SIP-Based Trunk Managed Voice Services Solution Design and Implementation Guide

First Published: January 22, 2009
Last Updated: January 22, 2009

Contents

Introduction, page 3

- Network Topology, page 3

Prerequisites, page 4

- Components Used, page 4
  - Cisco Unified Communications Manager, page 5
  - Cisco Unified Border Element, page 5
  - SCCP Analog Voice Gateway, page 5
  - Voice Mail at the Enterprise Headquarter Site, page 5
  - Cisco Adaptive Security Appliance Firewall Appliance, page 5
  - Cisco Survivable Remote Site Telephony, page 5
- Cisco IOS Software Releases, page 6
- Conventions, page 6

Solution Description, page 6

- Feature Summary, page 6
- SIP Trunking Design Considerations, page 7
- IP Connectivity, page 15
- Quality of Service, page 16
  - Congestion Management, page 16
  - Packet Marking, page 17
  - Call Admission Control, page 17
  - Delay, page 17

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Echo, page 18
Voice Mail, page 18
Dial Plan, page 18
Security, page 18
Authentication, page 18
Encryption of Media and Signaling, page 18
Firewall, page 19
Failover and Redundancy, page 19
Fax and Modem, page 19
Billing and Management, page 19
Best Practices for SIP Trunk implementation Using Cisco UBE, page 19
DTMF Transport, page 8
SIP Delayed Offer and Early Offer, page 8
Early Media Cut Through, page 9
SIP Trunk Transport Protocols, page 9
Monitoring SIP Trunk State, page 9
SIP Trunk Redundancy and Load Balancing, page 10
Caveats, page 21
Configurations, page 21
Configuration Verification, page 21
Troubleshooting, page 21
Related Information, page 22
Obtaining Documentation and Submitting a Service Request, page 23
Appendix: Enterprise 1 and Branch 1 SIP-Based Trunk Managed Voice Services Solution Example Configurations, page 24
Overview of Test Configurations, page 24
High-Level Operation, page 25
Test Topology, page 28
Example Configuration Details, page 29
Enterprise 1 HQ Cisco UBE Example Configuration, page 29
Enterprise 1 HQ Cisco Unified CM Example Configuration, page 32
Enterprise 1 HQ Cisco Unity and Cisco Unity Express Example Configuration, page 119
Enterprise 1 HQ and Cisco VG224 Analog Phone Gateway Example Configuration, page 119
Enterprise 1 HQ Cisco ASA Firewall Example Configuration, page 120
Branch 1 Cisco UBE, TDM Gateway, and Cisco Unified SRST Example Configuration, page 121
Branch 1 Cisco Unity Express 3.2 and Cisco Unified CM Example Configuration, page 125

Introduction

Cisco Unified Communications delivers fully integrated communications systems by enabling data and voice to be transmitted over a single network infrastructure using standards-based Internet Protocol (IP). Leveraging the framework provided by Cisco IP hardware and software products, Cisco Unified Communications delivers unparalleled performance and capabilities to address current and emerging communications needs in service provider, enterprise, and commercial business environments.

This guide discusses a solution network design to enable enterprise Session Initiation Protocol (SIP) trunk deployment with Cisco Unified Communications Manager (Cisco Unified CM) and Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST), one of the several SIP trunk solutions that Cisco is developing. The model of enterprise SIP trunk development with Cisco Unified CM and Cisco Unified SRST is especially geared for large enterprises with many branch offices. In this distributed model, the service provider (SP) furnishes the SIP trunk services for the enterprise to connect the enterprise headquarter with its enterprise branch offices. At the enterprise headquarter, Cisco Unified CM provides call control for voice services. Remote enterprise branch offices have Cisco Unified SRST deployed for voice services. The Cisco Integrated Services Router (Cisco ISR) running the Cisco Unified Border Element (Cisco UBE) is placed at the edge of the network. Cisco UBE plays an important role in serving multiple functions when connecting to other networks.

This design guide discusses the components deployed in the network, and provides sample router configurations for the Cisco UBE functions tested for the features included in this document.

Use this information to deploy enterprise SIP trunks with Cisco Unified CM and Cisco Unified SRST using service provider networks.

Network Topology

The components of the enterprise SIP trunk deployment with Cisco Unified CM and Cisco Unified SRST network topology is show in Figure 1. The service provider components are listed for completeness only and are not included in this guide.

Enterprise Headquarter

- Enterprise 1 HQ Cisco UBE Example Configuration, page 29
- Enterprise 1 HQ Cisco Unified CM Example Configuration, page 32
- Enterprise 1 HQ Cisco ASA Firewall Example Configuration, page 120
- Enterprise 1 HQ Cisco Unity and Cisco Unity Express Example Configuration, page 119
- Enterprise 1 HQ and Cisco VG224 Analog Phone Gateway Example Configuration, page 119

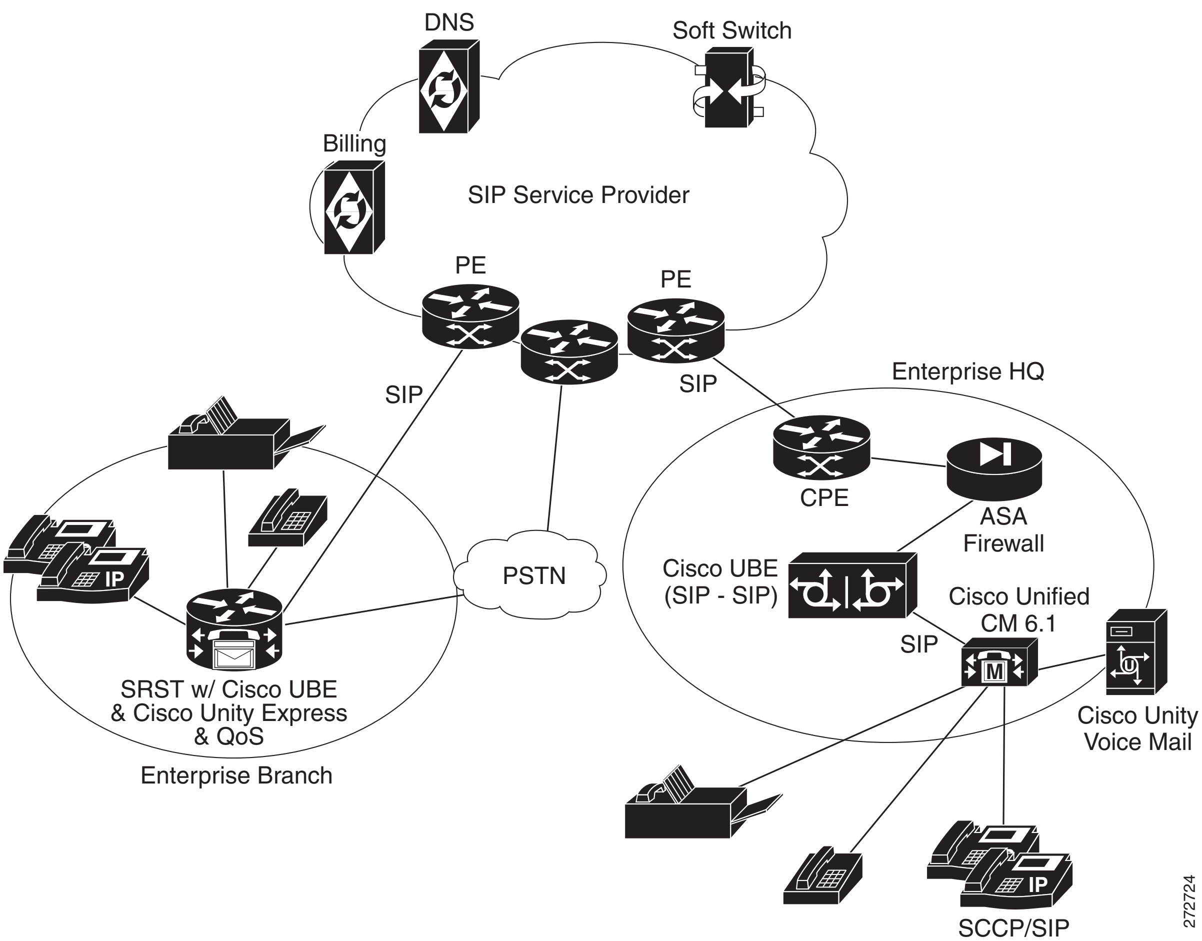
Enterprise Branch

- Branch 1 Cisco UBE, TDM Gateway, and Cisco Unified SRST Example Configuration, page 121
- Branch 1 Cisco Unity Express 3.2 and Cisco Unified CM Example Configuration, page 125

Service Provider

- PSTN hop-off gateway
- SIP Call Agent
- Multiprotocol Label Switching (MPLS) core network

Figure 1 Enterprise SIP Trunk Deployments Cisco Unified CM and Cisco Unified SRST with Cisco UBE



Prerequisites

Prerequisites are grouped into the following sections:

- Components Used, page 4
- Cisco IOS Software Releases, page 6
- Conventions, page 6

Components Used

The information in this guide is based on the software and hardware versions listed in the following sections. The configuration shown in this guide was created through the use of the devices in a specific lab environment. This section includes prerequisites for the following components:

- Cisco Unified Communications Manager, page 5
- Cisco Unified Border Element, page 5
- SCCP Analog Voice Gateway, page 5
- Voice Mail at the Enterprise Headquarter Site, page 5
- Cisco Adaptive Security Appliance Firewall Appliance, page 5
- Cisco Survivable Remote Site Telephony, page 5

Cisco Unified Communications Manager

The Cisco Unified CM at the enterprise headquarter site provides call control to voice services at the headquarter site and the branch offices. The Cisco Unified CM was tested using version 6.1.x.

Cisco Unified Border Element

A Cisco 3800 series platform was tested with Cisco IOS Release 12.4.(20)T1 and Cisco UBE version 1.2. The Cisco 2800 series Integrated Services Router (Cisco ISR) can also be used as a Cisco UBE.

SCCP Analog Voice Gateway

A Cisco VG224 analog voice gateway was used at the enterprise headquarter site to provide connectivity to analog phones and fax machines. The Cisco VG224 analog voice gateway was tested with Cisco IOS Release 12.4(20)T1.

Voice Mail at the Enterprise Headquarter Site

Voice mail at the enterprise headquarter site is provided by the Cisco Unity voice mail server, tested with version 3.2.

Cisco Adaptive Security Appliance Firewall Appliance

A Cisco ASA firewall appliance was placed at the ingress from the service provider servicing the enterprise headquarter site. It was tested with Cisco ASA 8.0(4).

Note The Cisco UBE at the enterprise headquarter site can also be used to provide Cisco IOS firewall functions. If the Cisco UBE is used to provide Cisco IOS zone-based firewall functions, the Cisco ASA firewall appliance is not needed.

Cisco Survivable Remote Site Telephony

A Cisco Unified SRST router was placed at the enterprise branch site. In addition to the Cisco Unified SRST functions, this router provides Cisco UBE, Cisco IOS firewall, conferencing transcoding, MTP, voice mail using Cisco Unity Express, TDM, and gateway functions. A Cisco 3800 series platform was tested with Cisco IOS Release 12.420T1. Cisco Unity Express was tested with version 3.2. The Cisco 2800 series Integrated Services Router (Cisco ISR) can also be used as an Cisco Unified SRST router.

Cisco IOS Software Releases

The test results described in this guide for the Cisco Unified Border Element were conducted using Cisco IOS Release 12.4(20)T1. We recommend Cisco IOS Release 12.4(20)T1 or later releases for the deployment of the features described in this guide.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Solution Description

The enterprise SIP trunk deployment with the Cisco Unified CM and Cisco Unified SRST solution topology allows the enterprise headquarter site to provide voice services from Cisco Unified CM to remote enterprise branch offices using SIP trunks from service providers. The enterprise branch offices are equipped with Cisco Unified SRST routers.

When Cisco Unified CM fails, but the WAN connection remains active and SRST takes over, the remote phones are able to make WAN calls through SIP to the call agaent. If a WAN connectivity failure occurs, the enterprise branch offices can continue to maintain basic IP phone and PSTN services.

The focus of services using this solution are:

- Voice services with call control provided by Cisco Unified CM at the enterprise headquarter site
- Voice services with Cisco Unified SRST at the enterprise branch offices

The following topics describe the solution:

- Feature Summary, page 6
- IP Connectivity, page 15
- Quality of Service, page 16
- Voice Mail, page 18
- Dial Plan, page 18
- Security, page 18
- Failover and Redundancy, page 19
- Fax and Modem, page 19
- Billing and Management, page 19
- Best Practices for SIP Trunk implementation Using Cisco UBE, page 19
- Caveats, page 21

Feature Summary

The features listed in this section were tested as part of the solution configuration.

Enterprise Headquarter Site Features

- Cisco Unified Communications Manager call control

- Cisco Unified Border Element
- Cisco ASA Firewall or Cisco IOS Zone-Based Firewall
- Cisco Unity Voice Mail Server
- Analog Phone and Fax Services

Enterprise Branch Offices Features

- Survivable Remote Site Telephony
- Cisco Unified Border Element
- Cisco IOS Firewall
- Cisco Unity Express Voice Mail
- Analog Phone and Fax Services
- PSTN Backup

Service Provider Features

- Multiprotocol Label Switching (MPLS) in the service provider backbone network
- PSTN Hop-Off Services (using service provider shared PSTN gateway)
- Optional Voice Mail Server

Basic Phone Features Served in the Topology

- Basic and Supplementary Calls
- DTMF Relay RFC 2833
- Fax and Modem Passthrough
- Supplementary services: Hold, Transfer, Forward, Conferencing, Transcoding, Music-on-Hold, Delayed Offer, Early Offer
- Calls to service provider PSTN gateway, inbound and outbound
- Voice mail services (Cisco Unity at the enterprise headquarter site and Cisco Unity Express at the enterprise branch offices)

SIP Trunking Design Considerations

SIP trunking design considerations described in the following sections should be assessed when deploying SIP trunks.

- DTMF Transport, page 8
- SIP Delayed Offer and Early Offer, page 8
- Early Media Cut Through, page 9
- SIP Trunk Transport Protocols, page 9
- Monitoring SIP Trunk State, page 9

DTMF Transport

There are several ways of transporting DTMF information between SIP endpoints. In general, these methods can be classified as Out of Band (OOB) and In Band (IB) signaling. In Band DTMF transport methods send either raw or signaled DTMF tones within the RTP stream and need to be processed by the endpoints that generate or receive them.

OOB signaling methods transport DTMF tones outside of the RTP steam, either directly to and from the endpoints or using a Call Agent, such as the Communications Manager, which interprets and forwards these tones as required.

OOB SIP DTMF signaling methods include:

- Unsolicited SIP Notify
- INFO method
- Key Press Markup Language (KPML)

KPML (RFC 4730) is the preferred OOB signaling method used by Cisco. KPML is supported on Advanced Cisco 79X1 Series IP Phones, Cisco Unified CM, and Cisco IOS Gateways (Cisco IOS Release 12.4 and later).

Unsolicited Notify is a proprietary DTMF transport method used only on Cisco IOS Gateways (Cisco IOS Release 12.2 and later).

IB DTMF transport methods send DTMF tones as either raw tones in the RTP media stream or as signaled tones in the RTP payload, using RFC 2833.

With SIP product vendors, RFC 2833 has become the predominant method of sending and receiving DTMF tones and is supported by the majority of Cisco voice products.

Because IB signaling methods send DTMF tones in the RTP media stream, the SIP endpoints in a session must either support the transport method used (for example, RFC 2833) or provide a method of intercepting this in band signaling and converting it. That is, if two endpoints are using a B2BUA as the call control agent (such as the Communications Manager) and they negotiate different DTMF transport methods, then the call control agent determines how these DTMF transport differences are handled. With Communications Manager, a DTMF transport mismatch (for example, In Band to Out of Band DTMF) is resolved by inserting a transcoder

SIP Delayed Offer and Early Offer

RFC 3261 defines two ways that Session Description Protocol (SDP) messages can be sent in the offer and answer, commonly known as Delayed Offer and Early Offer, which are mandatory requirements in the specification. In the simplest terms, an initial SIP Invite sent with SDP in the message body defines an Early Offer; whereas, an initial SIP Invite sent without SDP in the message body defines a Delayed Offer. In an Early Offer, the session initiator sends its capabilities in the SDP contained in the initial invite (for example, codecs supported). In a Delayed Offer, the session initiator does not send its capabilities in the initial invite and waits for the called device to send its capabilities first.

Cisco UBE uses the SIP *Offer/Answer* model for establishing SIP sessions, as defined in RFC 3264. In this context, an *Offer* is contained in the SDP fields sent in the body of a SIP message.

Note Service providers sometimes mandate an Early Offer call from the enterprise. In such cases Cisco UBE (Cisco IOS Release 12.4(20)T and later) can be configured to convert the Delayed Offer to the Early Offer.

Early Media Cut Through

The terms Early Offer and Early Media are often confused.

- Early Offer is the call setup where the initial Invite has the SDP Offer.
- Early Media is the preconnect media cut-through.

In certain circumstances, a SIP session can require that a media path be set up prior to completing a connection. To this end, the SIP protocol allows the establishment of Early Media after the initial Offer has been received by an endpoint. The reasons for using Early Media vary.

- The called device might establish an Early Media RTP path to reduce the effects of audio cut-through delay (clipping) for calls experiencing long signaling delays, or to provide a network-based voice message to the caller.
- The calling device might establish an Early Media RTP path to access a DTMF or voice driven IVR system (for example, airlines).

Both Early Offer and Delayed Offer calls support Early Media. Early Offer calls can typically stream Early Media after exchanging two messages (Invite with SDP and Trying). Delayed Offer calls can typically stream Early Media after exchanging four messages (Invite without SDP, 100 Trying, Session Progress with SDP and PRACK).

If Cisco UBE is configured to do DO->EO conversion, ensure that PRACK is enabled on CUCM, for call flows involving early media cut-through (18x w/SDP) to work seamless.

