CUCM to CUBE Integration Configuration Example

Document ID: 117300

Contributed by William Ryan Bennett and Steven Smith, Cisco TAC Engineers.

Jan 22, 2014

Contents

Introduction

This document describes the basics of Cisco Unified Border Element (CUBE) configuration with Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recommends that your system does not have Domain Name System (DNS) configuration and that you have knowledge of these topics:

- CUCM Version 8.6 through Version 10.x
- Cisco IOS® Version 15.1(2)T and later

Note: The IP addresses vary based on the addressing schemes in the network.

Components Used

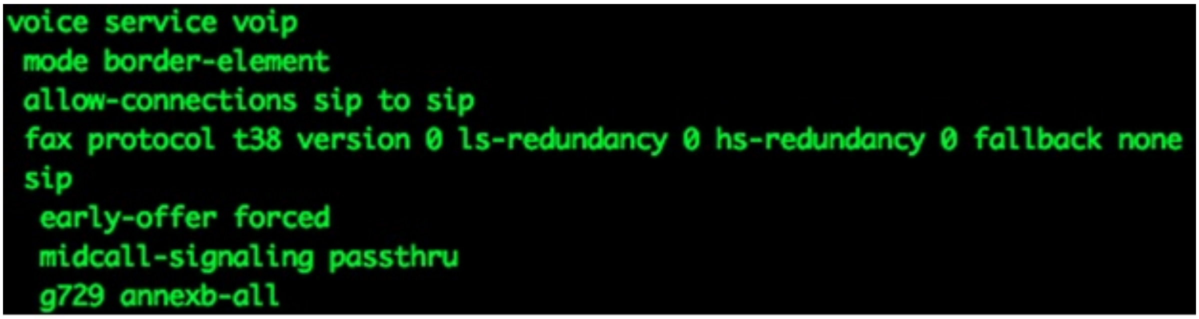
The information in this document is based on the fact that any number of CUCM servers, any Cisco Integrated Services Router (ISR), ISR Generation 2 (G2), or Cisco Aggregation Services Router (ASR) can be a CUBE. No Digital Signal Processors (DSPs) are required for basic CUBE operation.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

The CUBE−Side of the CUCM−to−CUBE Integration

When you first set up a CUBE, you must enable the router in order to route calls like a CUBE. This image shows a basic Voice Service VoIP configuration on a CUBE:



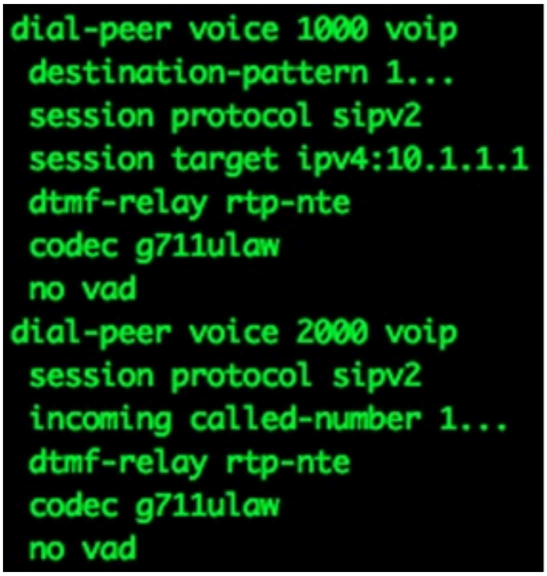
```
voice service voip
 mode border-element
 allow-connections sip to sip
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  early-offer forced
  midcall-signaling passthru
  g729 annexb-all
```

Here are some important points about this configuration:

- The first line of the configuration is ***mode border−element***, which enables CUBE on a router. Some devices do not have this configuration when they operate as a CUBE.
- ***Allow−connections sip to sip*** enables the CUBE to accept Session Initiation Protocol (SIP) calls and route them as SIP calls. There are options for H323 as well.
- ***Fax protocol t38*** is a default configuration for ISR G2 routers. It is not needed for CUBE configuration.
- ***Early−offer forced*** allows CUBE to route calls in a Delayed Offer to Early Offer scenario. Almost all of the providers require Early Offer SIP calls. It is actually recommended to send Early Offer from CUCM in order to avoid early media cut−through issues.
- ***Midcall−signaling passthru*** is only for SIP−to−SIP calls. It is required for some supplementary services to work.
- ***G729 annexb−all*** is optimal in cases where CUBE negotiates with providers who do not follow the RFC format for G729r8 and G729br8 codecs.

