Default
Calling Line Name Presentation* Default

Connected Party Transformations

Connected Line ID Presentation* Default
Connected Line Name Presentation* Default

JTAPI solutions

Introduction

Purpose

This modules reviews Cisco Unified CM configuration guidelines for the Agile Communication Environment (ACE) Call services, which require JTAPI.

The CCM JTAPI service provider is used for services where the ACE controls a Computer Telephony Integration (CTI)-capable terminal on the Cisco Unified CM system. This enables ACE to send control messages to the terminal to perform various functions, such as establish calls and obtain presence information.

For detailed support requirements, see *Agile Communication Environment Administration* (NN10850-005).

JTAPI checklist

X	Parameter	Value
	Verify that the CTI service is running.	The CTI Manager is installed automatically with the deployment of the Cisco Unified Communications Manager. Verify that the CTI service is running. From the Cisco Unified CM interface, select **System - Service Parameters**.
	Verify that the ACE controlled devices are configured to support CTI control operations.	Make sure that All Control of Device from CTI is enabled. From the Cisco Unified CM interface, select **System - Device - Phone Configuration**.
	Define ACE is as Application User that can control CTI devices, and assign controlled devices.	From the Cisco Unified CM interface, select **User Management - Application User**.

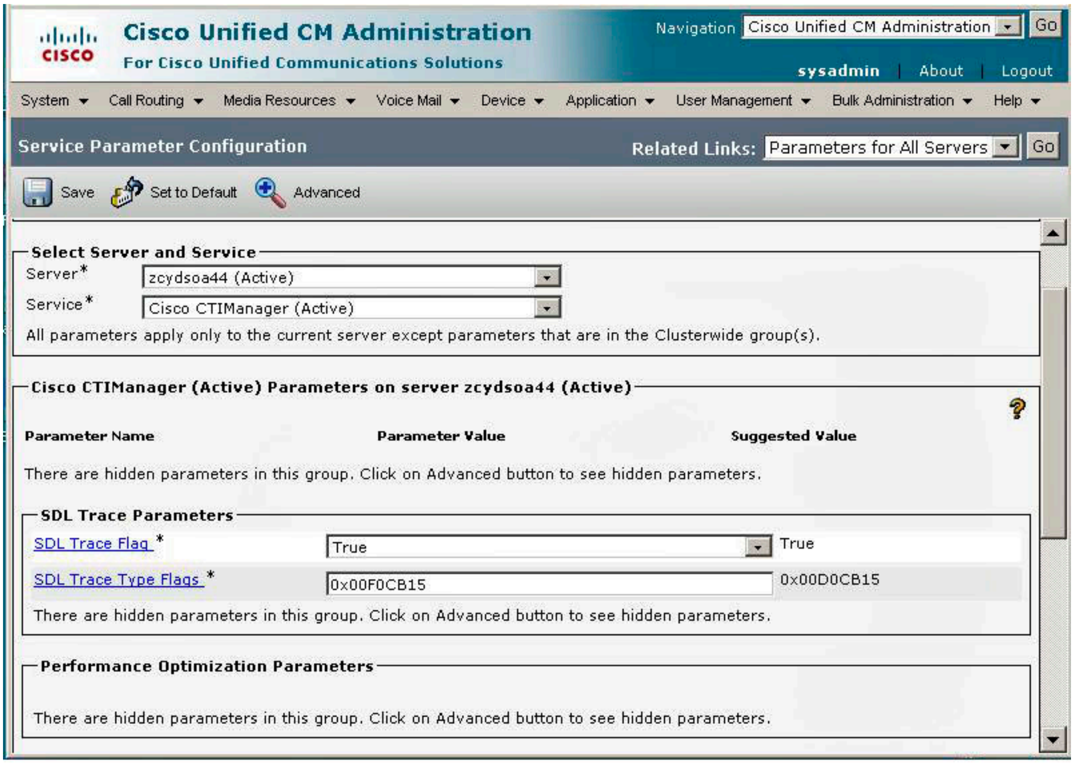
Configure CTI services for ACE

CTI Manager

Within the Cisco Unified CM network, a special software program called the CTI Manager provides the interface for CTI applications. The CTI Manager is installed automatically during the initial setup of the Cisco Unified CM.