SIP Trunk Transport Protocols

SIP Trunks can use either TCP or UDP as a message transport protocol. As a reliable, connection orientated protocol that maintains the connection state per SIP dialogue, TCP is preferred. However, TCP has a higher segment overhead, uses more bandwidth than UDP, and has a higher packet overhead. These TCP overhead features increase call setup times when compared with UDP, which is connectionless and relies on the SIP stack to maintain its state and reliability.

If your network is prone to packet loss, use TCP. If the networks do not experience packet loss, use UDP.

Monitoring SIP Trunk State

SIP servers can monitor individual SIP dialogues either by using the dialogue's TCP connection or within the SIP stack itself (for example, for UDP based transport). In a Cisco Unified CM environment, use this per-call trunk state tracking feature in conjunction with Cisco Unified CM Route Groups and Route Lists to route calls over multiple SIP trunks. Trunk state is monitored and state changes are detected on a per-call basis. Successive trunk connections are attempted when the first trunk and subsequently selected trunks are down.

To overcome the limitations of per-call, per trunk state detection, the following methods can be used to monitor the state and detect the state changes of each end of a SIP trunk:

- OPTIONS Method—The SIP OPTIONS method allows a UA to query another UA or a proxy server as to determine its capabilities. This query allows a client to discover information about the supported methods, content types, extensions, codecs, and so on, without actually placing a call.

  Cisco UBE sends an Out of Dialogue OPTIONS message to the device at the far-end of the SIP trunk to determine its state. The OPTIONS method is used as an application-level ping. The returned ping response is generally not as important as the fact that the trunk has confirmed that it is *alive*. Cisco Unified CM SIP trunks support the receipt of OPTIONS messages but do not send OPTIONS messages as keepalives. Cisco Unified CM version 5.x SIP trunks respond to OPTIONS messages with a "405—Method Not Acceptable" response. In Cisco Unified CM version 6.0.1, SIP trunks respond to an OPTIONS message with a "200—OK" response.
- INVITEs as keepalives—INVITEs that are sent to unused numbers on the SIP trunk is an alternative to the OPTIONS method as an application-level ping. Similar to the OPTIONS method, the response returned is generally not as important as the fact that the trunk has confirmed that it is *alive*. Cisco Unified CM responds to, but does not send SIP INVITEs as keepalives.

SIP Trunk Redundancy and Load Balancing

Redundancy can be achieved by combining the call admission control (CAC) features of IOS. In general, CAC can be applied based on IP address reachability, Total Memory, Total Calls, Total CPU, IP circuit max-calls, and max-connections. The following show several methods used to achieve redundancy based on:

- Dial-peer preferences and Dial-peer Hunting
- DNS SRV
- GK load balancing for H.323 Networks
- Route List & Route Group option from CCM

Dial-peer preferences and Dial-peer Hunting

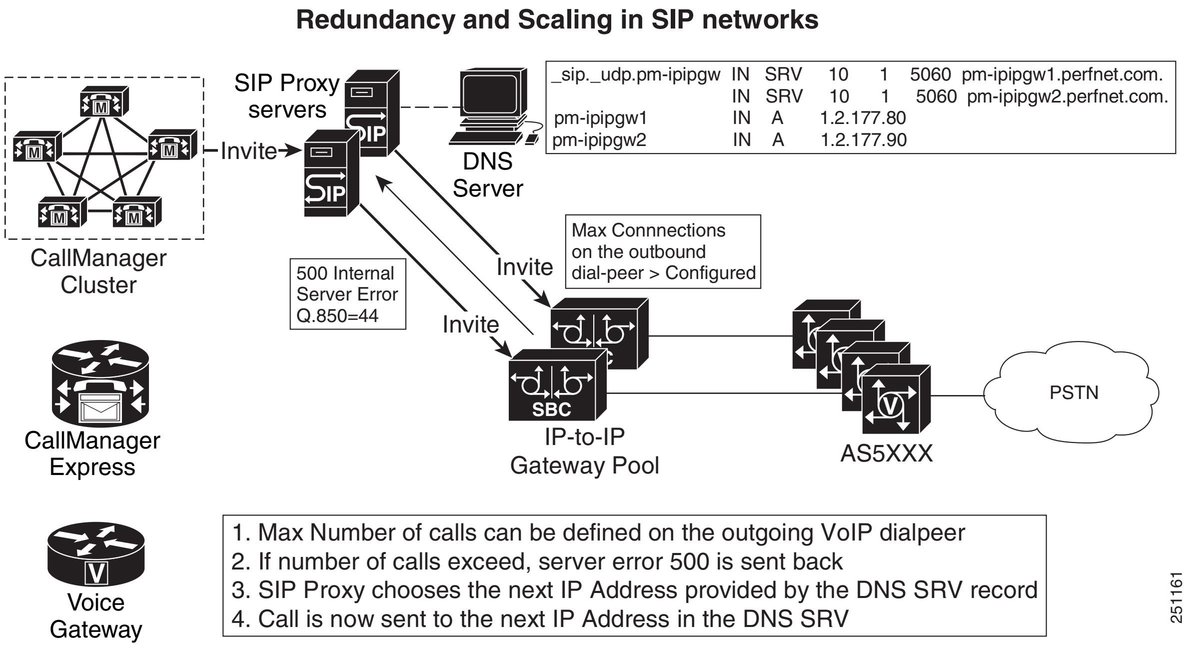
Use the following CLI example to achieve redundancy based on dial-peer preferences and dial-peer hunting:

```
!
dial-peer voice 3670000 voip
 description "first hunting for 3670000 to ent2-hq-ipip"
 destination-pattern 240367....
 session protocol sipv2
 session target ipv4:10.10.11.36
 codec g711ulaw
!
dial-peer voice 36700 voip
 description "second hunting for 3670000 to ent2-hq-ipip"
 destination-pattern 240367....
 preference 1
 session protocol sipv2
 session target ipv4:10.10.11.37
 codec g711ulaw
!
```

DNS SRV

Use the setup example shown in Figure 2 into achieve redundancy based on DNS SRV.

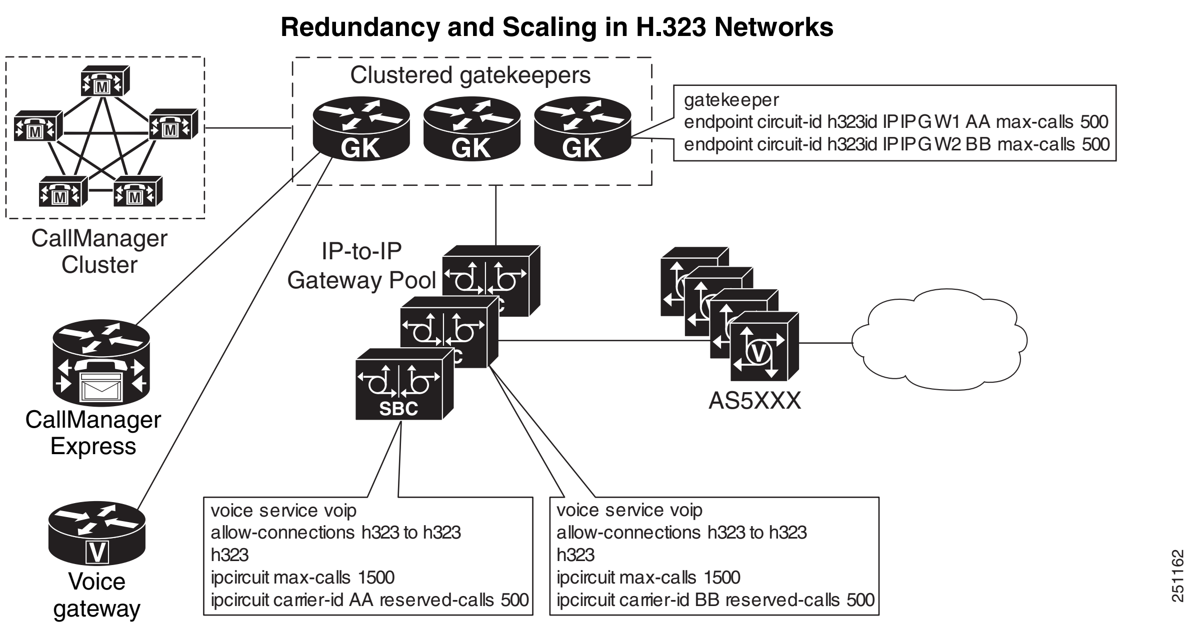
Figure 2 SIP Network Redundancy and Scaling Based on DNS SRV



GK load balancing for H.323 Networks

Use the setup example shown in Figure 3 to achieve redundancy based on GK load balancing for H.323 networks.

Figure 3 Redundancy and Scaling Based on GK Load Balancing for H.323 Networks



Route List & Route Group option from CCM

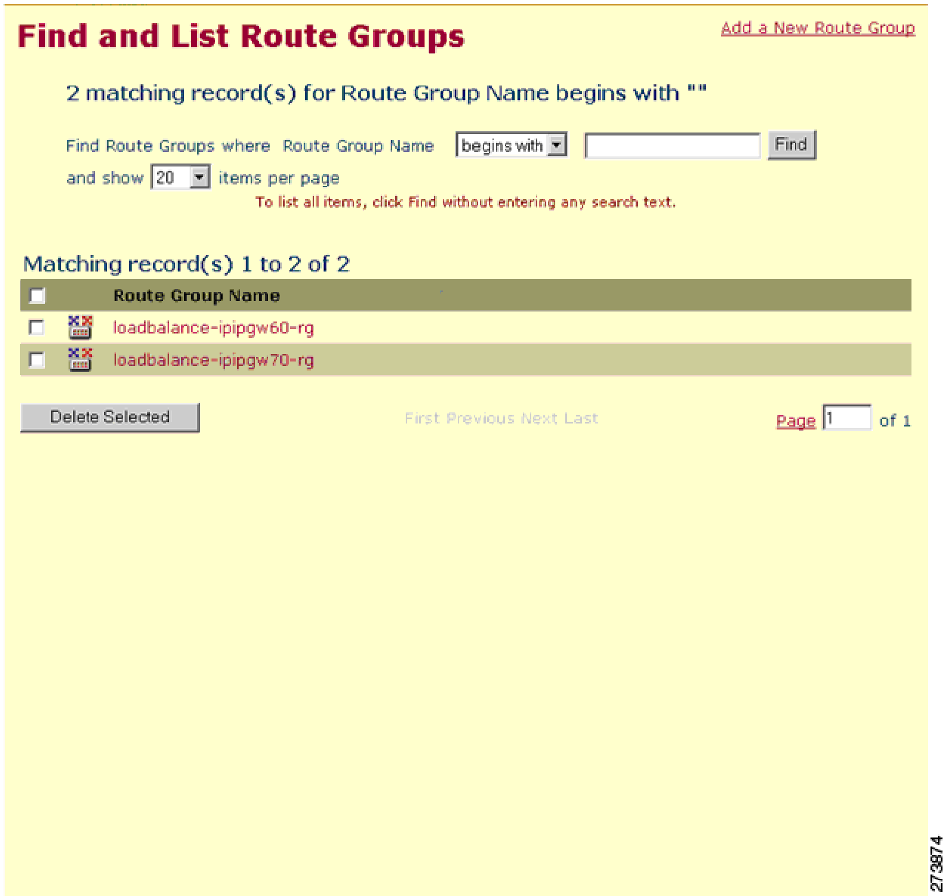
To achieve redundancy based on route list and route group using Cisco Unified CM, complete the following steps:

1. Configure one Route Group to each IPIPgw (see Figure 4).

Figure 4 Configuring Route Groups

2. Configure one Route List to club all Route Groups (see Figure 5).

Figure 5 Configuring A Route List for Route Groups



3. Configure Route List under Route Pattern Gateway or Route List (see Figure 6_.

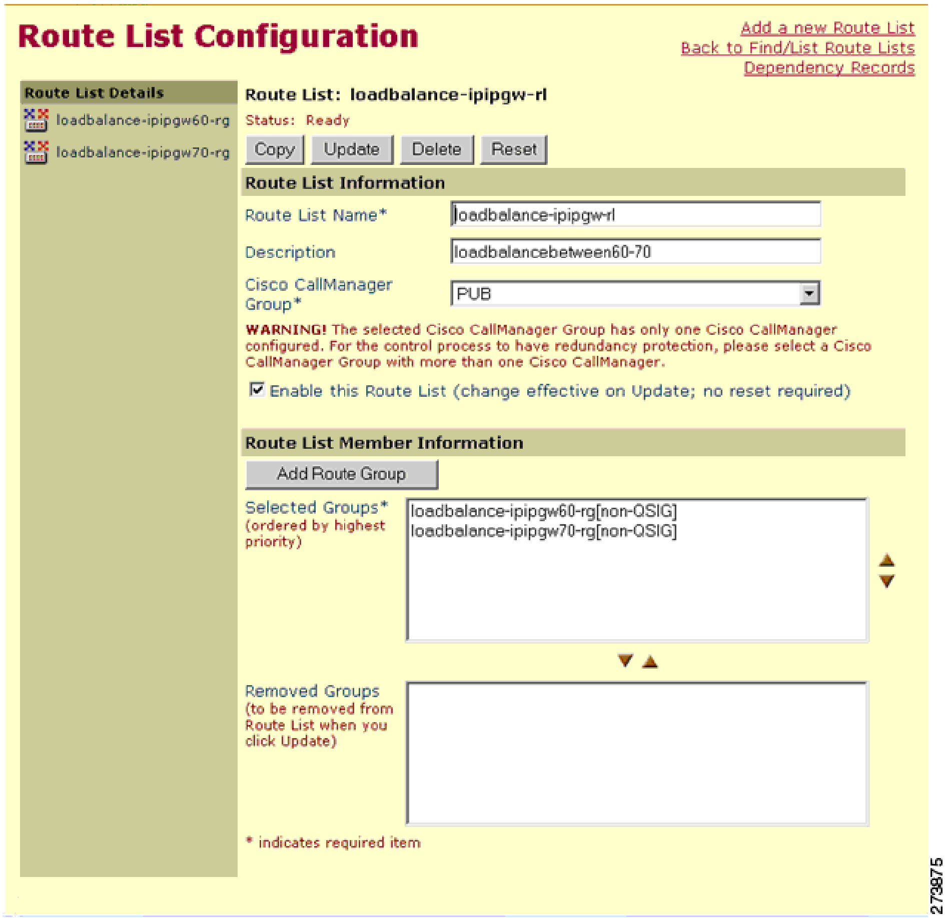
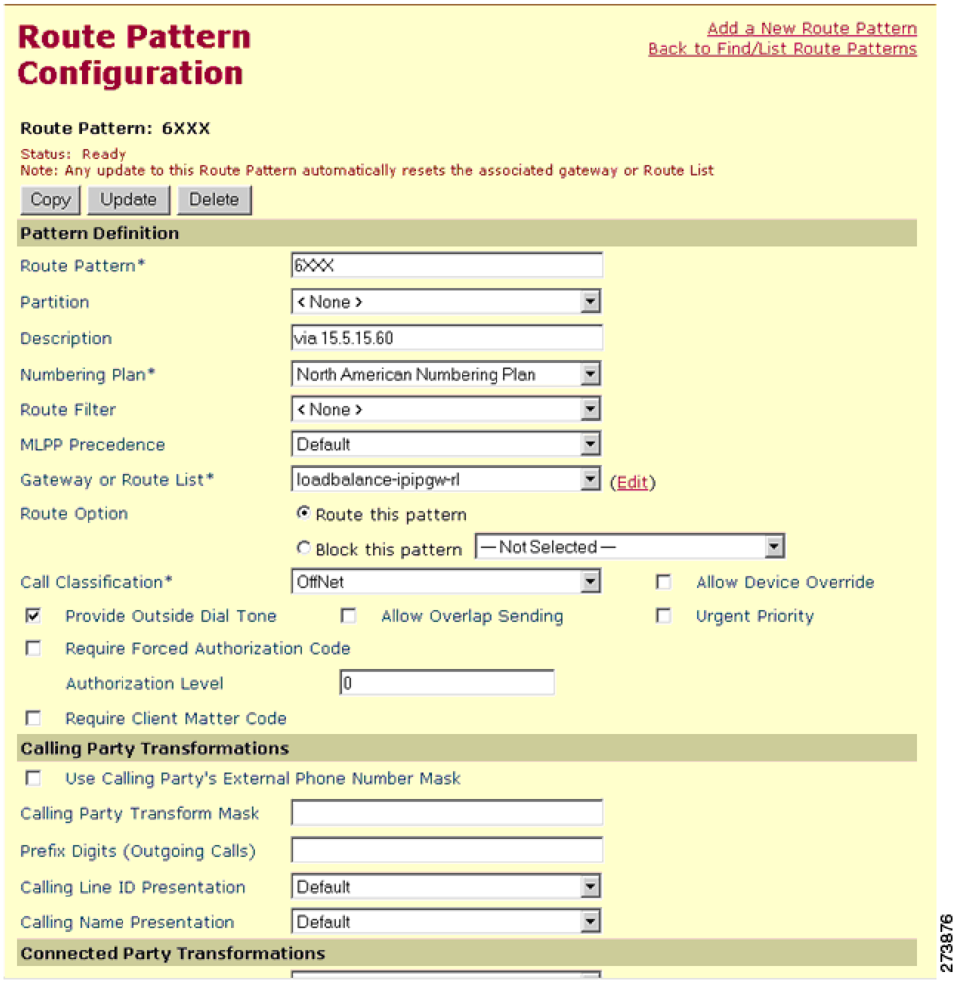


Figure 6 Configuring A Route List Under Route Pattern Gateway or Route List

4. Configure Max-Con under IPIPgw dial-peers towards Meeting Place, or Set the Global Call Treatment for total-calls.

Figure 7 Configuring Max-Con



IP Connectivity

The SIP trunks are typically provided by service providers (SPs). SP voice services are offered using a SIP trunk that uses the same physical IP interface also used to deliver data services. The options for the physical connection of SIP trunks from the SPs are shown in Table 1.