Dial−Peer Configuration on CUBE

Dial−peers on CUBE are like other dial−peers on Cisco IOS gateways. The difference is that the calls route from one VoIP dial−peer to another VoIP dial−peer.



```
dial-peer voice 1000 voip
 destination-pattern 1...
 session protocol sipv2
 session target ipv4:10.1.1.1
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
dial-peer voice 2000 voip
 session protocol sipv2
 incoming called-number 1...
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Notice that there are two dial−peers here: incoming and outgoing. CUBE ***always*** matches two dial−peers. Incoming dial−peers are from the CUBE perspective, either from the CUCM or from the SIP provider. Outgoing dial−peers are sent towards the CUCM or to the SIP Provider.

ICisco recommends that you perform most of the digit manipulation on CUCM through Significant Digits, External Phone Number Mask, and Translations. Refer to the Understanding Inbound and Outbound Dial Peers Matching on IOS Platforms article for more information about dial−peers.

Digit manipulation can be performed on CUBE, the same way it is performed on Cisco IOS Voice Gateways. Refer to the Number Translation using Voice Translation Profiles article for more information.

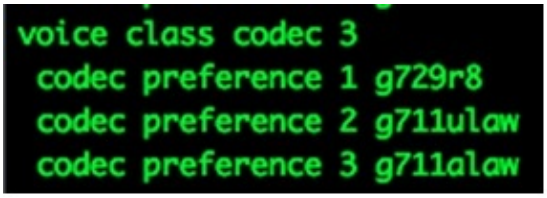
Basic IP Addressing

IP addressing on CUBE is accomplished the same way as on other Cisco IOS devices, but it uses the routing table in order to determine from which interface the CUBE sources SIP traffic. The ***show ip route A.B.C.D*** command provides information about the interface the CUBE uses in order to source SIP traffic. This is important when calls are sent to CUCM and when calls are sent to an SIP provider. Static routes might be needed in order to make this work.

In some cases, you might have to bind SIP to a particular interface, such as a loopback interface on the CUBE. SIP binding can cause side effects, such as when the CUBE does not listen for SIP traffic on a particular interface. Cisco recommends that you not use bindings and let the routing table decide, but this is not always possible. You can apply SIP bindings under ***Voice Service VoIP > SIP***, or on individual dial−peers. SIP bindings are explained more in the Configuring SIP Bind Features article.

Voice−Class Codecs on CUBE

Voice−class codecs are used for CUBE in order to offer multiple codecs when calls use a particular VoIP dial−peer. This is the same as it was on a Cisco IOS Voice Gateway, but when it is a CUBE, codecs are filtered from one VoIP call leg to the other. It uses codecs that are available on both the incoming dial−peer and the outgoing dial−peer. The codecs that match both are sent offers. When CUBE receives a SIP message with Session Description Protocol (SDP), it also matches this against the voice−class codecs. This allows CUBE to filter codecs based on what is received from the SIP message with SDP, the inbound dial−peer, and the outbound dial−peer. The other SIP User Agent (UA) then responds to the codecs offered.