To verify that the service is active, select **System - Service Parameters** and then select **Cisco CTI Manager** from the Service drop list. In the example, the Cisco CTI Manager is active.

Service Parameter Configuration - CTI Manager


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Service Parameter Configuration
Related Links: Parameters for All Servers Go
Save Set to Default Advanced

Select Server and Service

Server* zcydsoa44 (Active)

Service* Cisco CTIManager (Active)

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

Cisco CTIManager (Active) Parameters on server zcydsoa44 (Active)

Parameter Name	Parameter Value	Suggested Value

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

SDL Trace Parameters

SDL Trace Flag *	True	True
SDL Trace Type Flags *	0x00F0CB15	0x00D0CB15

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

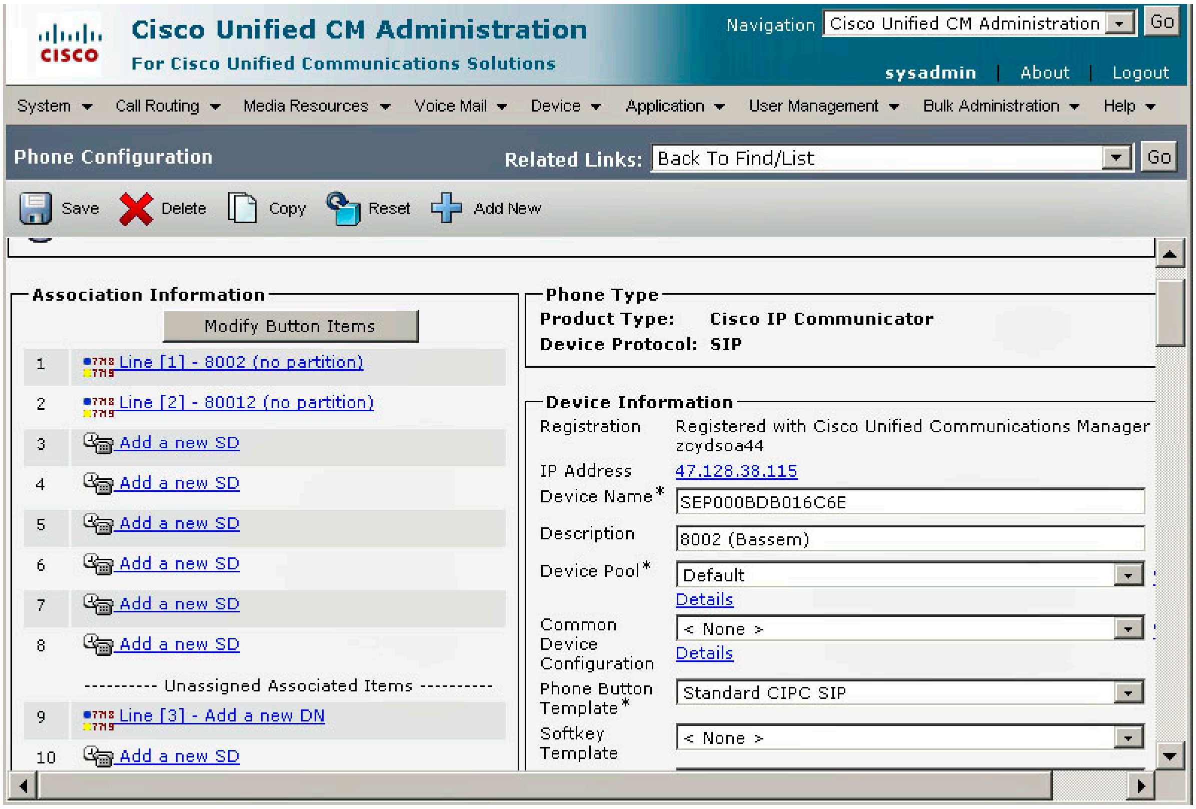
Performance Optimization Parameters

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Allow Control of Device from CTI

The **Allow Control of Device from CTI** option must be enabled on each device (phone) that ACE will monitor and control; for example, a Cisco Unified Personal Communicator softphone. To verify the phone's configuration, complete these steps from the Cisco Unified CM interface.