The sample configuration in the "Configurations" section on page 21 shows a Gigabit Ethernet interface.

Some service providers that offer both data and voice services over a single IP interface also offer MPLS services. With MPLS services, voice packets must be sent with an MPLS label so that the service provider can terminate the traffic, and data marked with a different label can be tunneled through the backbone network. Marking voice traffic with an MPLS label requires the Virtual Routing and Forwarding (VRF)-Aware voice feature available on the Cisco ISRs in Cisco IOS Release 12.4(20)T.

Table 1 Cisco CPE Router Network Connectivity Options

Physical Connection	Data Link
Fast Ethernet, Gigabit Ethernet	Metro Ethernet
Broadband Interface (HWIC-CABLE, WIC1-ADSL, WIC1-SHDSL)	Cable modem, digital subscriber line (DSL), asymmetric digital subscriber line (ADSL)
T1/E1 (WIC-1DSU-T1, VWIC-2MFT-T1, VWIC-2MFT-E1)	Point-to-Point Protocol (PPP), Frame Relay, ATM

Quality of Service

Quality of Service (QoS) is a fundamental requirement for any IP interface that carries voice traffic. Several specific QoS considerations and their configurations are discussed in this section:

- Congestion Management, page 16
- Packet Marking, page 17
- Call Admission Control, page 17
- Delay, page 17
- Echo, page 18

Congestion Management

When you use a single connection for both voice and data, you must carefully consider congestion management and bandwidth allocation to prevent data flows from affecting voice quality.

VoIP signaling and media traffic can be identified and classified as priority traffic using the QoS tools available within Cisco IOS software. Use Low Latency Queuing (LLQ) for media traffic streams. During congestion, LLQ queues restrict throughput to the configured bandwidth and packets exceeding this bandwidth are dropped. Therefore, signaling traffic should use class-based weighted fair queuing (CBWFQ), because signaling traffic bursts during call setup and teardown. The configurations for LLQ and CBWFQ are shown in the "Configurations" section on page 21. See *Quality of Service for Voice Over IP* for more information.

You can estimate the bandwidth to allocate to voice traffic by considering:

- Codec used by the calls
- Maximum number of simultaneous calls over the SIP trunk
- Payload size of the packets (that is, the sampling size of the codec)

The service provider can limit the maximum number of calls allowed across the SIP trunk based on the CAC techniques discussed in the "Billing and Management" section on page 19. This maximum number of calls allowed can be part of the service level agreement (SLA) between the service provider and the end customer.

When a Layer 2 connection technology, like Frame Relay or ATM, is used, additional traffic shaping and traffic management mechanisms must be deployed to ensure QoS on the egress interface. See *Configuring Frame Relay* for more information.

Packet Marking

You must set appropriate differentiated services code point (DSCP) values on the media and signaling packets leaving the SIP trunk from the customer premises to receive the desired service level in the service provider's network. By default, Cisco IOS software on the CPE router marks voice media packets, sourced on the router, with DSCP EF (101110) for expedited forwarding and signaling packets, sourced on the router, with DSCP AF31 (011010) for assured forwarding.

QoS policies may use either DSCP or IP precedence to classify voice packets. IP precedence interprets the low order three bits of the 6-bit DSCP value. In this way DSCP EF maps to CS5, while DSCP AD31 maps to CS3, which are appropriate IP precedence settings for voice media and signaling traffic.

Call Admission Control

Different types of Call Admission Control (CAC) are used in this solution. CAC can be based on bandwidth, maximum connections, CPU load, or memory available. CAC can be enabled at Cisco Unified CM or Cisco UBE.

Bandwidth-based CAC monitors the amount of bandwidth available in the network and controls routing of calls accordingly. This provides guaranteed control of bandwidth usage for voice calls. On Cisco Unified CM, bandwidth-based CAC is available and tested.

The number of simultaneous outbound calls can also be limited by the **max-conn** command on the VoIP dial peer used to route calls from the Cisco UBE router to the service provider network. This is the mechanism tested in the configuration example given in this guide.

The Cisco UBE can control the number of calls by setting the CPU load or memory available. This is configurable on the Cisco UBE by setting the threshold such that CAC is triggered when the threshold is reached.

The service provider can also control the total number of inbound and outbound calls from the SIP feature server, which is probably the best place for CAC policies to be implemented.

Note We recommend also implementing a limit such as that set by the **max-conn** command on the Cisco UBE side to protect against poor voice quality on the IP access link into the customer site if the number of calls exceeds the available bandwidth.

Delay

The telephone industry standard ITU-T G.114 recommends the maximum desired one-way delay for a voice packet be no more than 150 milliseconds (ms). With a round-trip delay of 300 ms or more, users can experience annoying talk-over. In addition to congestion management with proper queuing techniques, you can use link fragmentation and interleaving (LFI) on slower access links to ensure that the end-to-end delay budget for voice packets is met. LFI is usually necessary on links of less than 768K access speeds.

Variable delay in packet rate results in jitter. The jitter buffer in Cisco voice gateways runs in an adaptive mode and can remove the jitter from the packet flow for moderate end-to-end jitter in the network. See *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)* for more information on jitter. Delay can also cause echo.

Echo

Echo is caused by a time-division multiplexing (TDM) connection, or acoustic echo resulting from IP connections and endpoints. An improperly insulated phone, headset, or speakerphone could be the cause of echo experienced across a SIP trunk call. The analog phone user can also hear echo because of a very hot, or very high volume, signal on the TDM interface. *Echo Analysis for Voice over IP* explains how to adjust the settings for the voice port to eliminate echo caused by a hot signal and contains details on troubleshooting the source of echo. Delayed echo could be from the PSTN connectivity in the service provider's network. Cancel this echo on the PSTN gateway.

Voice Mail

Voice mail is provided by the Cisco Unity server at the enterprise headquarter site. At the enterprise branch offices, voice mail is provided by Cisco Unity Express embedded in the Cisco Unified SRST router.

The service provider can offer voice mail services using a hosted server. In this configuration, the service provider SIP server is responsible for functions such as call forward busy, call forward no answer, and Message Waiting Indicator (MWI).

Dial Plan

In this solution topology, the voice services are provided by the service provider using a call agent. The dial plan is also controlled by the service provider. The configuration shows the call routing configuration for VoIP dial peers needed on the Cisco UBE.

Security

The following security features are included in the solution network design:

- Authentication, page 18
- Encryption of Media and Signaling, page 18
- Firewall, page 19

Authentication

SIP registration and call method authentication can be provided using Digest Authentication. This method uses a single username and password for the entire SIP trunk, as shown in the “Configurations” section on page 21. The password is encrypted using Message Digest 5 (MD5).

Encryption of Media and Signaling

VPN technology can be used to encrypt the media and signaling streams between the Cisco UBE router and the core network. Cisco UBE also supports Transport Layer Security (TLS) and Secure RTP (SRTP) internally between phones and the router.

Firewall

At the enterprise headquarter site, either the Cisco ASA firewall appliance or Cisco IOS Zone-based firewall can be used to defend against outside attacks from the IP interface entering the headquarter. At the enterprise branch offices, the Cisco IOS Zone-based firewall features in the Cisco Unified SRST router are used. The firewall serves as a checkpoint for the customer LAN traffic exiting from the router to the service provider network.

Access control lists (ACLs) are required to filter out unwanted traffic on physical links to the Internet. These ACLs are used primarily to stop unauthorized access, Denial of Service (DoS) attacks, or distributed DoS (DDoS) attacks that originate from the service provider or a network connected to the service provider, and also to prevent intrusions and data theft.

In this test configuration, the Cisco ASA firewall appliance was used at the enterprise headquarter site and Cisco IOS firewall features were used at the enterprise branch offices.

Failover and Redundancy

If a complete SIP trunk failure or IP interface failure occurs, backup PSTN lines connected directly to Cisco Unified SRST can be used for PSTN access. In the Cisco Unified SRST router configuration shown in the "Configurations" section on page 21, backup PSTN access was tested for alternate call routing when SIP trunk access was down.

Fax and Modem

Fax pass-through and modem pass-through calls were tested between the enterprise headquarter site and branch offices and to the PSTN hop-off gateway. Fax and modem calls were tested with the G.711 codec.

Billing and Management

Typically the service provider is able to do billing without using any information from the managed Cisco UBE router.

Each call through the Cisco UBE router is considered to have two call legs. The start and stop records are generated for each call leg and can be polled through Simple Network Management Protocol (SNMP) using the DIAL-CONTROL-MIB. For more information, see the following documents:

- *CDR Logging with Syslog Servers and Cisco IOS Gateways*
- *Equivalent MIB Objects for VoIP show Commands*
- *RADIUS VSA Voice Implementation Guide*

Best Practices for SIP Trunk implementation Using Cisco UBE

By using the following Cisco UBE configuration methods, you can achieve a more effective SIP trunk topology implementation.

- Configure explicit incoming and outgoing dial-peers for Cisco UBE to apply the appropriate treatment to calls (for example, translations, codec, DTMF-type, SIP Normalization, and so on).
- Configure VoIP dial-peers with appropriate descriptions. For example:

  - description *** dial-peer to Service Provider ***
  - description *** dial-peer to Publisher Cisco Unified CM ***
  - description *** dial-peer to Subscriber Cisco Unified CM ***
- Always use a keepalive mechanism, such as Out of Dialog OPTIONS-ping, over the SIP trunk to detect upstream entity failure before routing calls to the service provider.
- Configure the Cisco UBE for media inactivity based on RTP, or RTCP, or both to accelerate the detection of *hung* calls.
- Because it is the most widely deployed and most interoperable DTMF mechanism for SIP trunks, use RFC 2833 to configure DTMF.
- If Cisco UBE is configured to do Delayed Offer to Early Offer conversions, ensure that PRACK is enabled on Cisco Unified CM, for call flows involving early media cut through (18x w/SDP) to work seamlessly.
- Fine tune the failover timers, especially when using clustered/DNS-SRV addressing.

  To ensure minimum Post Dial Delay during failover situations, fine tune the **sip-ua retry** *xxx* **parameters**, where *xxx* is the request name and response code. We recommend the value for INVITEs as *retry invite 2*.
- Do not configure Cisco HSRP on the router that runs Cisco UBE functionality.

  The Layer 3 and Layer 7 embedded SIP addresses can be unpredictable when Cisco HSRP is enabled. Refer to the caveats section for exact Bug-ID's.
- Use SIP profiles to insert or remove elements in the SIP headers.

  SIP Profiles is a very powerful SIP message normalization and protocol repair tool that can quickly fix or create a workaround to minor interoperability issues when two SIP implementations communicate with each other. This feature is available in Cisco IOS 12.4(15)XZ and Cisco IOS 12.4(20)T and later.
- If SIP trunk capacity requires a stack of Cisco UBEs to scale capacity, consider using the Cisco Unified SIP Proxy and Cisco UBE scaling architecture at the HQ location.
- Pay close attention to DTMF interoperability and call flows.

  Adjust the payload types for DTMF as needed when the default Cisco values are in conflict (for example, PT 96 is used for RFC 2833, which is by default reserved for cisco fax-relay).
- Adjust SIP incoming and outgoing ports as required to accommodate send and listen devices on non-standard SIP ports.
- Always test call flows with supplementary services as they present the most likely interoperability issues.
- Configure ACLs on Cisco UBE to allow traffic only from valid call agents and endpoints to avoid toll-fraud.

  You can configure CLI commands such as **allow term**.
- Configure fax traffic on TDM PSTN access if at all possible
- Mark all the outbound voice traffic with the appropriate DSCP values so that it gets the right priority in the service provider network. All other traffic should be appropriately marked.
- Provision backup FXO trunks on the Cisco CPE router to provide emergency PSTN access if the SIP trunk is down.
- The service provider should ensure appropriate call routing for emergency (911) calls using the shared hop-off PSTN gateway.

Caveats

In general, the following global caveats exist with this solution:

- The same static codec must be used on all voice calls. It can be any codec type, but the same codec must be maintained.
- The G.711ua codec must be used for the fax/modem calls in the network.
- Headquarter site or remote branch local calls must be configured with G.711 codecs.
- Voice calls over the WAN must be configured with G.729 codecs.
- Video was not tested as part of this solution.
- H.323 calls were not tested as part of this solution.
- Use of Cisco HSRP is not recommended in this solution as it can cause unexpected results with SIP signaling.

Configurations

The "Appendix: Enterprise 1 and Branch 1 SIP-Based Trunk Managed Voice Services Solution Example Configurations" section on page 24 provides configuration examples, screen figures, and other helpful information you need to configure the features on the Cisco UBE router at the edge of the service provider network described in this guide.

Note Use the Command Lookup Tool (registered customers only) or the Cisco IOS master commands list at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html for more information on the commands used in this guide.

Configuration Verification

Use the following **show** commands to display and verify your Cisco UBE configuration:

- **show dial-peer voice summary**
- **show sip-ua register status**

The firewall configuration can be verified with the following commands:

- **show ip inspect sessions**
- **show ip inspect statistics**

Troubleshooting

Note See Important Information on Debug Commands before you use **debug** commands.

Use the following **debug** commands to troubleshoot your configuration:

- **debug ccsip messages**

  This command shows all SIP Service Provider Interface (SPI) message tracing. It traces the SIP messages exchanged between the SIP UA client (UAC) and the access server.

- **debug ccsip all**

  This command enables all SIP-related debugging including:

  - **debug voip app**

    This command displays all application debug messages, including Application Framework (AFW) and DSAPP debugs.

  - **debug voip ccapi inout**

    This command traces the execution path through the call control API, which serves as the interface between the call session application and the underlying network-specific software. You can use the output from this command to understand how calls are being handled by the voice gateway.

  - **debug ephone mtp**

    This command enables Media Termination Point (MTP) debugging.

  - **debug sccp events**

    This command displays debugging information for SCCP events and its related applications transcoding and conferencing.

Related Information

The following information is referenced in this guide:

- *Cisco Unified Communications Manager Express 4.1 Multi-party Conferencing Enhancements*
- *CDR Logging with Syslog Servers and Cisco IOS Gateways*
- Cisco 2800 Series Integrated Services Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco Cable High-Speed WAN Interface Cards
- Cisco High Density Analog and Digital Extension Module for Voice and Fax
- Cisco IAD243X Business Class Integrated Access Device
- Cisco Systems - Support
- *"Configuring Conferencing"* chapter of the Cisco Unified Communications Manager Express System Administrator Guide
- *Configuring Frame Relay and Frame Relay Traffic Shaping*
- *Configuring SIP Support for Hookflash*
- *Echo Analysis for Voice over IP*
- *Enterprise QoS Solution Reference Network Design Guide*
- *Equivalent MIB Objects for VoIP show Commands*
- IP Communications Voice/Fax Network Module
- *Quality of Service for Voice Over IP*
- *RADIUS VSA Voice Implementation Guide*
- *Service Provider Quality-of-Service Overview*
- *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Appendix: Enterprise 1 and Branch 1 SIP-Based Trunk Managed Voice Services Solution Example Configurations

This appendix contains configuration examples to configure a SIP-based managed voice services solution using the Cisco Unified Border Element, Cisco Unified Communications Manager, Cisco Unity, and Cisco Unity Express, depending on your configuration requirements.

- Overview of Test Configurations, page 24
- High-Level Operation, page 25
- Test Topology, page 28
- Example Configuration Details, page 29
- Enterprise 1 HQ Cisco UBE Example Configuration, page 29
- Enterprise 1 HQ Cisco Unified CM Example Configuration, page 32
- Enterprise 1 HQ Cisco Unity and Cisco Unity Express Example Configuration, page 119
- Enterprise 1 HQ and Cisco VG224 Analog Phone Gateway Example Configuration, page 119
- Enterprise 1 HQ Cisco ASA Firewall Example Configuration, page 120
- Branch 1 Cisco UBE, TDM Gateway, and Cisco Unified SRST Example Configuration, page 121
- Branch 1 Cisco Unity Express 3.2 and Cisco Unified CM Example Configuration, page 125

Overview of Test Configurations

The following main components are used in the Voice Enterprise 1 configuration.

Enterprise 1 HQ Components

The main components of the Enterprise 1 Headquarters (HQ) include:

- Cisco Unified CM (version 6.1)
- SCCP IP Phones
- VG224 (version 12.4(20)T1) analog lines for Fax/Modem support
- Cisco UBE (Cisco IOS Release 12.4(20)T1)

Enterprise 1 and Branch 1 Components

The main components of the Enterprise 1 and Branch 1 include:

- Cisco UBE/Cisco Unified SRST/Analog lines for Fax/Modem
- SCCP IP Phones

Caveats

The following caveats apply to the SIP-based Trunk Voice Enterprise 1solution:

Global Caveats

In general, the following global caveats exist with this solution:

- The same static codec must be used on al voice calls. It can be any codec type, but the same codec must be maintained.
- The G.711ua codec must be used for the fax/modem calls in the network.
- Headquarter site or remote branch local calls must be configured with G.711 codecs.
- Voice calls over the WAN must be configured with G.729 codecs.
- Video was not tested as part of this solution.
- H.323 calls were not tested as part of this solution.
- Use of Cisco HSRP is not recommended in this solution as it can cause unexpected results with SIP signaling.

Cisco Unified CM 6.1.0.9901-372 Caveats

1. Cisco Unified CM version 6.1 does not support Early Offer g729r8; Delayed Offer is configured on Cisco Unified CM, and Early Offer is enforced on Cisco UBEs.
2. Cisco Unified CM does not support the midcall audio codec change (CSCsr03120).
3. Enhance SIP Trunk display to minimize confusion (CSCsv80045).

High-Level Operation

Anyone trying to configure the Voice Enterprise 1 topology should be very familiar with networking in general and the specific configurations of the following Cisco applications:

- Cisco Unified CM
- Cisco ASA 8.0(4) Firewall
- Cisco Unity
- Cisco Unity Express

CAll Flow Within Enterprise 1

All endpoints (Cisco Unified CM, HQ/Branch Cisco UBEs, IP phones, and so on) in the Voice Enterprise 1 network are configured to be routable. Calls within the enterprise use SCCP/MGCP for call control.