```
voice class codec 3
 codec preference 1 g729r8
 codec preference 2 g711ulaw
 codec preference 3 g711alaw
```

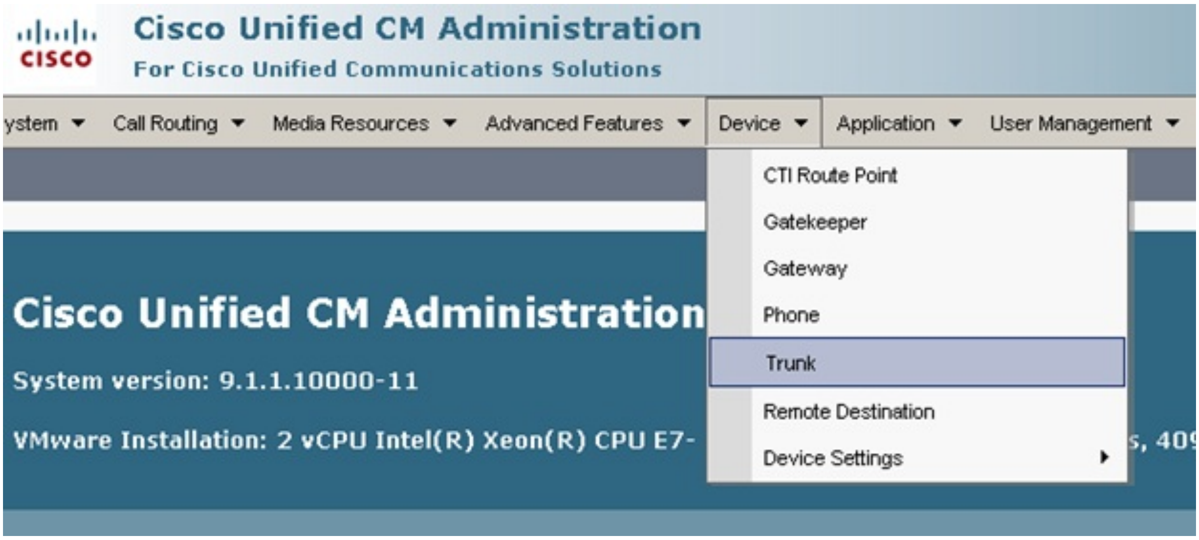
The voice−class codec in the previous image contains three codecs, ***g729r8***, ***g711ulaw***, or ***g711alaw***. The image shows them in the order in which the Cisco IOS gateway prioritizes how the codecs are offered to the far end. Voice−class codecs are applied to dial−peers.

Cisco IOS Toll−Fraud Application

The toll−fraud application in Cisco IOS is useful because it can prevent unwanted SIP access, but without proper planning, it can cause some issues with normal operation. The toll−fraud application in Cisco IOS allows the router to specify the devices that can communicate with it to make calls (H323 or SIP). IP addresses that are used as session targets on dial−peers are automatically allowed to send calls to the Cisco IOS Voice Gateway without extra configuration. This usually includes all of the SIP Providers and CUCM servers in the environment, but not always. If it does not, these must be manually added to the CUBE. Only the signaling addresses must be added, not the media addresses. Refer to the Toll−Fraud Prevention Feature in IOS Release 15.1(2)T article for more information.