1. Select **Device - Phone**. The Find and List Phones window appears.
2. Select a device from window; for example, a **CICP** (Cisco IP Communicator). A corresponding page appears.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Add New
Modify Button Items

Association Information

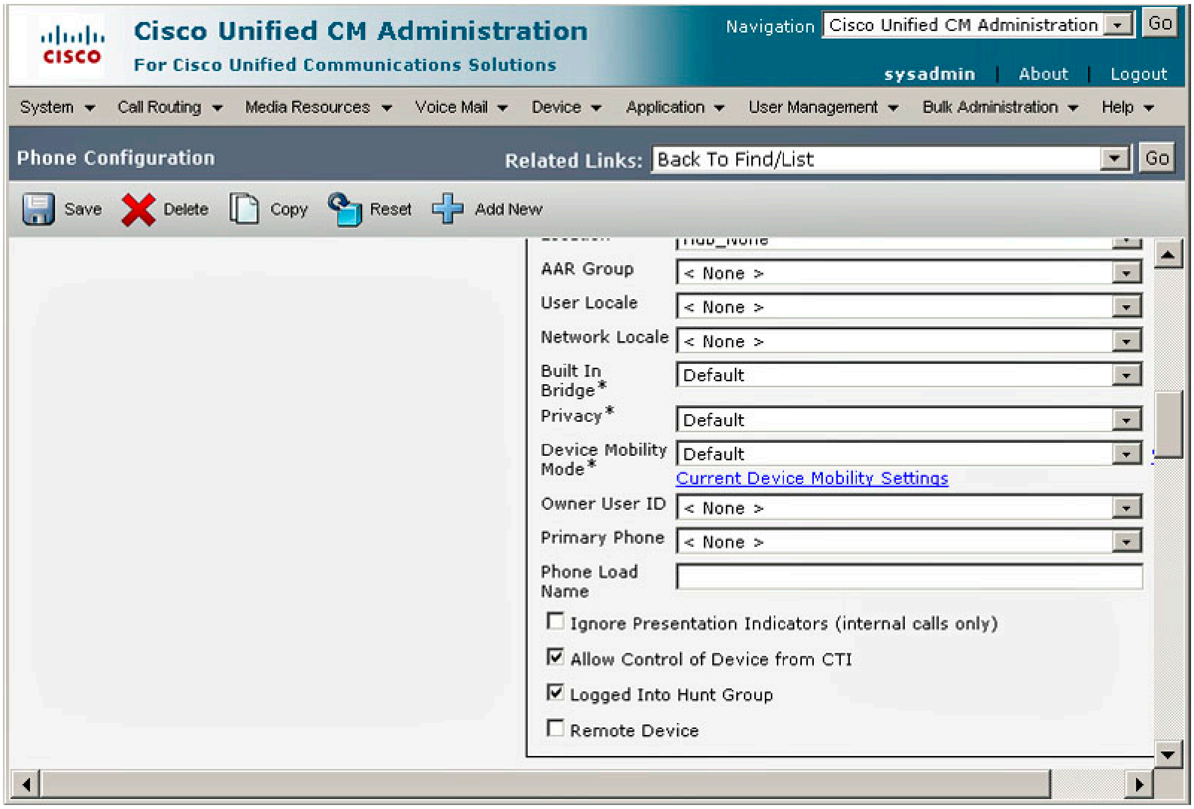
1	Line [1] - 8002 (no partition)
2	Line [2] - 80012 (no partition)
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
7	Add a new SD
8	Add a new SD
	---------- Unassigned Associated Items ----------
9	Line [3] - Add a new DN
10	Add a new SD

Phone Type
Product Type: Cisco IP Communicator
Device Protocol: SIP

Device Information

Registration	Registered with Cisco Unified Communications Manager zcydsoa44
IP Address	47.128.38.115
Device Name*	SEP000BDB016C6E
Description	8002 (Bassem)
Device Pool*	Default Details
Common Device Configuration	< None > Details
Phone Button Template*	Standard CIPC SIP
Softkey Template	< None >