During normal operation, call flow from HQ to Branch 1 are as follows:

IP/VG224 FXS Phone (over SCCP) > Cisco Unified CM (over SCCP/MGCP) > IP/Branch Cisco UBE FXS Phone

During normal operation, Branch l call flows to HQ is in the reverse direction.

HQ Call Flow to Enterprise Offsite Remote Endpoint

During normal operation, call flow from HQ to outside of the enterprise is as follows:

IP/VG224 FXS phone (over SCCP) > Cisco Unified CM (over SIP) > HQ Cisco UBE (over SIP) > Service Provider SIP Proxy Server

During normal operation, external call flow to the enterprise HQ is in the reverse direction.

Branch 1 Call Flow to Enterprise Offsite Remote Endpoint

Call flow from Branch 1 to outside of the enterprise would be as follows:

IP/Branch Cisco UBE FXS phone (over SCCP/MGCP) > Cisco Unified CM (over SIP) > Branch Cisco UBE (over SIP) > Service Provider SIP Proxy Server

For normal operation, external call flow to the enterprise Branch 1 is in the reverse direction.

Note Between Cisco Unified CM and Branch Cisco UBE, signaling and voice RTP packets must pass through the enterprise HQ Cisco UBE, and it is not shown in the call flow because it is transparent.

Cisco Unified CM is used to control the number of uplink calls (CAC—bandwidth) for both the enterprise HQ and branch.

For purposes of security, the Cisco ASA can be placed at the front end of the HQ Cisco UBE.

High-Level Configuration Summaries

The following topics summarize the scope of a current enterprise solution.

Protocols

The following is a list of protocols used between components:

- SCCP: Cisco Unified CM and all IP Phones
- SCCP: Cisco Unified CM and Cisco VG224
- MGCP: Cisco Unified CM and Cisco UBE/Cisco Unified SRST TDM
- SIP–SIP: Cisco Unified CM HQ/Branch Cisco UBE and WAN (External to Enterprise)

Codecs

The following is a list of codecs used between components:

- g711ulaw: HQ/Branch IP Phone to IP Phone local calls
- G729r8: HQ/Branch IP Phone to remote endpoint across WAN
- Pass-through g711ulaw: HQ/Branch Fax/Modem to Fax/Modem local calls
- Pass-through g711ulaw:HQ/Branch Fax/Modem to remote endpoint Fax/Modem across WAN

Note Cisco Unified CM (version 6.1) does not support Early Offer g729r8. HQ/Branch Cisco UBEs are therefore configured to overcome this lack of support by using the Early Offer g729r8 for voice calls across the WAN to remote SIP endpoints. Remote voice calls terminating at the enterprise are forced to use g729r8. Cisco UBEs are also configured to force the pass-through of g711ulaw for Fax/Modem calls in both directions.

DSP Farms

Separate DSP farms are installed and configured on the enterprise HQ and Branch Cisco UBEs. Although only conference resources are used for these solutions, MTP and Transcoder resources are also configured and are registered to Cisco Unified CM for example purposes only.

Supplementary Services

The following is a list of supplementary services.

- CALL FORWARD
- CALL TRANSFER—Attended and Blind
- CALL HOLD, MUSIC on HOLD
- HARDWARE CONFERENCING

Call Admission Control

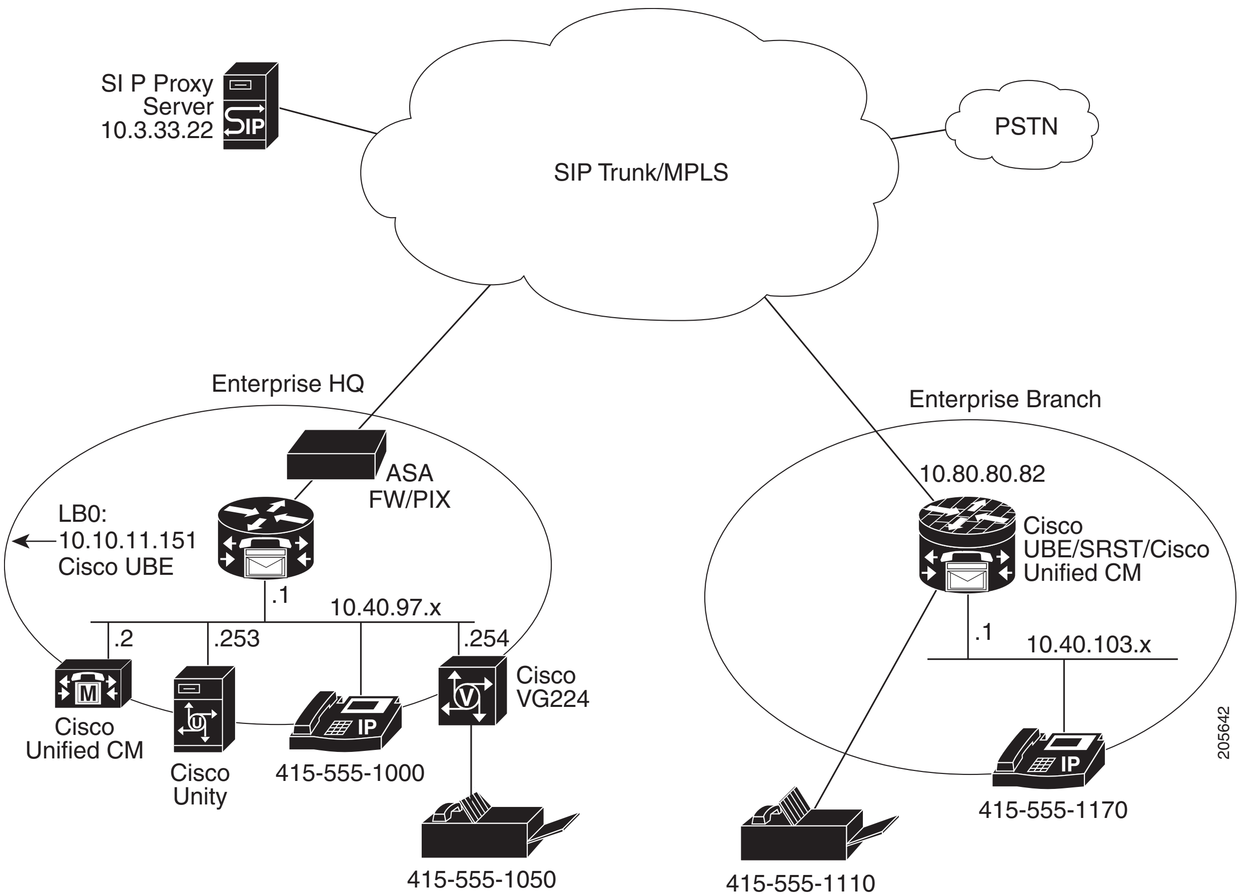
The call admission control (CAC) restrictions that are imposed by Cisco Unified CM for the whole enterprise are as follows:

1. BANDWIDTH—With Static Location. Cisco Unified CM restricts max voice and fax/modem calls to configured bandwidth threshold for both enterprise HQ and the Branch uplinks under “Location/Audio calls information.”
2. NUMBER of CALLS—The Branch Cisco UBE must be configured to activate when in Cisco Unified SRST mode only, which means that the max-calls/bandwidth threshold should be larger than the setting for Cisco Unified CM. Cisco Unified CM would be the triggering mechanism under normal circumstances.
3. CPU%—Cisco UBE at the enterprise HQ and the Branch restrict the maximum voice and fax/modem calls to configured CPU% threshold.
4. MEMORY—Cisco UBE at the enterprise HQ and the Branch restrict the maximum voice and fax/modem calls to the configured available memory threshold.

Test Topology

Figure 8 shows the setup test topology used in example configurations described in the following sections.

Figure 8 Test Topology



Example Configuration Details

The IP addresses used with SIP in the network are as follows:

- HQ Cisco UBE: 10.10.11.151
- Cisco Unified CM: 10.40.97.2
- Service Provider SIP Proxy Server: 10.3.33.22
- Br1 Cisco UBE: 10.80.80.82

The selection of the static codec for either a voice or fax call is implemented by tightly integrating the configurations of Cisco Unified CM and site Cisco UBE. For the DO-to-EO to originate from the originator's local Cisco UBE and for the correct codec to be used with the Service Provider SIP proxy server, the following configuration example has been set up:

1. When the enterprise HQ IP Phone initiates the long-distance call pattern 91xxxxxxxxxx, through Route Pattern/Location/Partition/Trunk configurations on Cisco Unified CM, SIP INVITE with destination 61xxxxxxxxxx is forwarded to the HQ Cisco UBE. A new SIP leg with the destination number 1xxxxxxxxxx and codec g729r8 is offered to the service provider's SIP proxy server by the HQ Cisco UBE after translation and forced EO manipulation.
2. When the enterprise HQ FXS phone initiates the long-distance call pattern 91xxxxxxxxxx, through Route Pattern/Location/Partition/Trunk configurations on Cisco Unified CM, SIP INVITE with destination 71xxxxxxxxxx is forwarded to the HQ Cisco UBE. A new SIP leg with the destination number 1xxxxxxxxxx and codec g711u is offered to the service provider's SIP proxy server by the HQ Cisco UBE after translation and forced EO manipulation.
3. When the Branch 1 IP Phone initiates the long-distance call pattern 91xxxxxxxxxx, through Route Pattern/Location/Partition/Trunk configurations on Cisco Unified CM, SIP INVITE with destination 61xxxxxxxxxx is forwarded to the Branch 1 Cisco UBE. A new SIP leg with the destination number 1xxxxxxxxxx and codec g729r8 is offered to the service provider's SIP proxy server by the Branch 1 Cisco UBE after translation and forced EO manipulation.
4. When Branch 1 FXS phone initiates the long-distance call pattern 91xxxxxxxxxx, through Route Pattern/Location/Partition/Trunk configurations on Cisco Unified CM, SIP INVITE with destination 71xxxxxxxxxx is forwarded to the Branch 1 Cisco UBE. A new SIP leg with the destination number 1xxxxxxxxxx and codec g711u is offered to the service provider's SIP proxy server by the Branch 1 Cisco UBE after translation and forced EO manipulation.

Calls terminating at the enterprise are also tightly controlled as to whether they are IP phone (g729r8) or FXS phone (g711u), where the latter is mainly used for fax/modem purposes. Received calls that do not match these criteria are rejected.

The dial-plan for the enterprise HQ and the Branch sites can be any global numbering plan. In the following example, the same area code was used for the enterprise HQ 1 and the Branch 1.

Enterprise 1 HQ Cisco UBE Example Configuration

The following is a command-line interface (CLI) configuration example for the enterprise 1 HQ Cisco Unified Border Element for the test topology described in Figure 8.

```
Ent1_HQ_CUBE1#
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
```

```
 voice service voip
 address-hiding
 allow-connections sip to sip
 fax protocol pass-through g711ulaw
 modem passthrough nse codec g711ulaw
 sip
  bind control source-interface Loopback0
  bind media source-interface Loopback0
  min-se  2000
  header-passing error-passthru
  options-ping 1200
  listen-port non-secure  5090
  midcall-signaling passthru
!
voice translation-rule 1
 rule 1 /^61/ /1/
 rule 2 /^71/ /1/
!
voice translation-profile OUTGOING-SIP-TRK-DIGIT-STRIP
 translate called 1
!
!
interface Loopback0
 ip address 10.10.11.151 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 10.40.97.1 255.255.255.0
duplex full
 speed 100
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1
 ip address 10.40.99.2 255.255.255.0
duplex full
 speed 100
 media-type rj45
 no keepalive
!
ip rtcp report interval 9000
!
sccp local GigabitEthernet0/0
sccp ccm 10.40.97.2 identifier 5 priority 1 version 6.0
sccp
!
sccp ccm group 10
 associate ccm 5 priority 1
 associate profile 10 register MTP111222333
 associate profile 12 register CON111222333
 associate profile 11 register XCODE111222333
!
dspfarm profile 11 transcode
 codec g711ulaw
 codec g729r8
 maximum sessions 10
 associate application SCCP
!
dspfarm profile 12 conference
 description conference bridge
 codec g711ulaw
 codec g729r8
 maximum sessions 10
 associate application SCCP
!
```

```
dspfarm profile 10 mtp
 codec g711ulaw
 maximum sessions software 5
 associate application SCCP
!
dial-peer voice 2000 voip
 description *** Voice: LAN to WAN - Incoming Dial-Peer ***
 huntstop
 codec g729r8
 session protocol sipv2
 incoming called-number 6T
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2001 voip
 description *** Voice: LAN to WAN - Outgoing Dial-Peer ***
 translation-profile outgoing OUTGOING-SIP-TRK-DIGIT-STRIP
 huntstop
 destination-pattern 6T
 codec g729r8
 voice-class sip early-offer forced
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.3.33.22
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2100 voip
 description *** Voice: WAN to LAN - Incoming Dial-Peer ***
 huntstop
 codec g729r8
 session protocol sipv2
 incoming called-number 415T
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2101 voip
 description *** Voice: WAN to LAN - Outgoing Dial-Peer ***
 huntstop
 destination-pattern 415T
 codec g729r8
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.40.97.2
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 3000 voip
 description *** Fax: LAN to WAN - Incoming Dial-Peer ***
 huntstop
 session protocol sipv2
 incoming called-number 7T
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3001 voip
 description *** Fax: LAN to WAN - Outgoing Dial-Peer ***
 translation-profile outgoing OUTGOING-SIP-TRK-DIGIT-STRIP
 huntstop
 destination-pattern 7T
 voice-class sip early-offer forced
 max-redirects 5
 session protocol sipv2
```

```
 session target ipv4:10.3.33.22
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3100 voip
 description *** Fax: WAN to LAN - Incoming Dial-Peer ***
 huntstop
 session protocol sipv2
 incoming called-number 415555105[0,1]
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3101 voip
 description *** Fax: WAN to LAN - Outgoing Dial-Peer ***
 huntstop
 destination-pattern 415555105[0,1]
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.40.97.2
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
gateway
 media-inactivity-criteria all
 timer receive-rtcp 5
 timer receive-rtp 180
!
sip-ua
 keepalive target ipv4:10.3.33.22
 authentication username yyyy password 7 xxxxxxxxxx
 no remote-party-id
 retry invite 2
 retry bye 2
 retry cancel 2
 timers keepalive active 600
 reason-header override
 g729-annexb override
!
Ent1_HQ_CUBE1#
```

Enterprise 1 HQ Cisco Unified CM Example Configuration

The following example shows the required field and parameter entries for example configuration of the Cisco Unified CM for the topology shown in Figure 8. Parameters are entered using the Cisco Unified CM GUI. The example parameters windows entries are shown in following sections:

- Configuring the Cisco Unified CM System Parameters, page 33
- Configuring the Cisco Unified CM Call Routing Parameters, page 63
- Configuring the Cisco Unified CM Media Resources Parameters, page 78
- Configuring the Cisco Unified CM Voice Mail Parameters, page 95
- Configuring the Cisco Unified CM Device Parameters, page 102

Configuring the Cisco Unified CM System Parameters

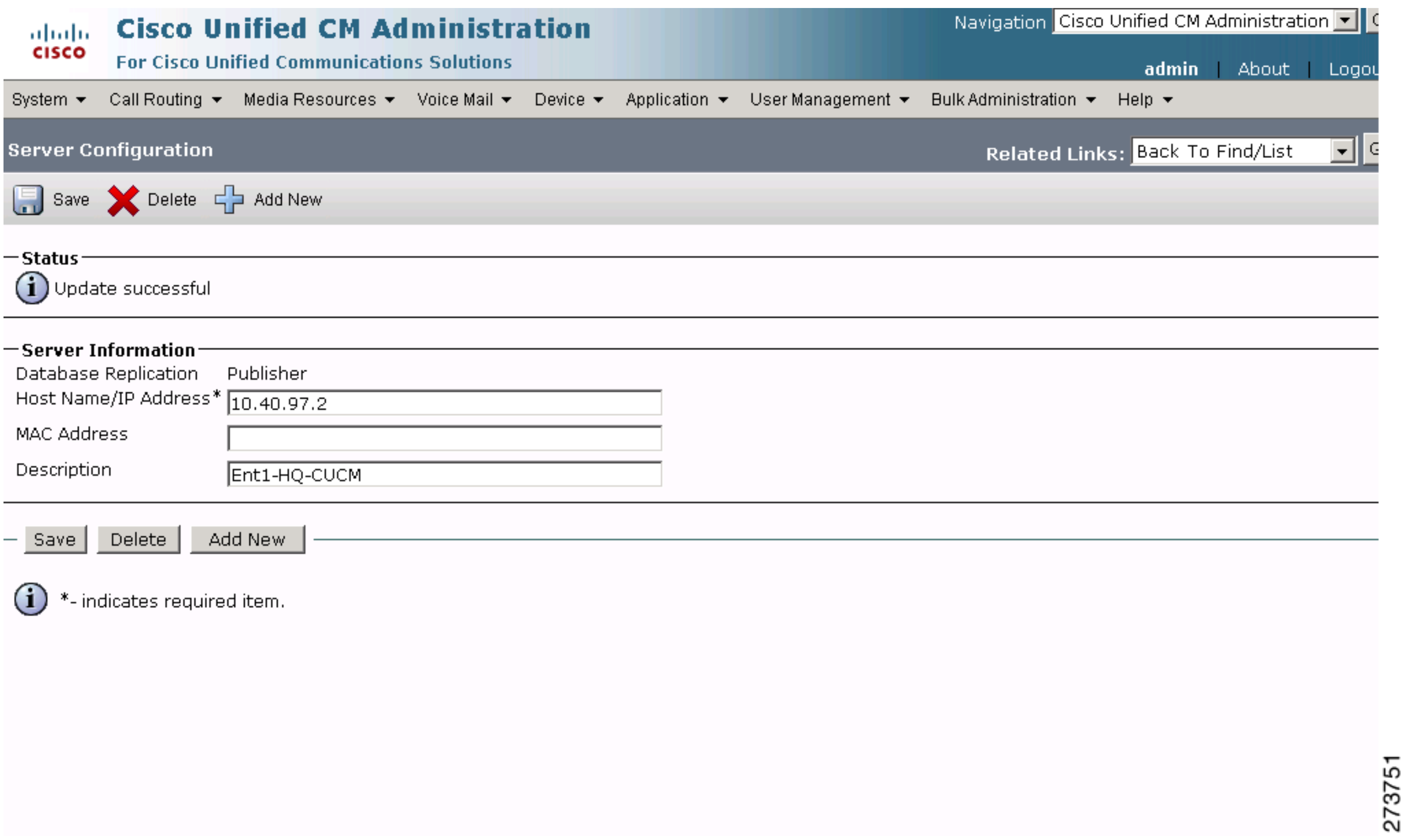
Use the Cisco Unified Communications Manager Administration window to configure system parameters. The system parameter example configurations are shown in the following sections:

- System: Server Parameters, page 33
- System: Region Parameters, page 34
- System: Device Pool Parameters, page 47
- System: Location Parameters, page 56

System: Server Parameters

To configure the system server parameters for the Cisco Unified CM, click on **System** > **Server** menu in the Cisco Unified CM Administration window.