The CUCM−Side of the CUCM−to−CUBE Integration

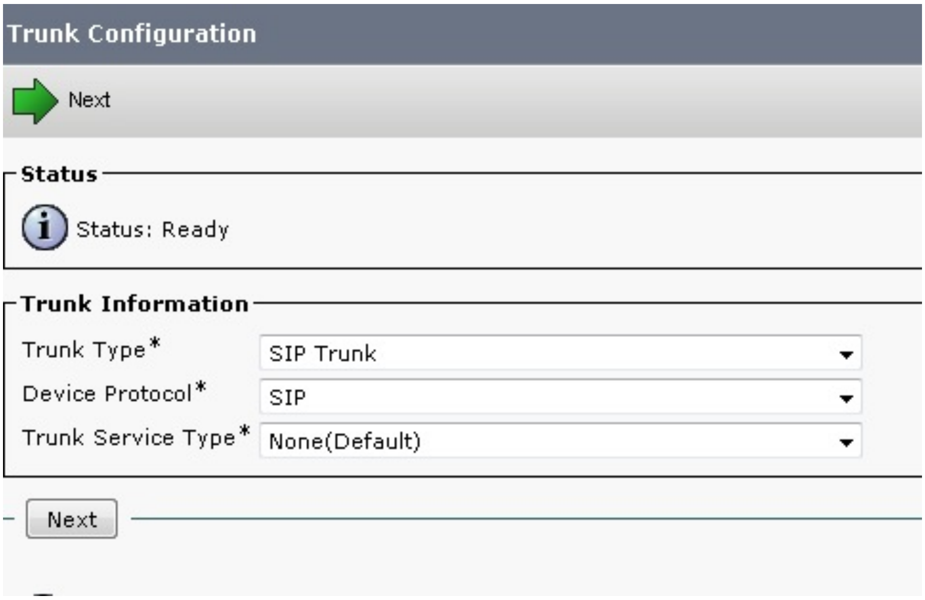
1. In order to add the trunk to the CUCM configuration, navigate to this location:



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Cisco Unified CM Administration
System version: 9.1.1.10000-11
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E7-

2. Select ***Add New*** and proceed to set up the SIP trunk as shown here:



Trunk Configuration

Next

Status

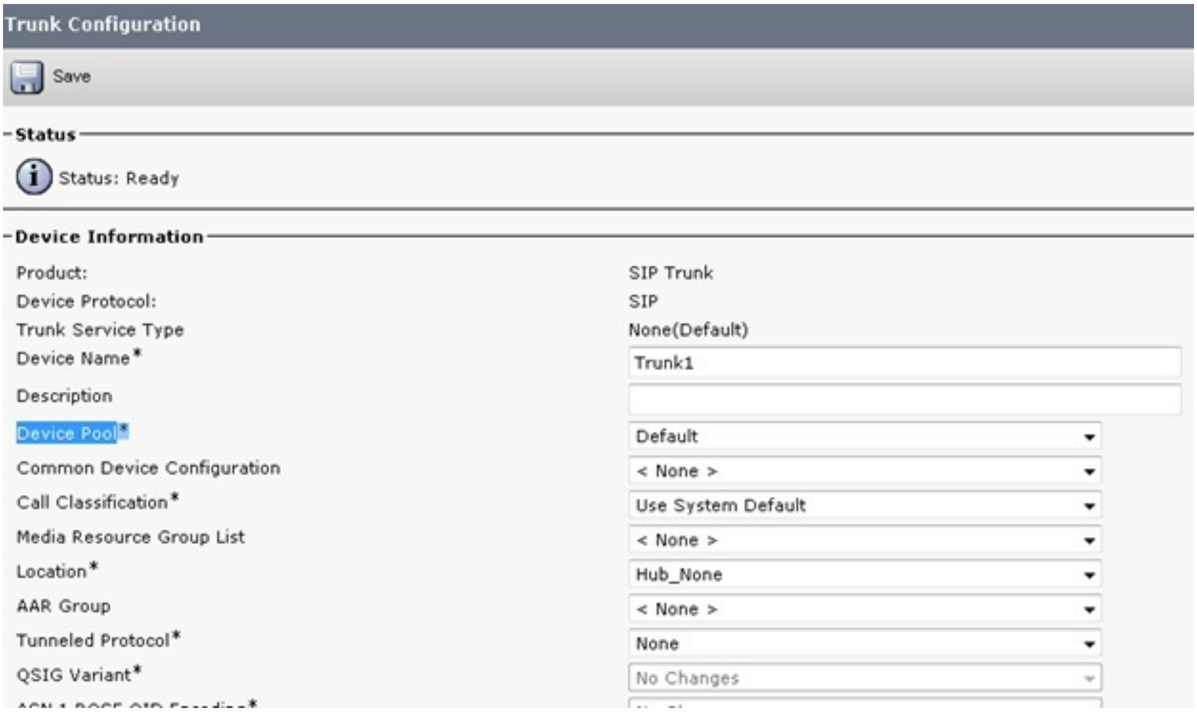
Status: Ready

Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Next

3. Within the trunk configuration page, remember to select the proper device pool that allows calls inbound to the particular CUCM server that accepts calls.



Trunk Configuration

Save

Status

Status: Ready

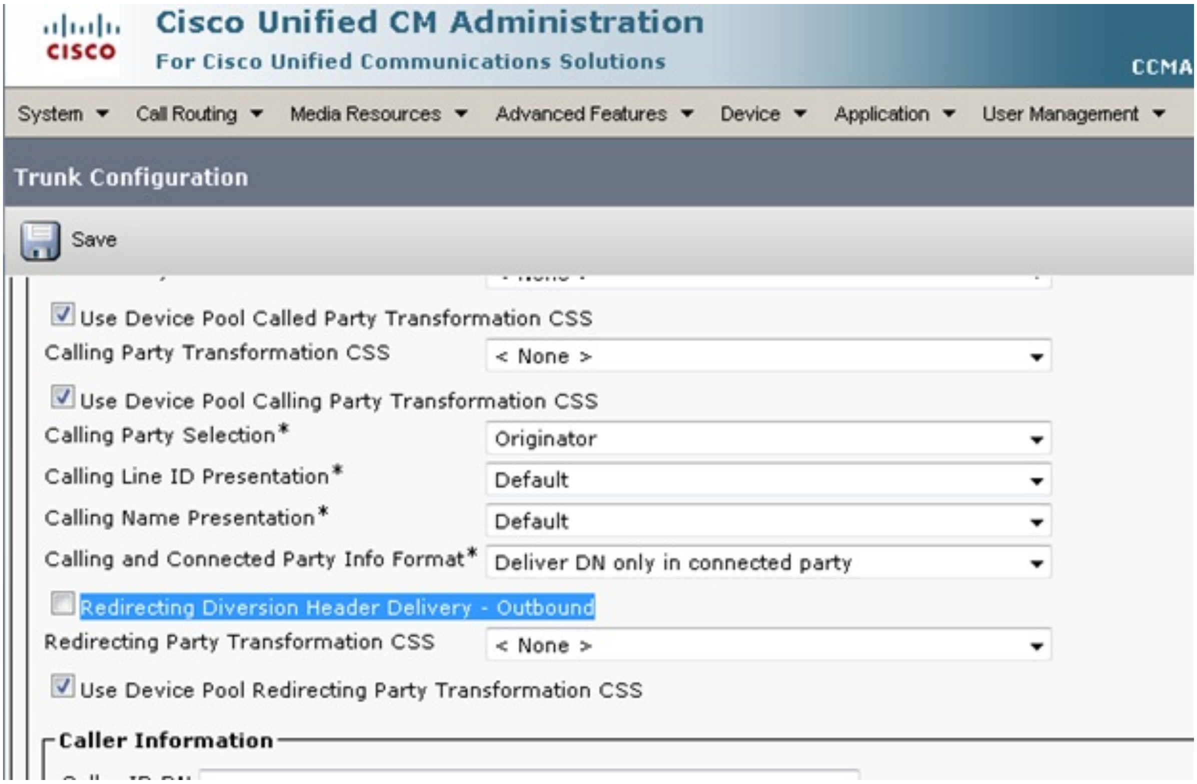
Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	Trunk1
Description	
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes

Once the trunk is created, ensure that the route patterns access it correctly either through a SIP Route Pattern or a Route List / Route Group setup.

The Redirecting Diversion Header can be ticked for inbound or outbound calls.