3. Scroll to the bottom of the Device Information section, and verify that the **Allow Control of Device from CTI** box is checked.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System
Call Routing
Media Resources
Voice Mail
Device
Application
User Management
Bulk Administration
Help
Phone Configuration
Related Links: Back To Find/List Go
Save
Delete
Copy
Reset
Add New

AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Privacy*	Default
Device Mobility Mode*	Default Current Device Mobility Settings
Owner User ID	< None >
Primary Phone	< None >
Phone Load Name	

□ Ignore Presentation Indicators (internal calls only)

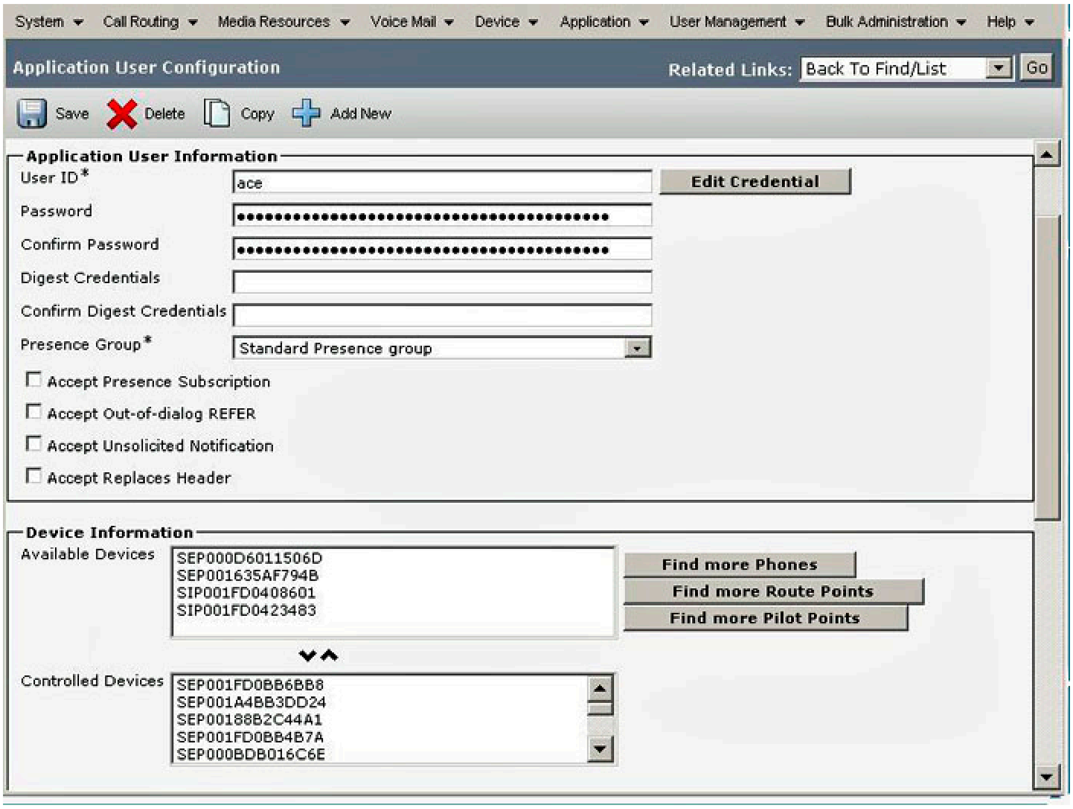
☑ Allow Control of Device from CTI

☑ Logged Into Hunt Group

□ Remote Device

ACE Application User

Configure ACE as Application User using the Unified CM interface (**User Management** - **Application User**). The Application User Configuration window is divided into multiple sections. In the top section, Application User Information, enter general information about ACE.