Figure 9 System Server Enterprise 1 HQ Cisco Unified CM Administration Window



System: Region Parameters

To configure the system region parameters for the Cisco Unified CM, click **System** > **Region** menu in the Cisco Unified CM Administration window.

Figure 10 System Region Cisco Unified CM Administration Window

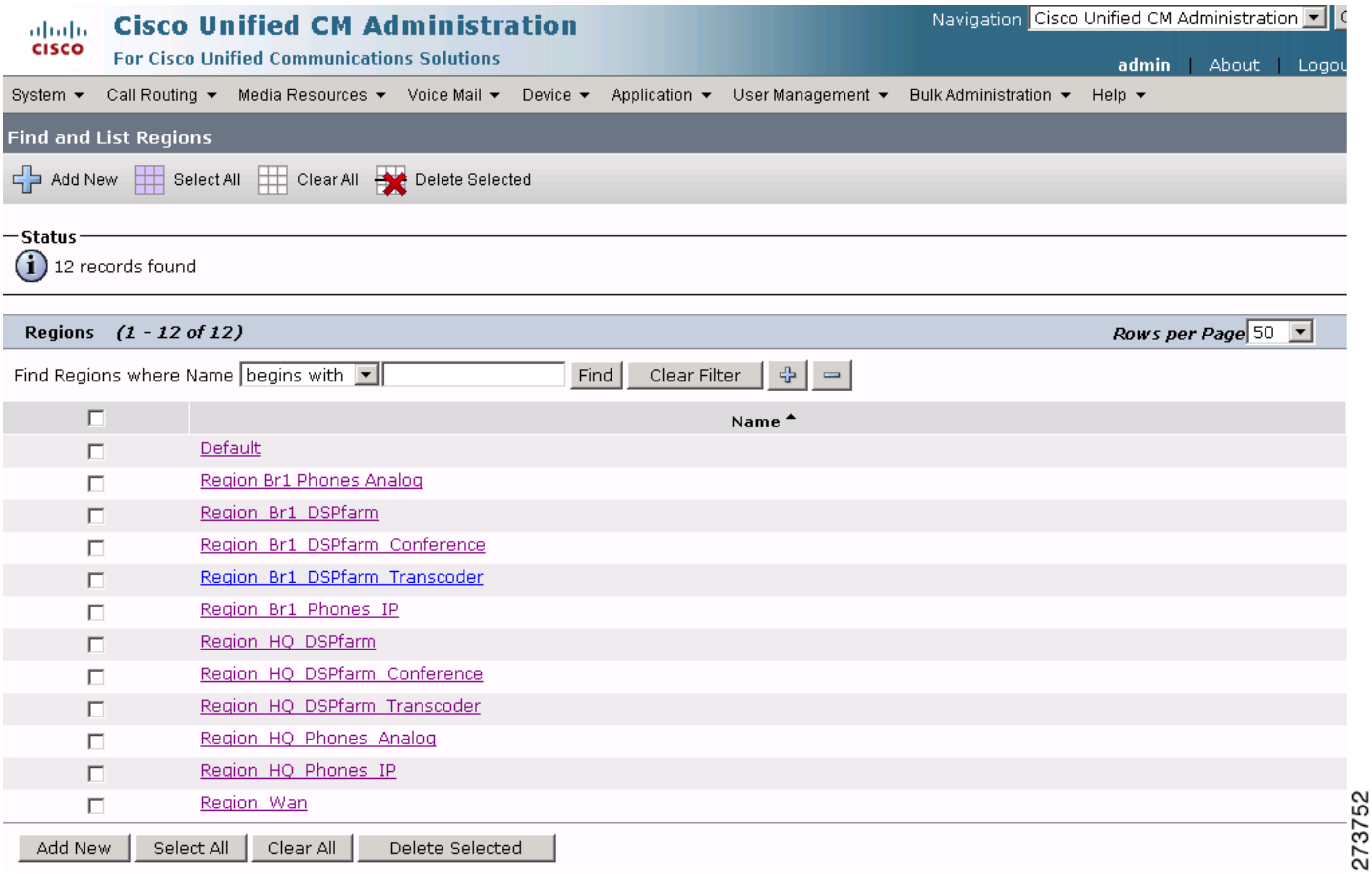


Figure 11 System Region Default Cisco Unified CM Administration Window

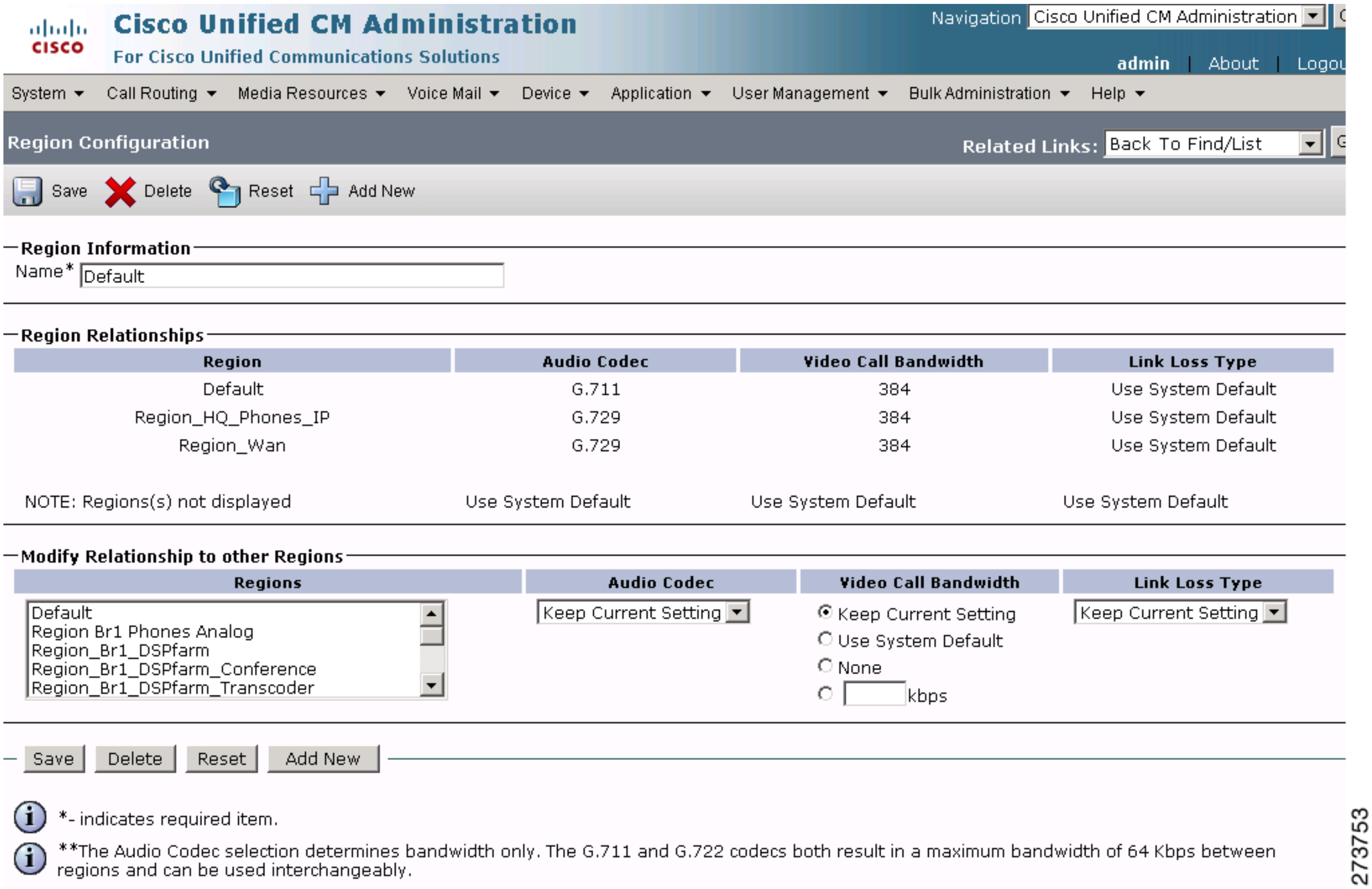
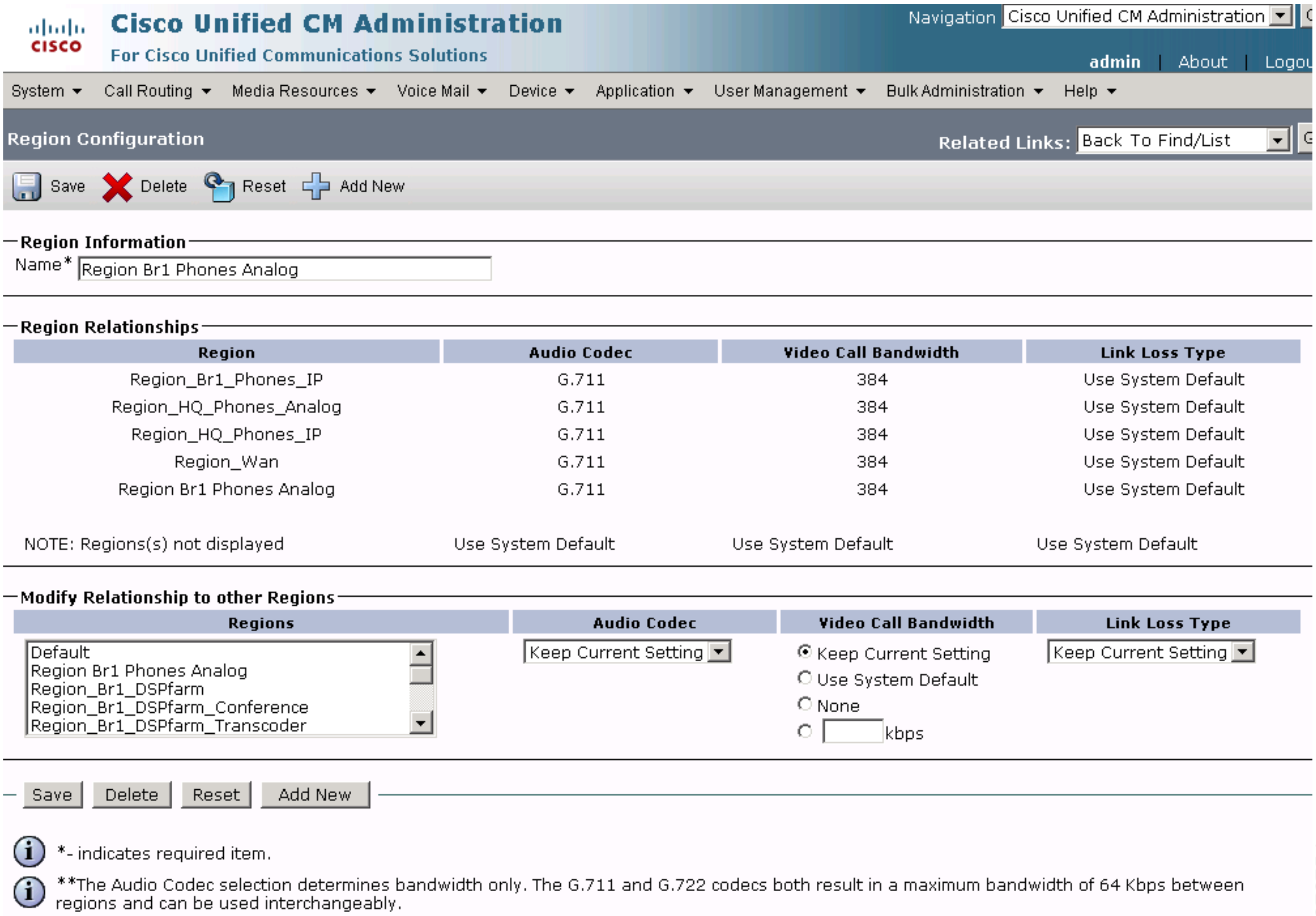
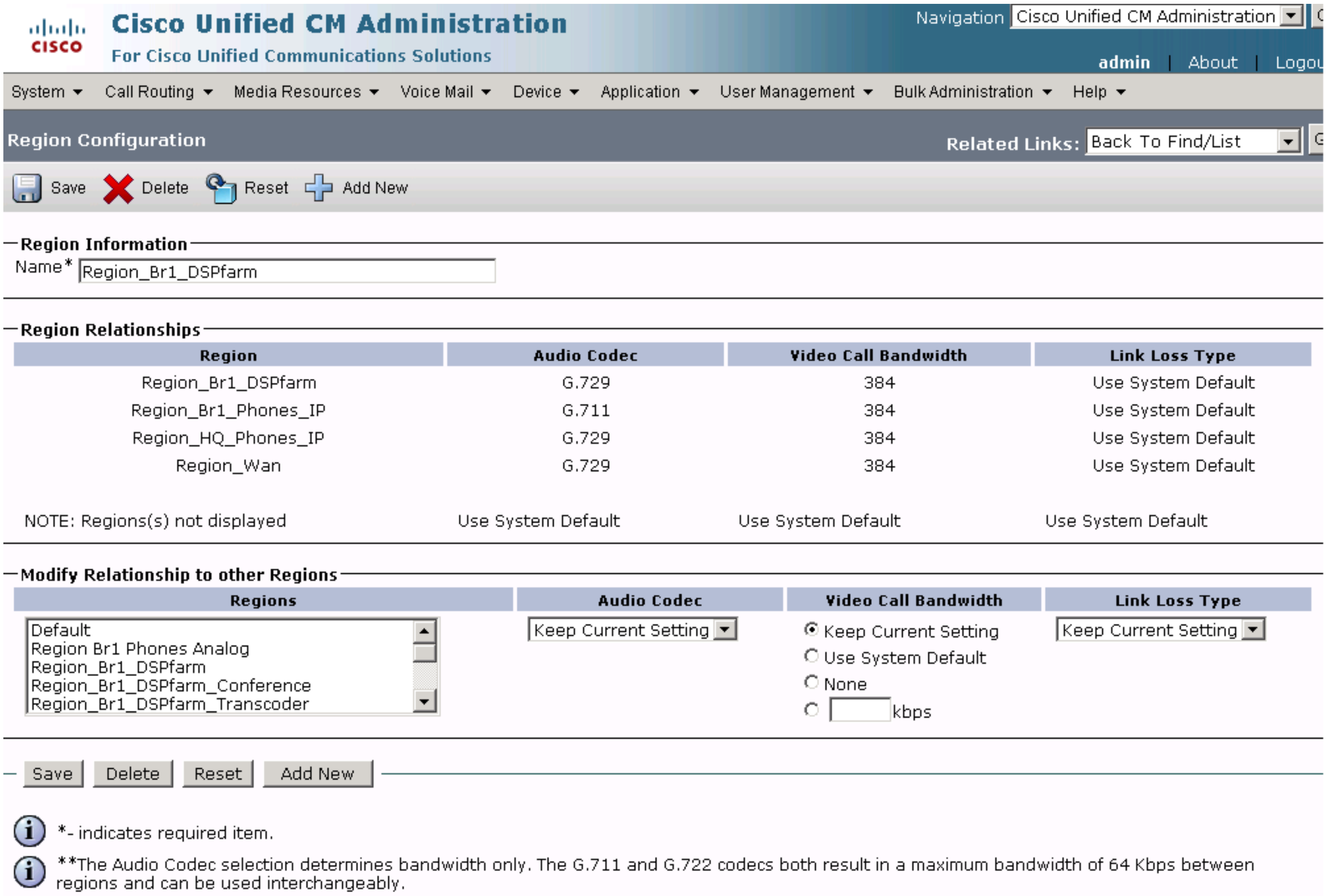


Figure 12 System Region-Region Branch 1 Phones Analog Cisco Unified CM Administration Window



273754

Figure 13 System Region-Region Branch 1 DSP Farm Cisco Unified CM Administration Window



273755

Figure 14 System Region-Region Branch 1 DSP Farm Conference Cisco Unified CM Administration Window