When External Numbers are forwarded into the VoIP Network, SIP invite messages come with relayed diversion information into CUCM. It shows the originating calling party. For example, if a call flow is integrated with Cisco Unity Connection (UC) and goes into voicemail, UC uses the initial diversion source (external forwarded number) as the destination mailbox. So it is possible that they could get the default opening greeting instead of the subscribers mailbox as expected. It depends on the call flow and requirements of your topology whether this is going to be required for the configuration.



☑ Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS: < None >

☑ Use Device Pool Calling Party Transformation CSS

Calling Party Selection*: Originator

Calling Line ID Presentation*: Default

Calling Name Presentation*: Default

Calling and Connected Party Info Format*: Deliver DN only in connected party

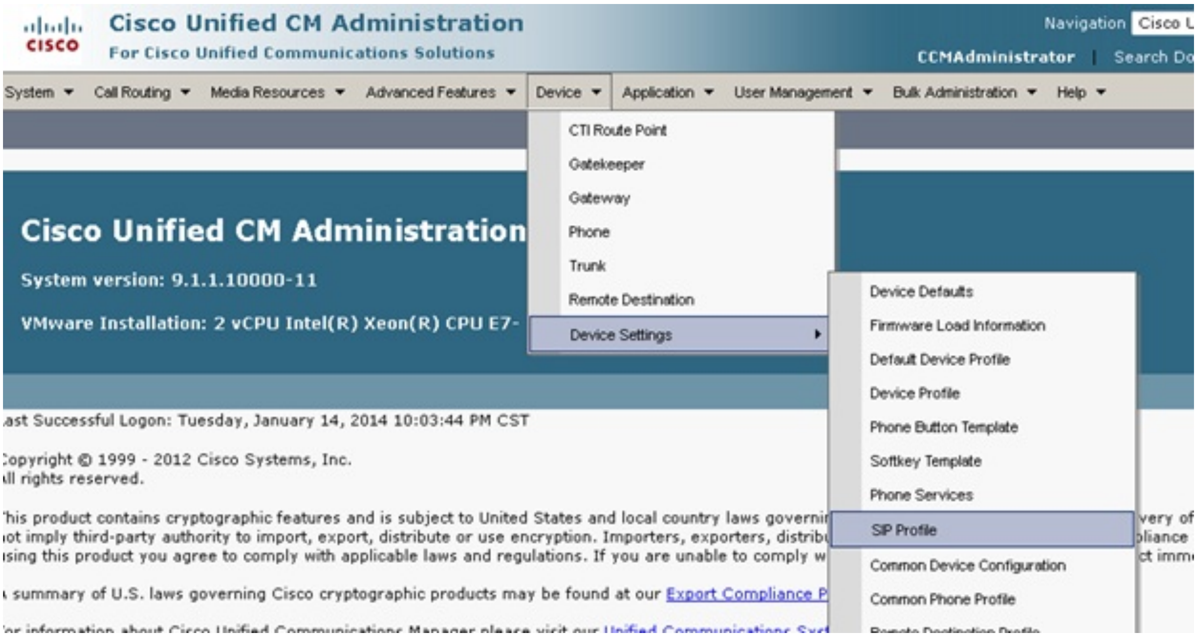
□ Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS: < None >

☑ Use Device Pool Redirecting Party Transformation CSS

Caller Information

4. The SIP profile for Early Offer is often needed when you connect the CUBE to a provider. If the trunk connects to another Cisco device, then you might not want to select the Media Transport Protocol (MTP) insert, based on the far−end devices. This image shows the SIP profile location and where to select the box for Early Offer.