Application User Configuration

Application User Information

User ID* ace

Password ••

Confirm Password ••

Digest Credentials

Confirm Digest Credentials

Presence Group* Standard Presence group

☐ Accept Presence Subscription

☐ Accept Out-of-dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

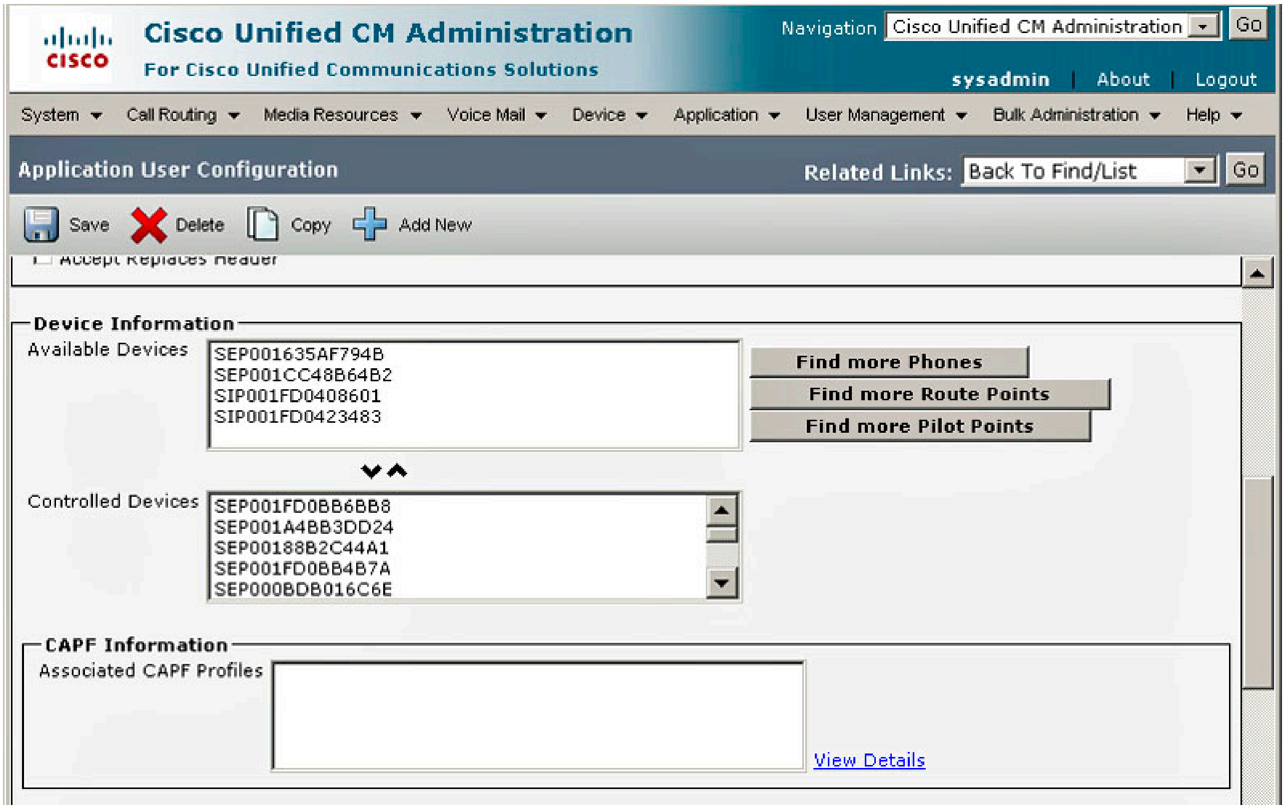
Device Information

Available Devices
SEP000D6011506D
SEP001635AF794B
SIP001FD0408601
SIP001FD0423483

Controlled Devices
SEP001FD0BB6BB8
SEP001A4BB3DD24
SEP00188B2C44A1
SEP001FD0BB4B7A
SEP000BDB016C6E

Device Information

In the Device Information section of the Application User Configuration window, assign the devices (IP Phones) that are ACE controlled.