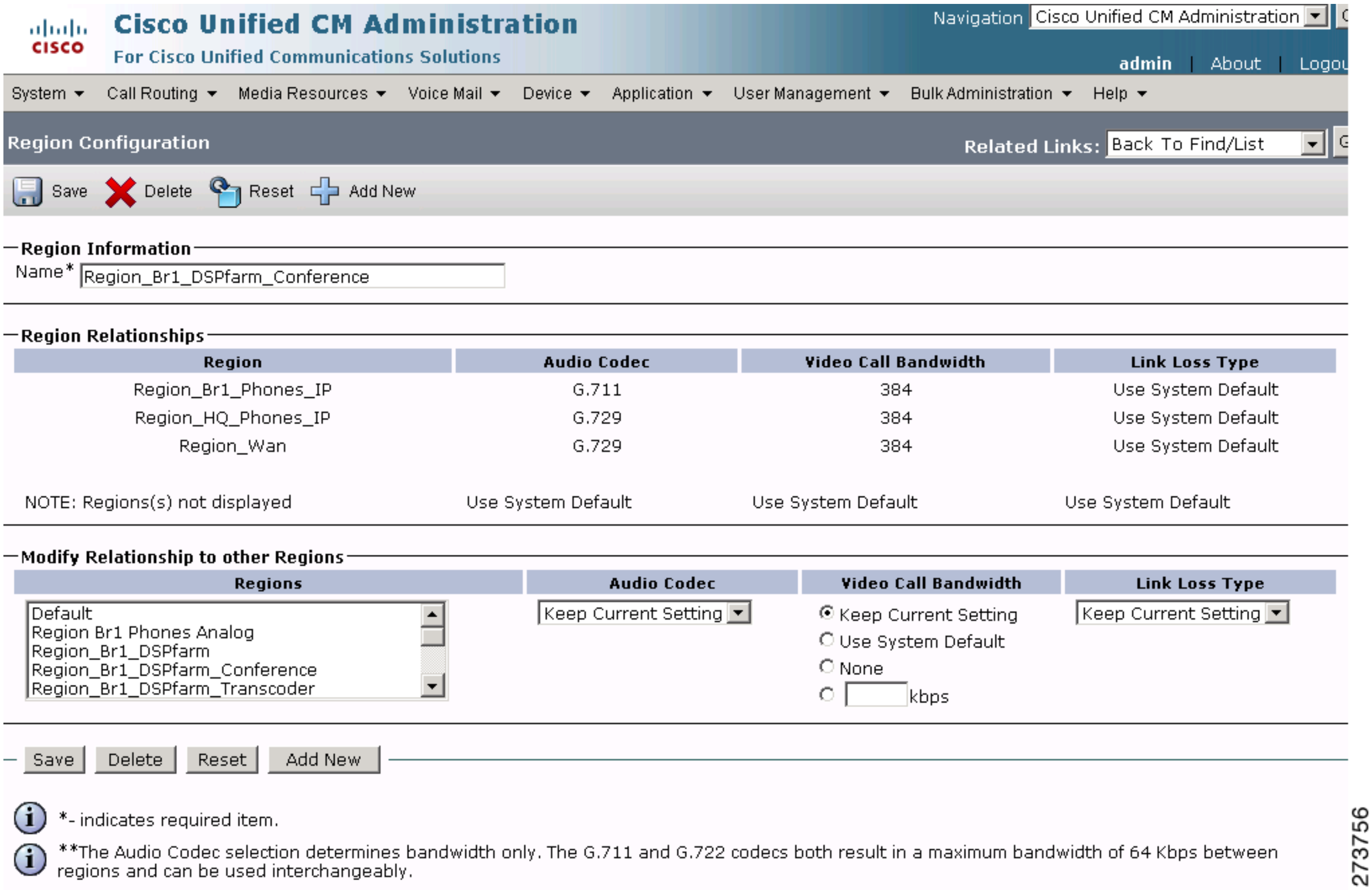
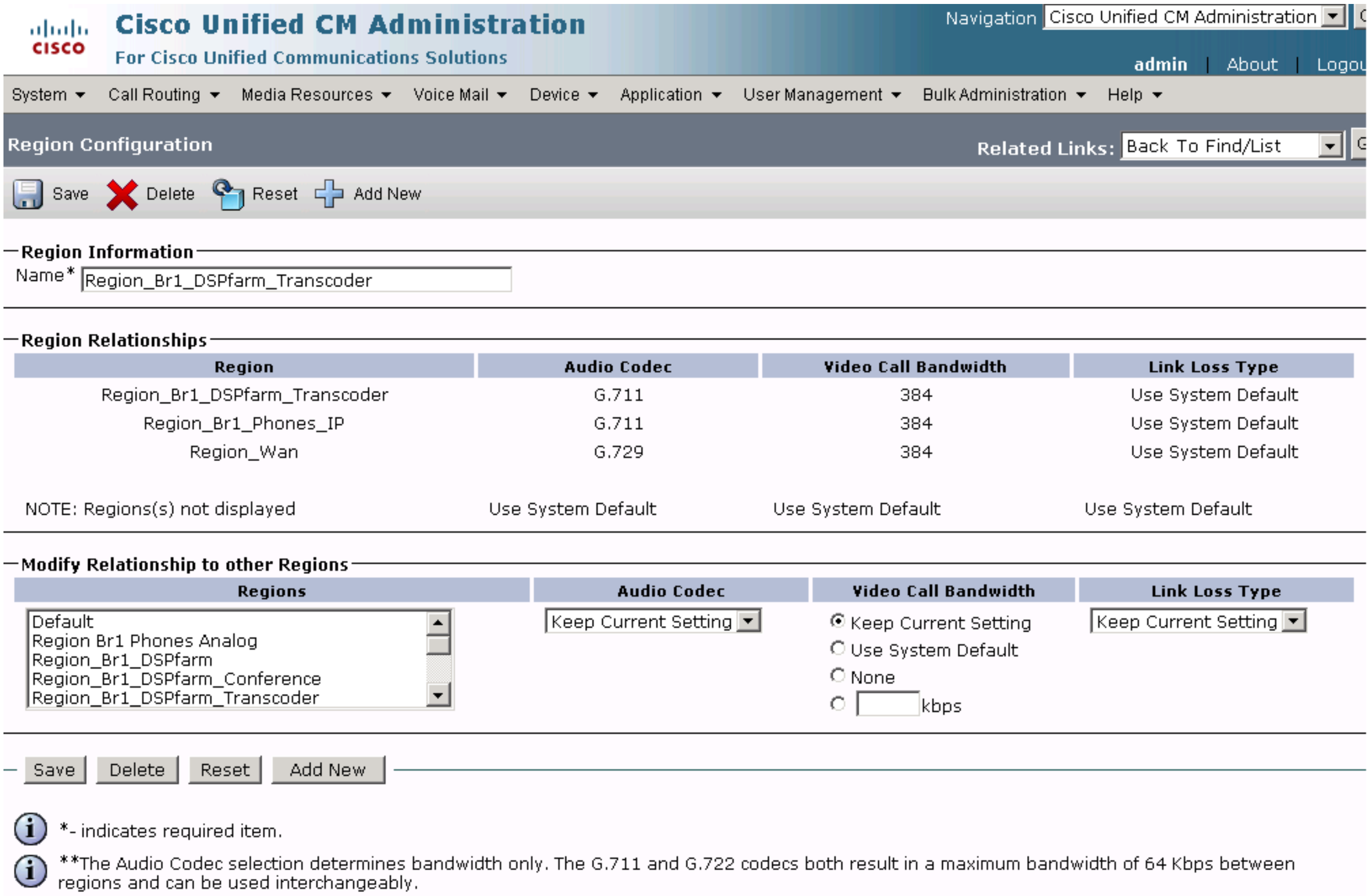
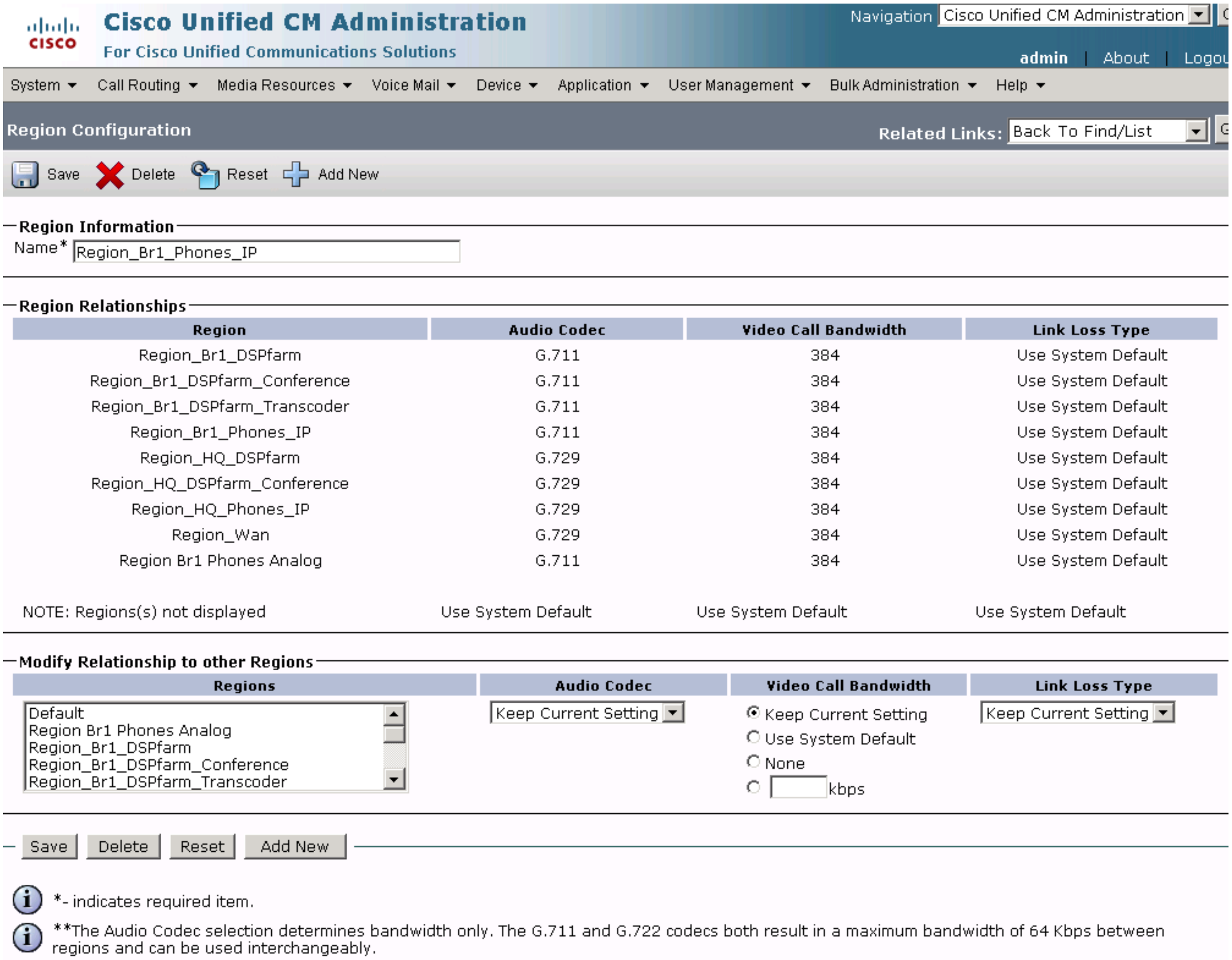


Figure 15 System Region-Region Branch 1 DSP Farm Transcoder Cisco Unified CM Administration Window



273757

Figure 16 System Region-Region Branch 1 Phones IP Cisco Unified CM Administration Window



273758

Figure 17 System Region-Region HQ DSP Farm Cisco Unified CM Administration Window

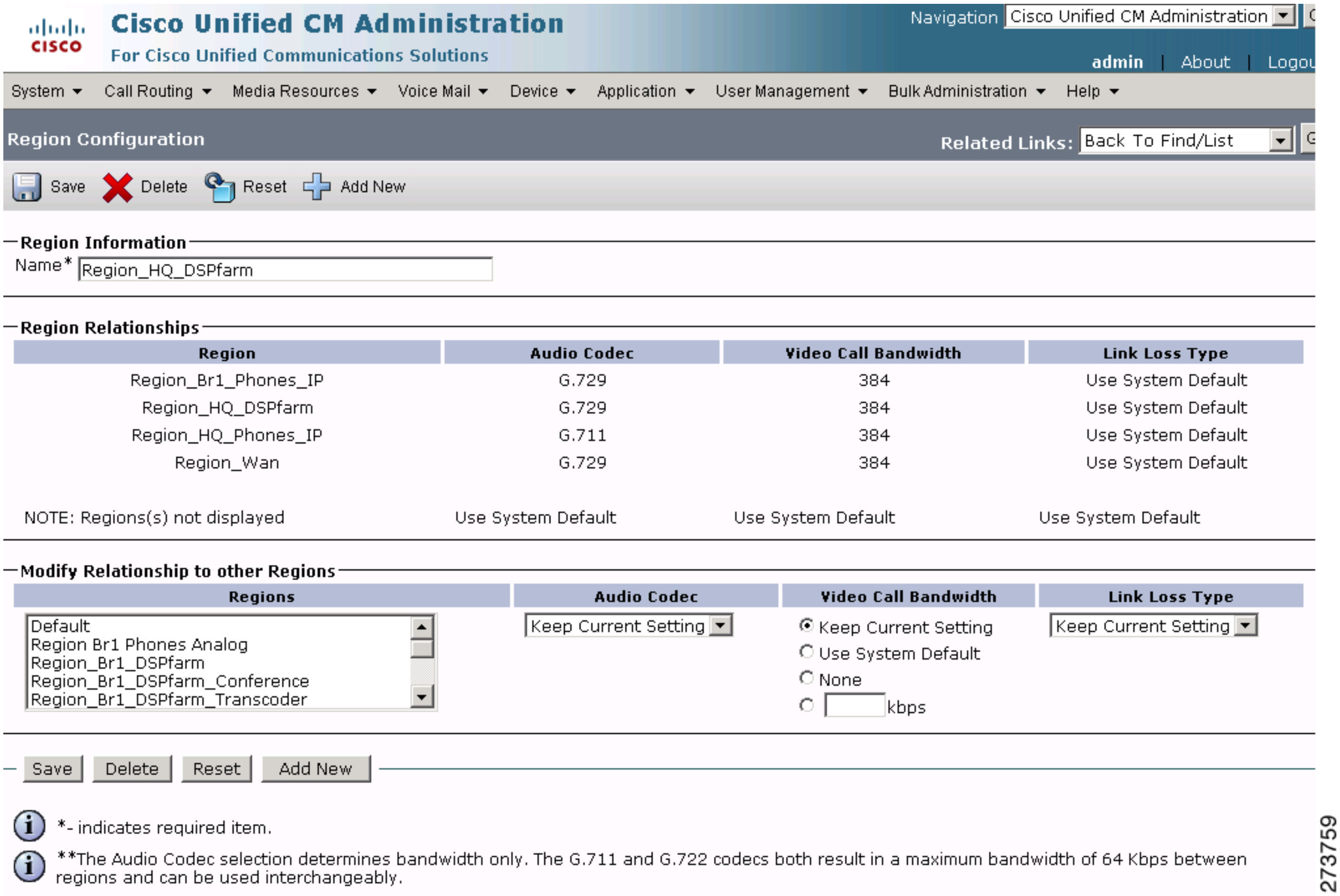
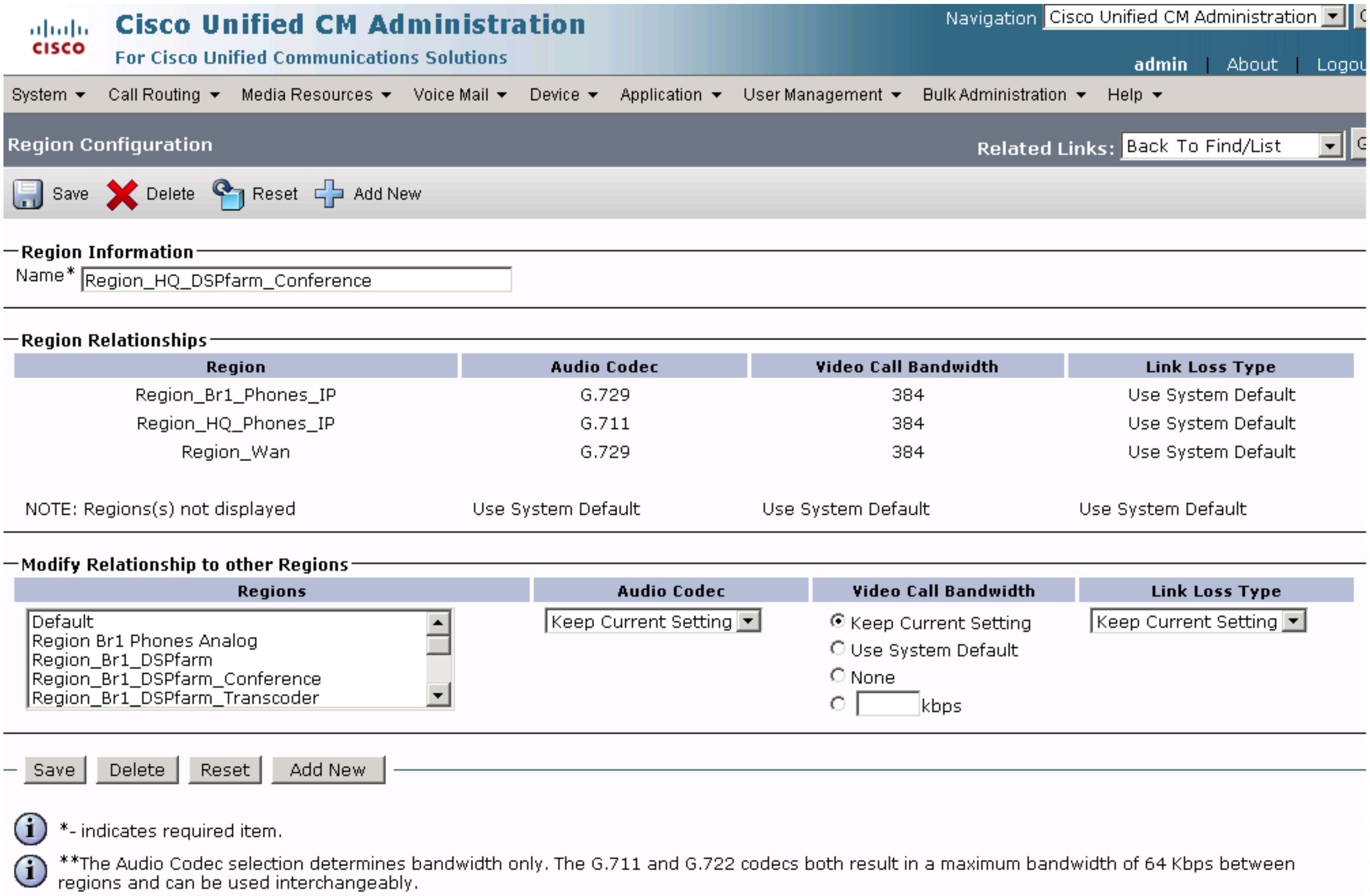