Cisco Unified CM Administration

System version: 9.1.1.10000-11

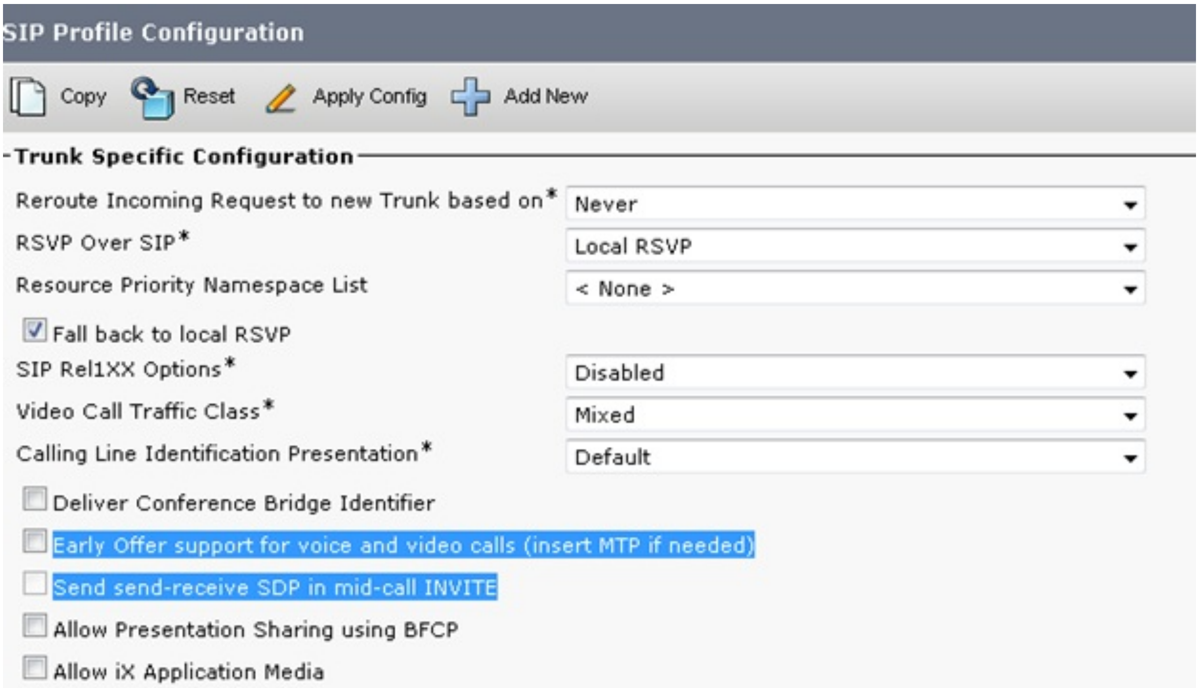
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E7-

ast Successful Logon: Tuesday, January 14, 2014 10:03:44 PM CST

opyright © 1999 - 2012 Cisco Systems, Inc.
ll rights reserved.

his product contains cryptographic features and is subject to United States and local country laws governi
ot imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distrib
sing this product you agree to comply with applicable laws and regulations. If you are unable to comply w

summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance P



Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on* Never

RSVP Over SIP* Local RSVP

Resource Priority Namespace List < None >

☑ Fall back to local RSVP

SIP Rel1XX Options* Disabled

Video Call Traffic Class* Mixed

Calling Line Identification Presentation* Default

☐ Deliver Conference Bridge Identifier

☐ Early Offer support for voice and video calls (insert MTP if needed)

☐ Send send-receive SDP in mid-call INVITE

☐ Allow Presentation Sharing using BFCP