Accept Replaces Header

Device Information

Available Devices: SEP001635AF794B, SEP001CC48B64B2, SIP001FD0408601, SIP001FD0423483

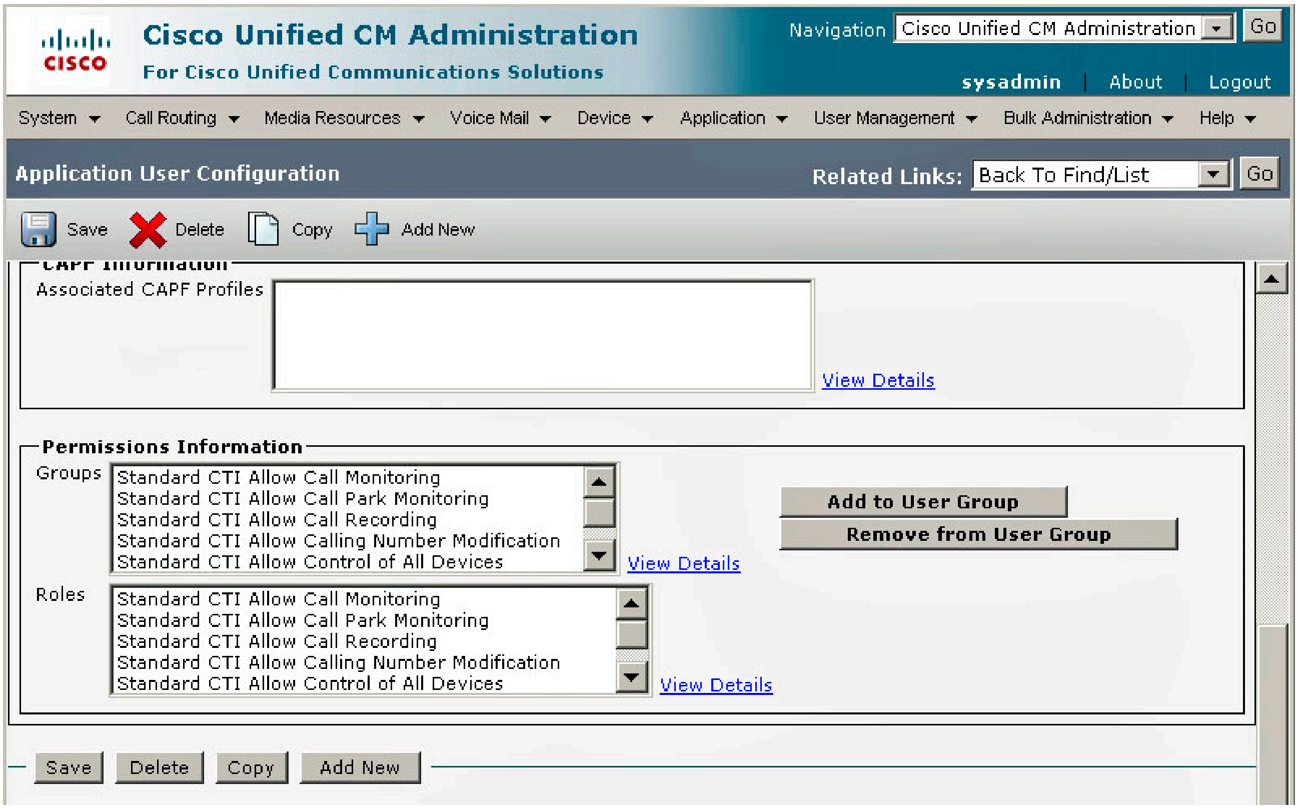
Controlled Devices: SEP001FD0BB6BB8, SEP001A4BB3DD24, SEP00188B2C44A1, SEP001FD0BB4B7A, SEP000BDB016C6E

CAPF Information

Associated CAPF Profiles

Permissions Information

In the Permissions Information section Application User Configuration, allow ACE to control CTI devices.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
sysadmin | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Application User Configuration
Related Links: Back To Find/List Go
Save Delete Copy Add New
CAPF Information
Associated CAPF Profiles
View Details
Permissions Information
Add to User Group
Remove from User Group
Save Delete Copy Add New

Groups
- Standard CTI Allow Call Monitoring
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices

View Details

Roles
- Standard CTI Allow Call Monitoring
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices

View Details