Figure 18 System Region-Region HQ DSP Farm Conference Cisco Unified CM Administration Window



273760

Figure 19 System Region-Region HQ DSP Farm Transcoder Cisco Unified CM Administration Window

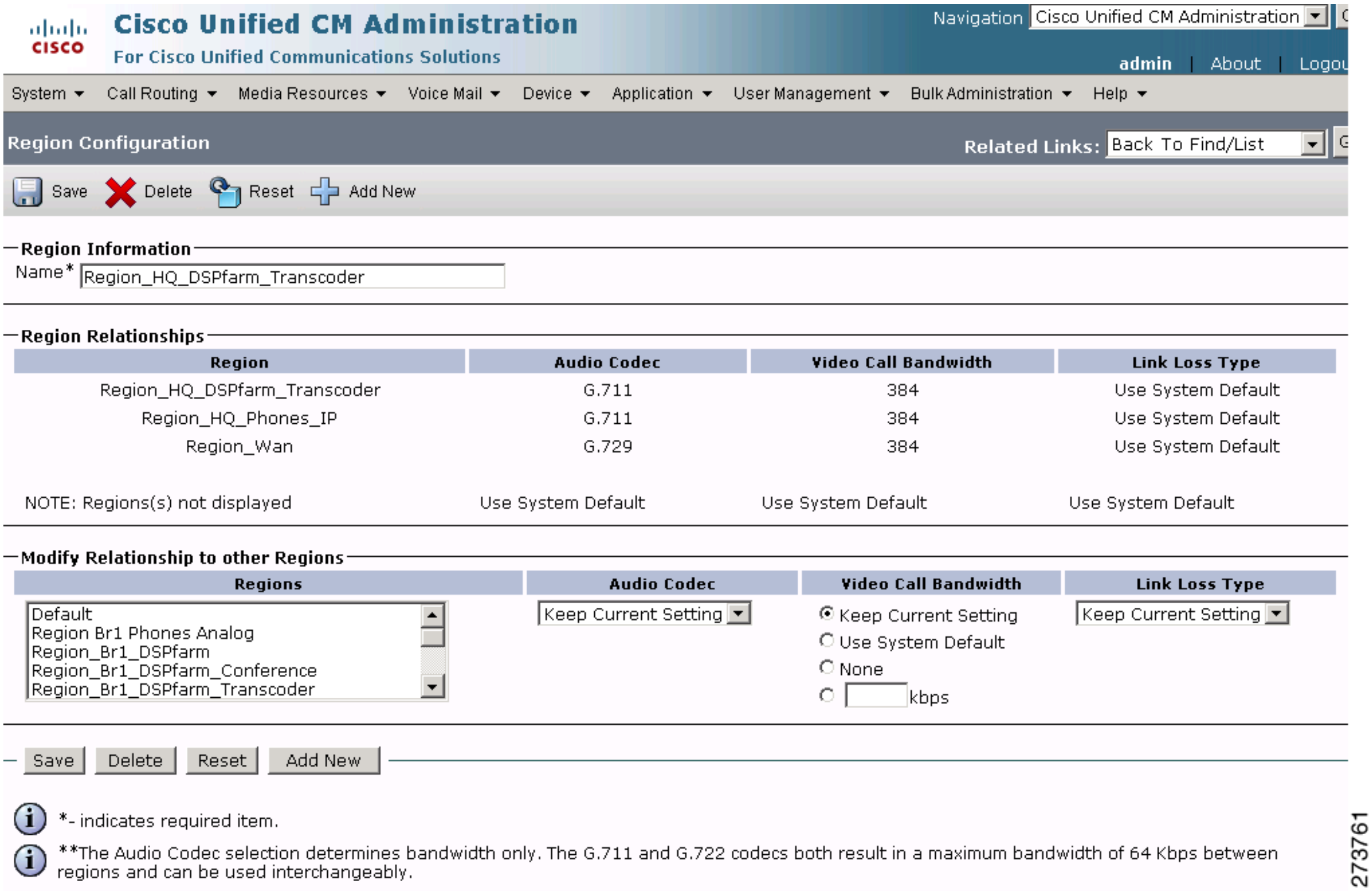
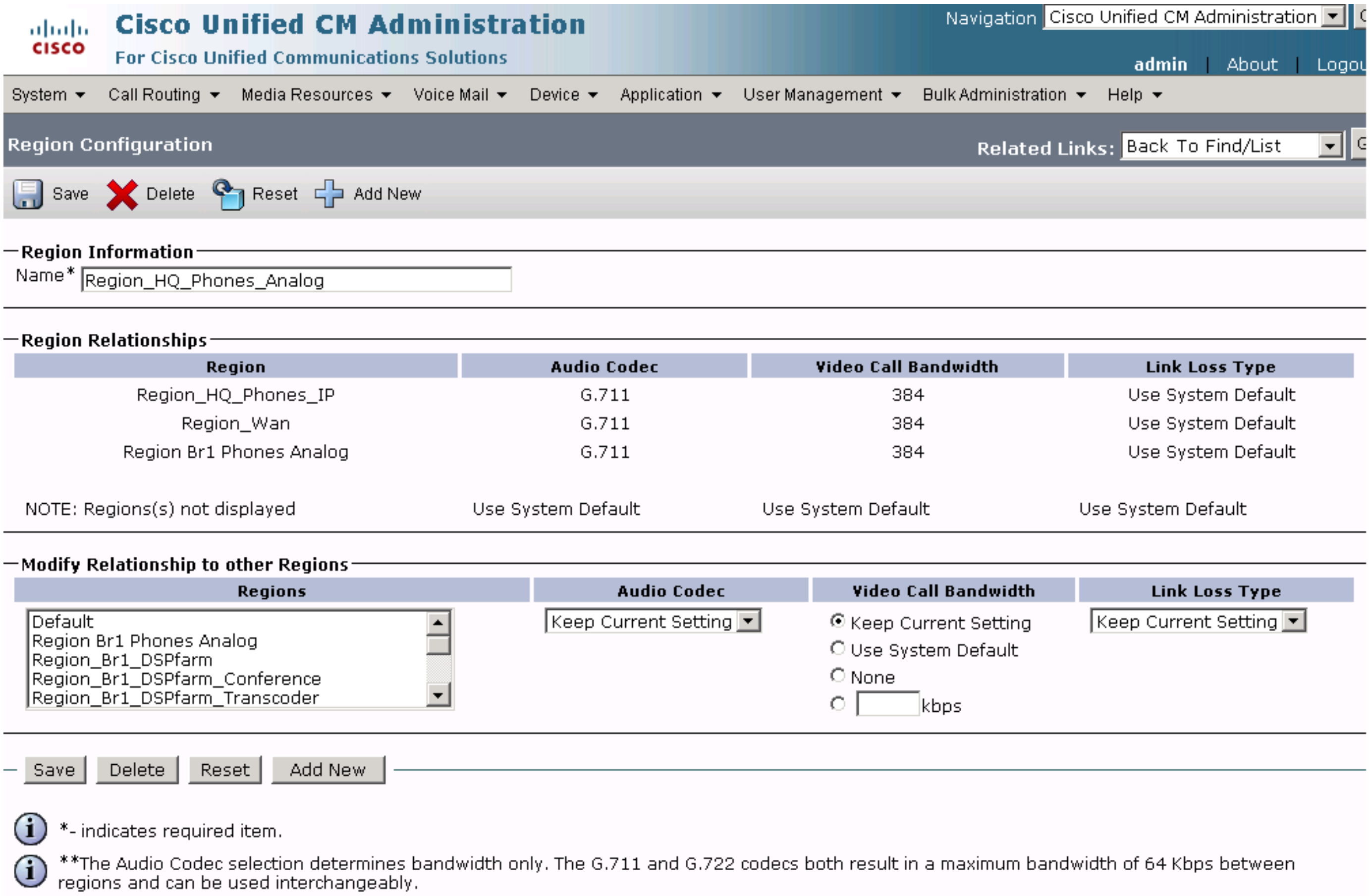


Figure 20 System Region-Region HQ Phones Analog Cisco Unified CM Administration Window



273762

Figure 21 System Region-Region HQ Phones IP Cisco Unified CM Administration Window

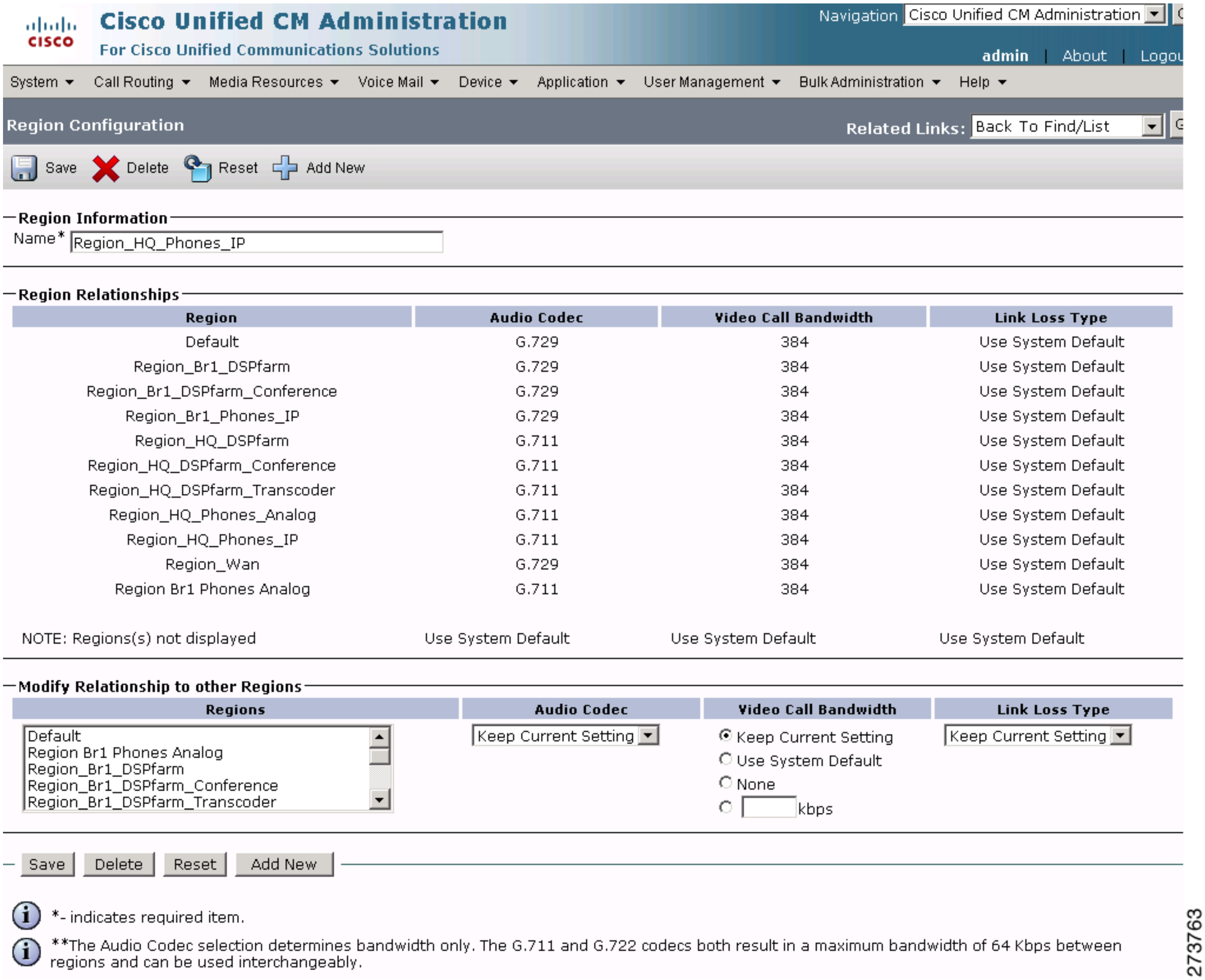
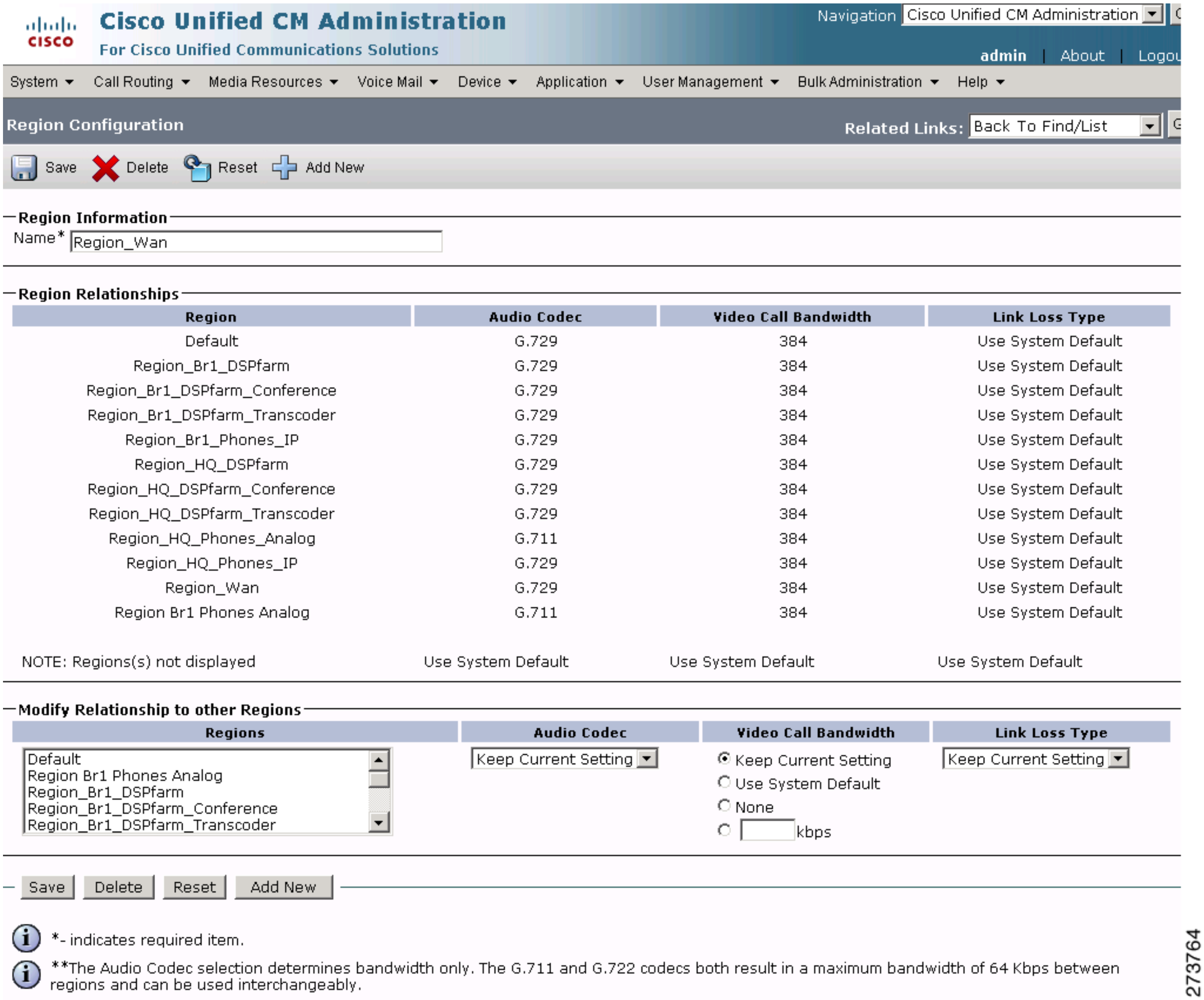