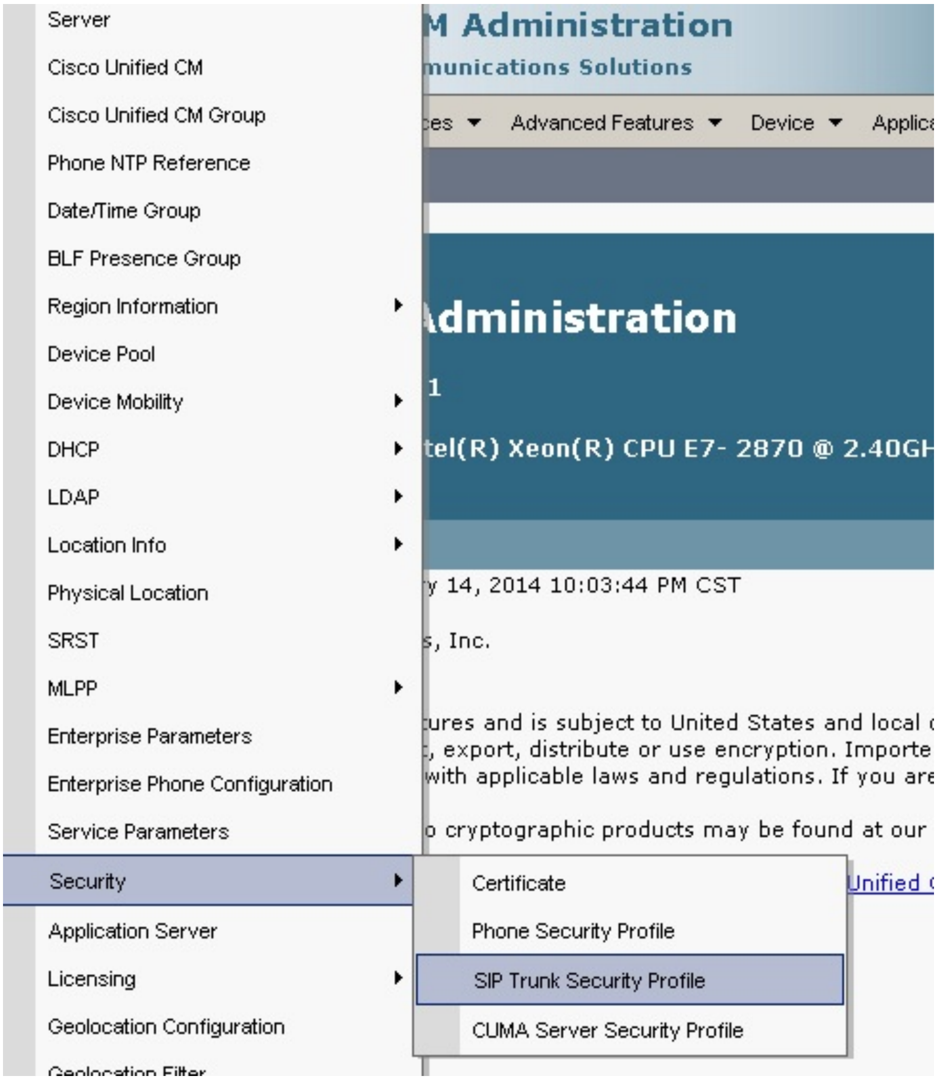
☐ Allow iX Application Media

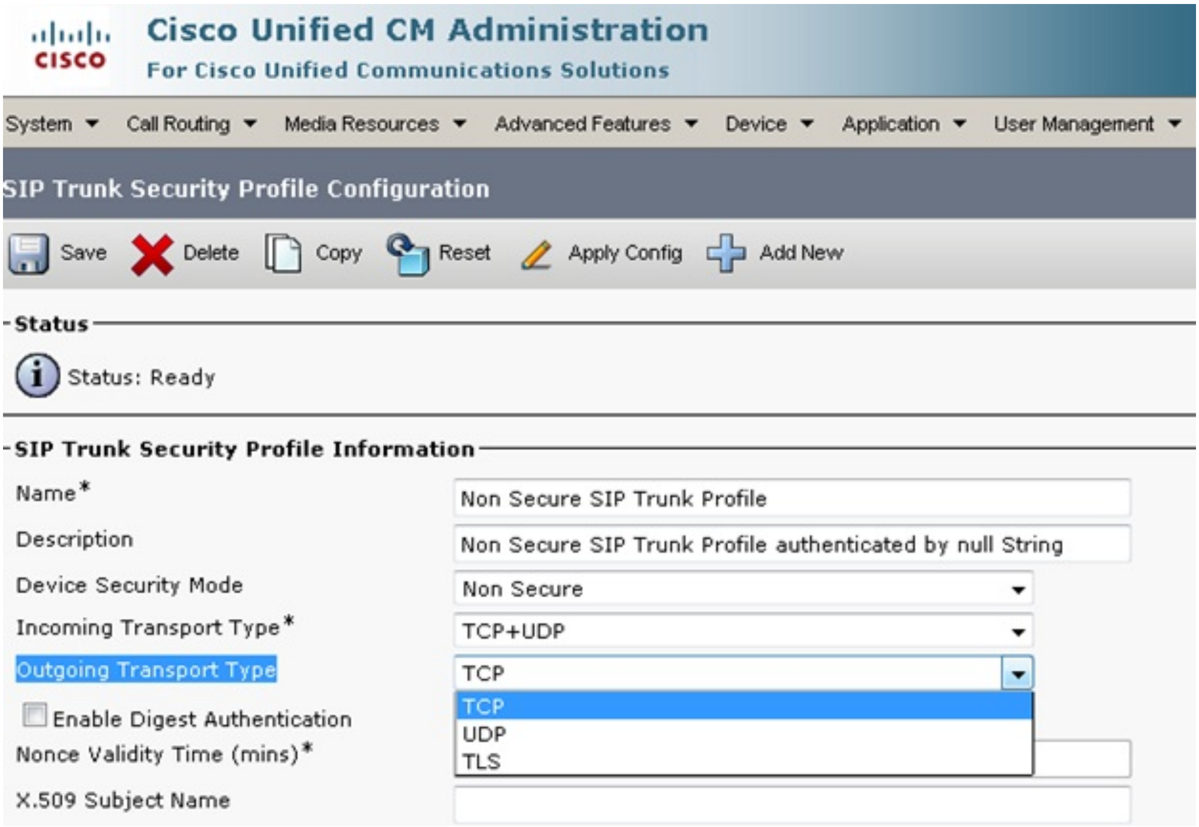
Early Offer often helps to resolve early media issues that arise when you integrate the CUCM server and CUBE to other third−party products. It is also recommended within the Solution Reference Network Design (SRND).

If the profile is going to be modified, it is always best to create a new profile to use instead of the default profile.

Note: This checkbox is used when end users do not want to have an MTP used on every call.

5. It might be necessary to change from TCP/UDP for the protocol within the SIP security profile based on the call flow. In order to make this change, navigate to ***SIP Trunk Security Profiles > Non Secure SIP Trunk Profile***:





SIP Trunk Security Profile Configuration

Status

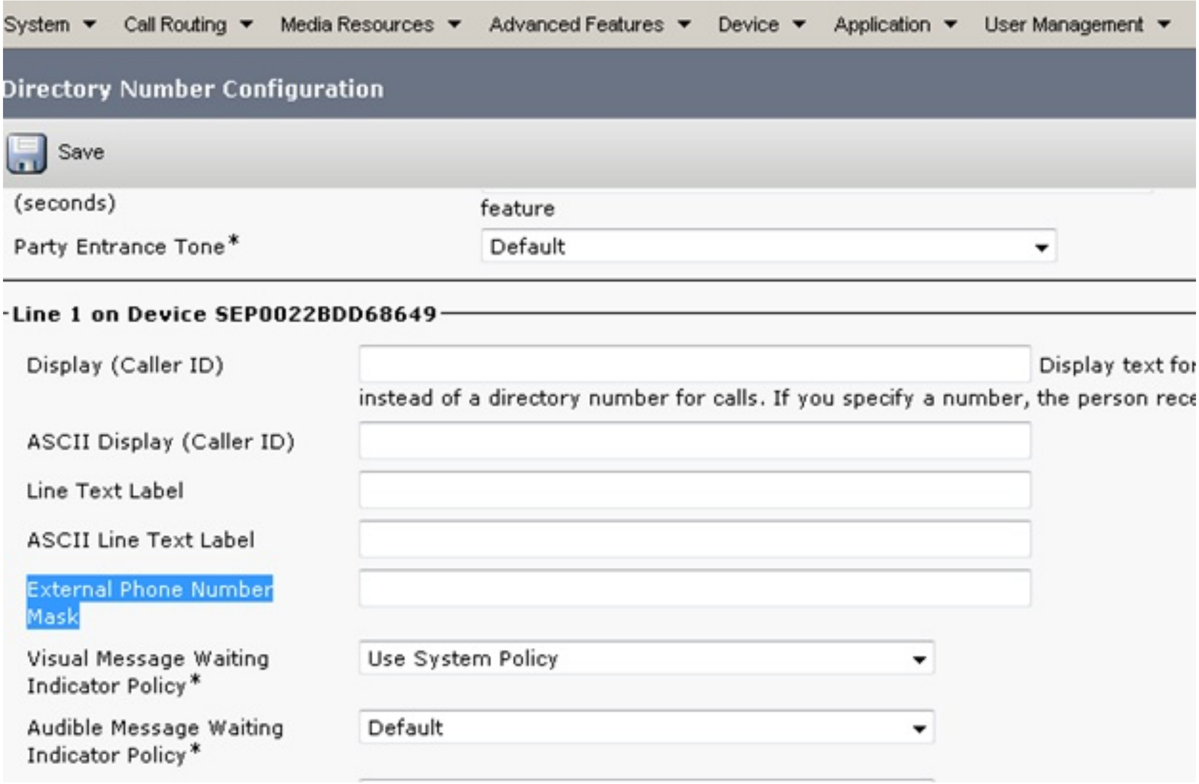
Status: Ready

SIP Trunk Security Profile Information

Name*	Non Secure SIP Trunk Profile
Description	Non Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP TCP UDP TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	
X.509 Subject Name	

Calls will fail, and CUBE/CUCM traces are required in order to understand what happens during the failure, but this feature can be modified in order to confirm that it is not the cause of the problem. However, once this is modified, you must reset/restart the trunk in order to make the change occur.

6. In some circumstances, the External Phone Mask on the phone configuration might need to be added in order for the call to proceed, because some Telcos do not allow the call to proceed without the expected mask. In order to make this modification, go to the Directory Number (DN) configuration page of the calling party phone, make the change necessary for the box, and reset/restart the phone after the changes are saved.



Directory Number Configuration

(seconds) feature

Party Entrance Tone* Default

Line 1 on Device SEP0022BDD68649

Display (Caller ID) Display text for

instead of a directory number for calls. If you specify a number, the person rece

ASCII Display (Caller ID)

Line Text Label

ASCII Line Text Label

External Phone Number Mask

Visual Message Waiting Indicator Policy* Use System Policy

Audible Message Waiting Indicator Policy* Default

Verify

Make test calls in order to verify that your configuration works correctly. If the test calls fail, take detailed CUCM service traces or CUBE traces in order to understand the problem.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.