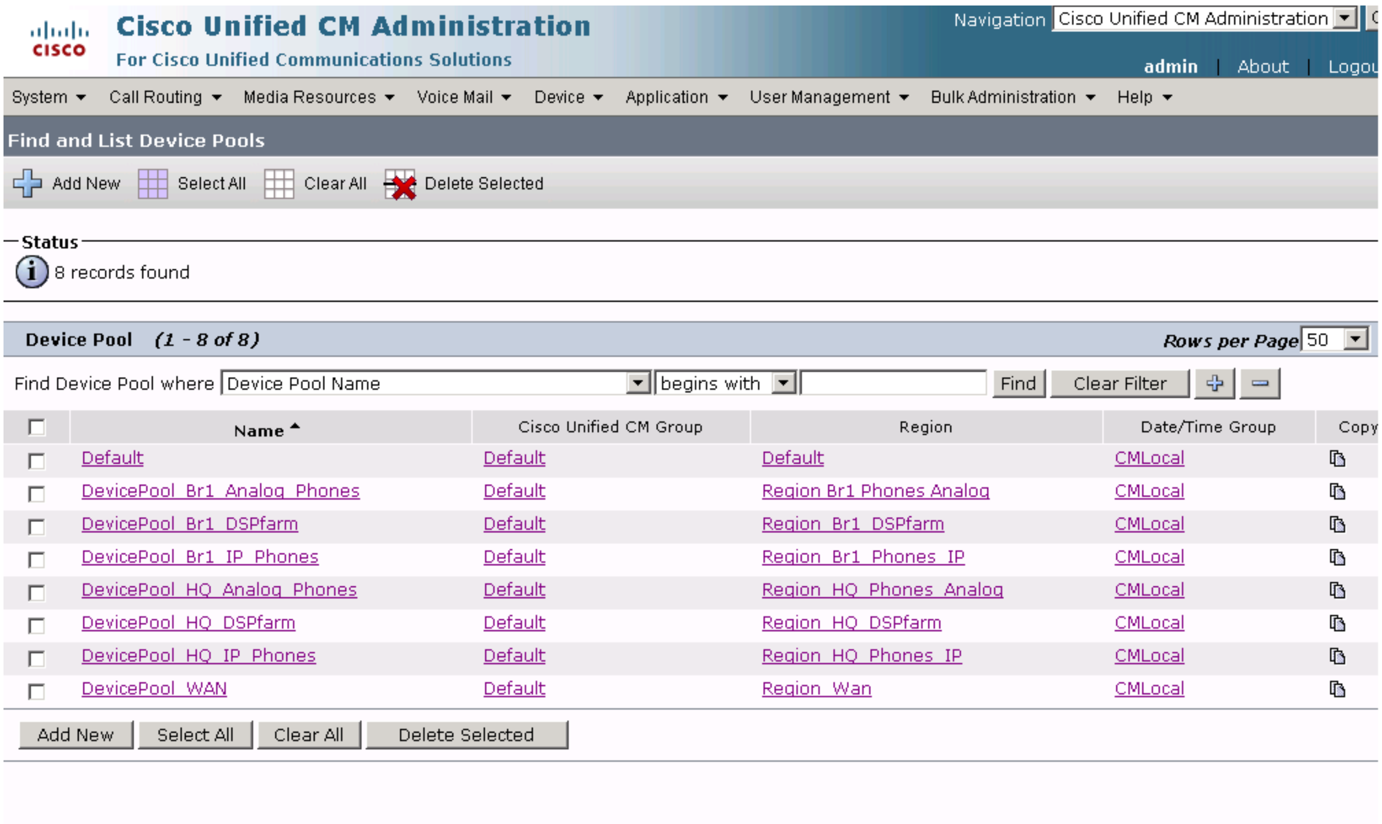
Figure 22 System Region-Region WAN Cisco Unified CM Administration Window



System: Device Pool Parameters

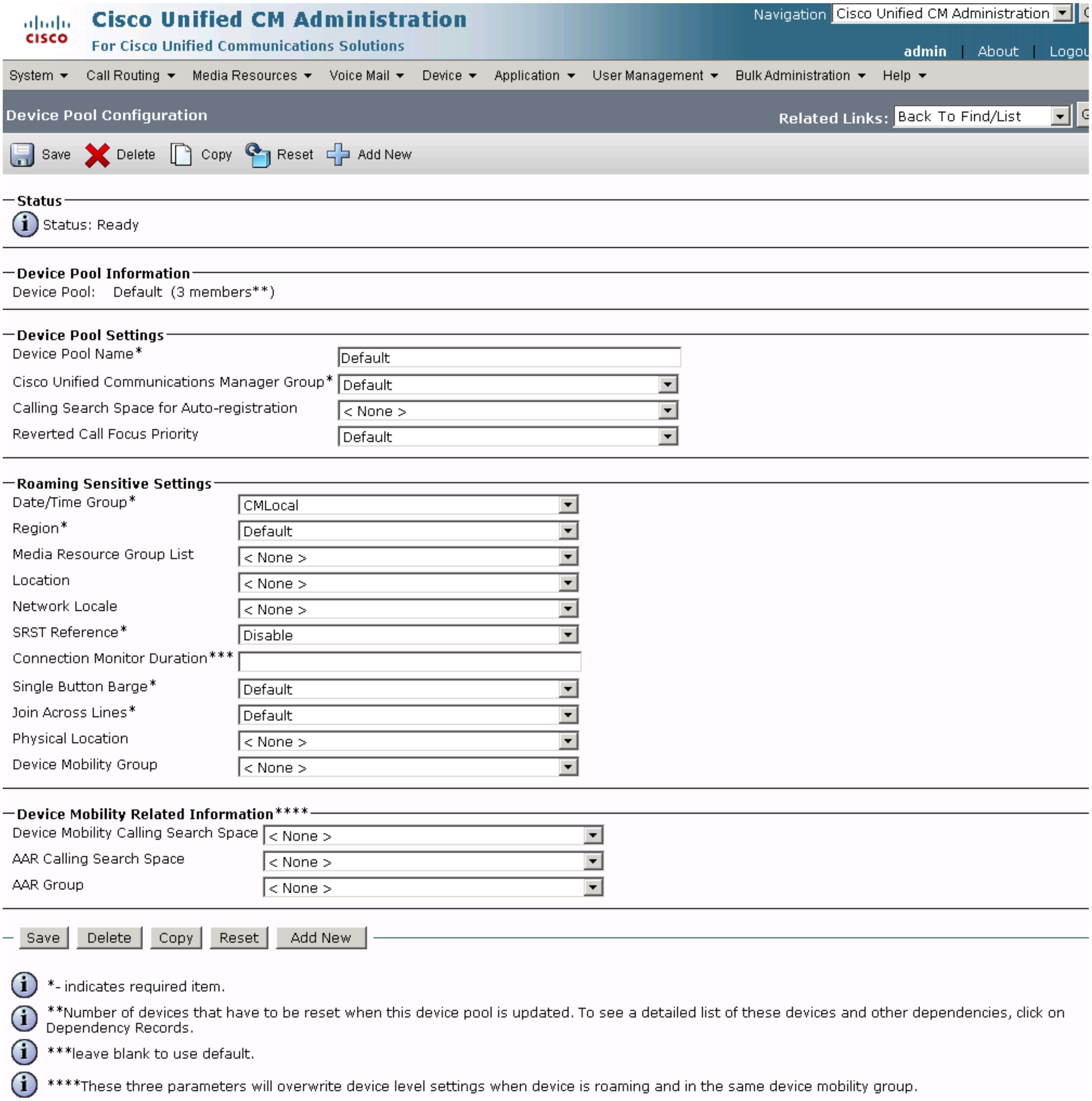
To configure the system device pool parameters for the Cisco Unified CM, click **System** > **Device Pool** menu in the Cisco Unified CM Administration window.

Figure 23 System Device Pool Cisco Unified CM Administration Window



273765

Figure 24 System Device Pool Default Cisco Unified CM Administration Window



273766

Figure 25 System Device Pool-DevicePool Branch 1 Analog Phones Cisco Unified CM Administration Window

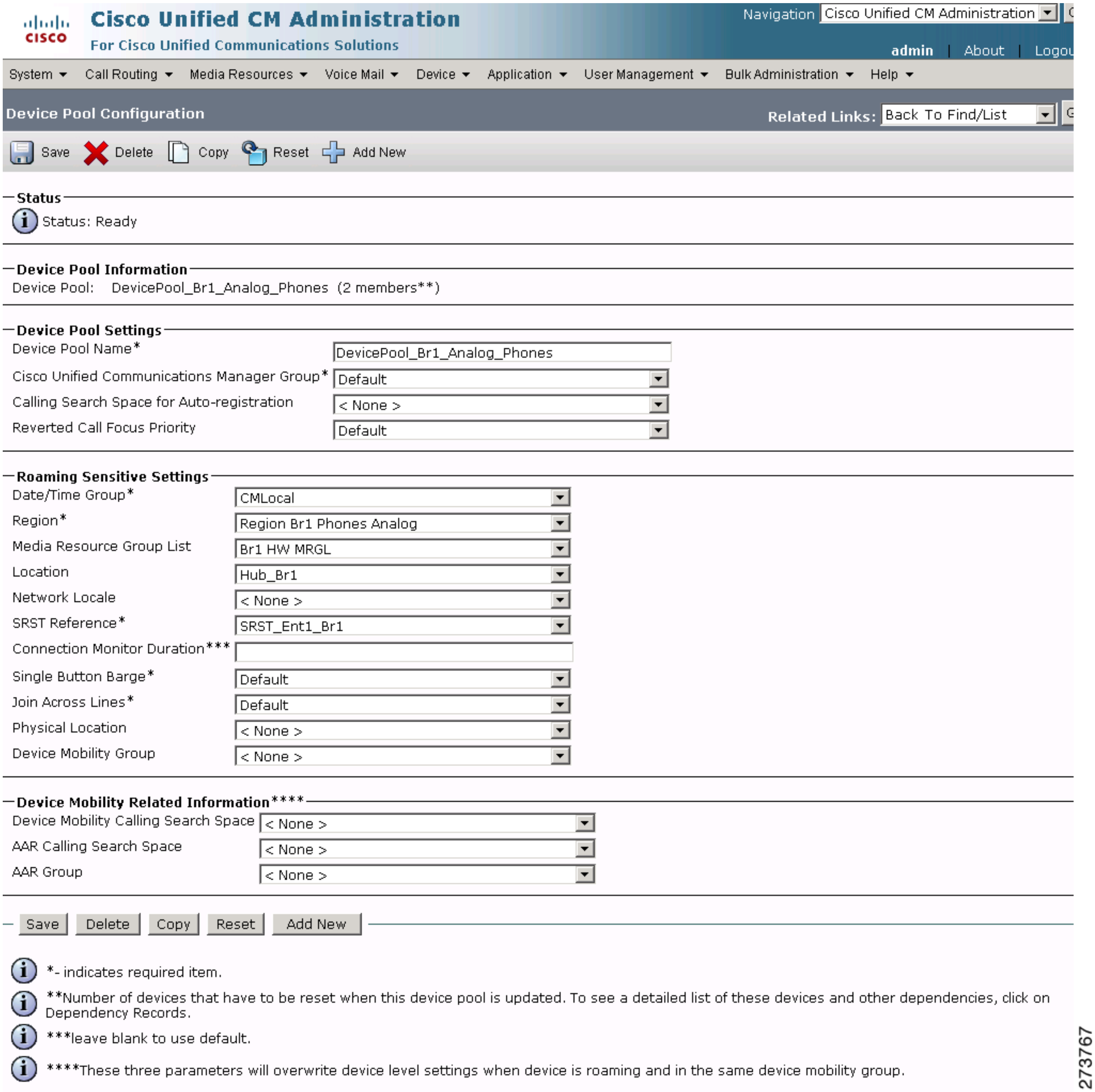
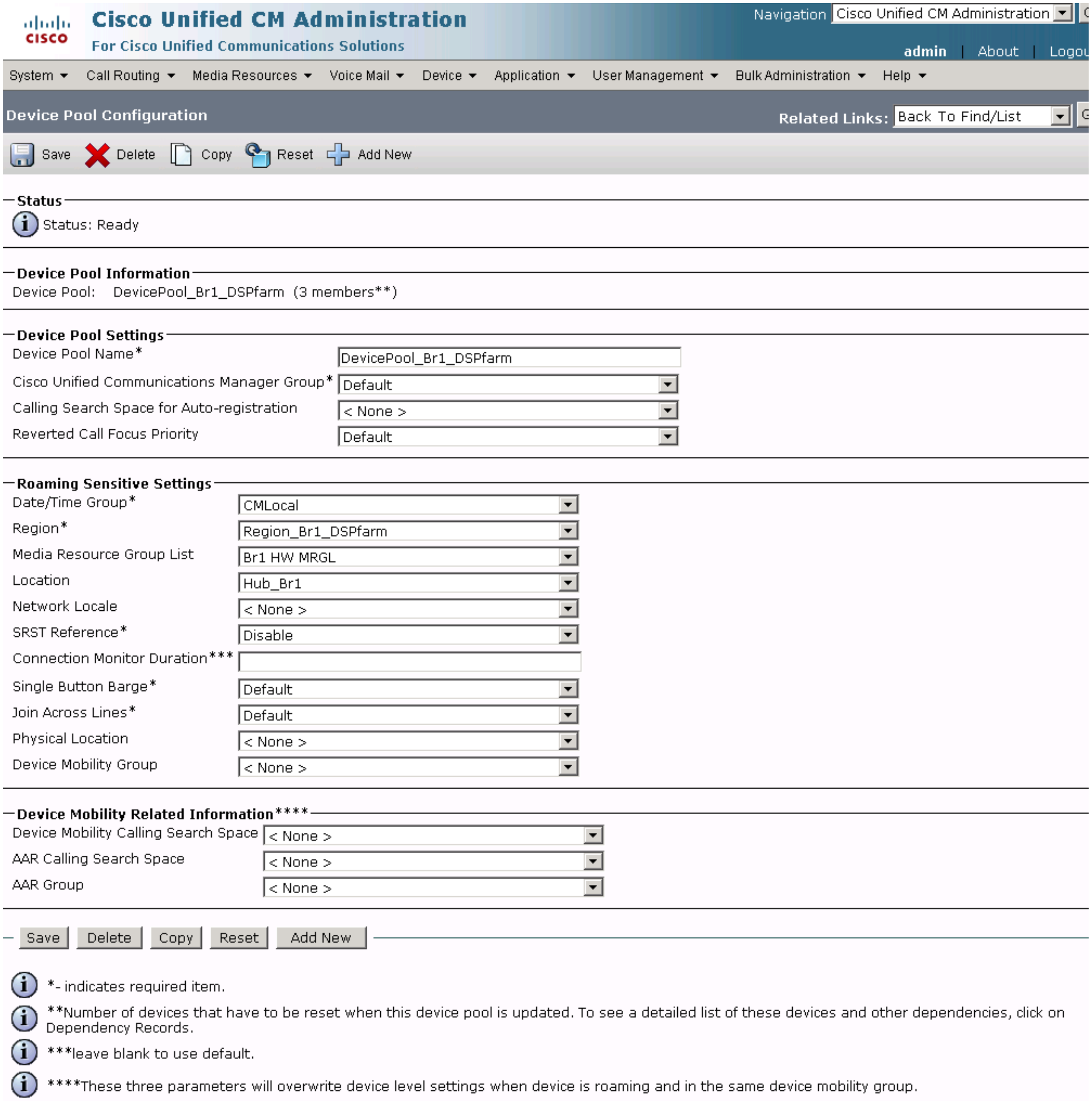
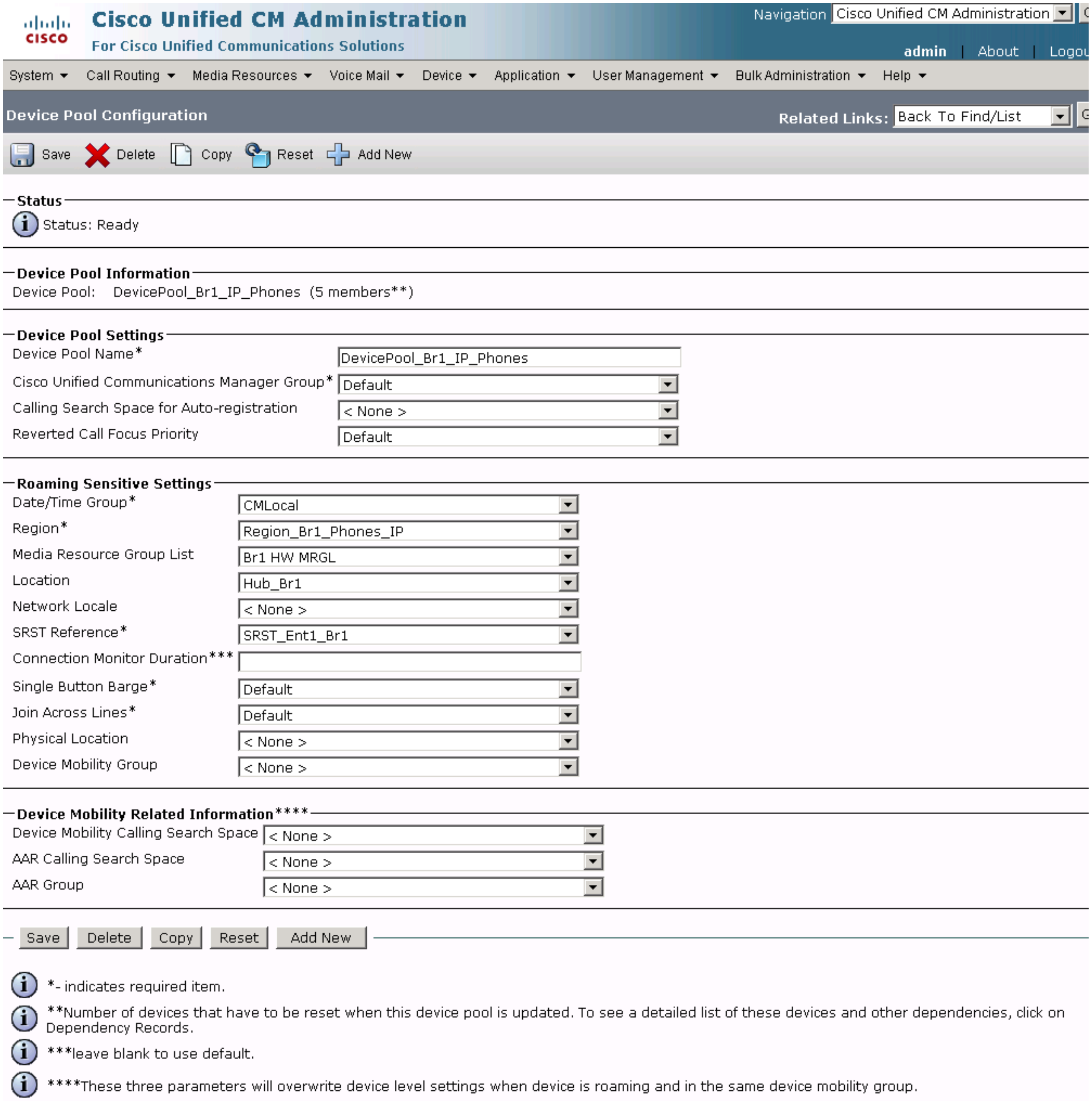


Figure 26 System Device Pool-DevicePool Branch 1 DSP Farm Cisco Unified CM Administration Window



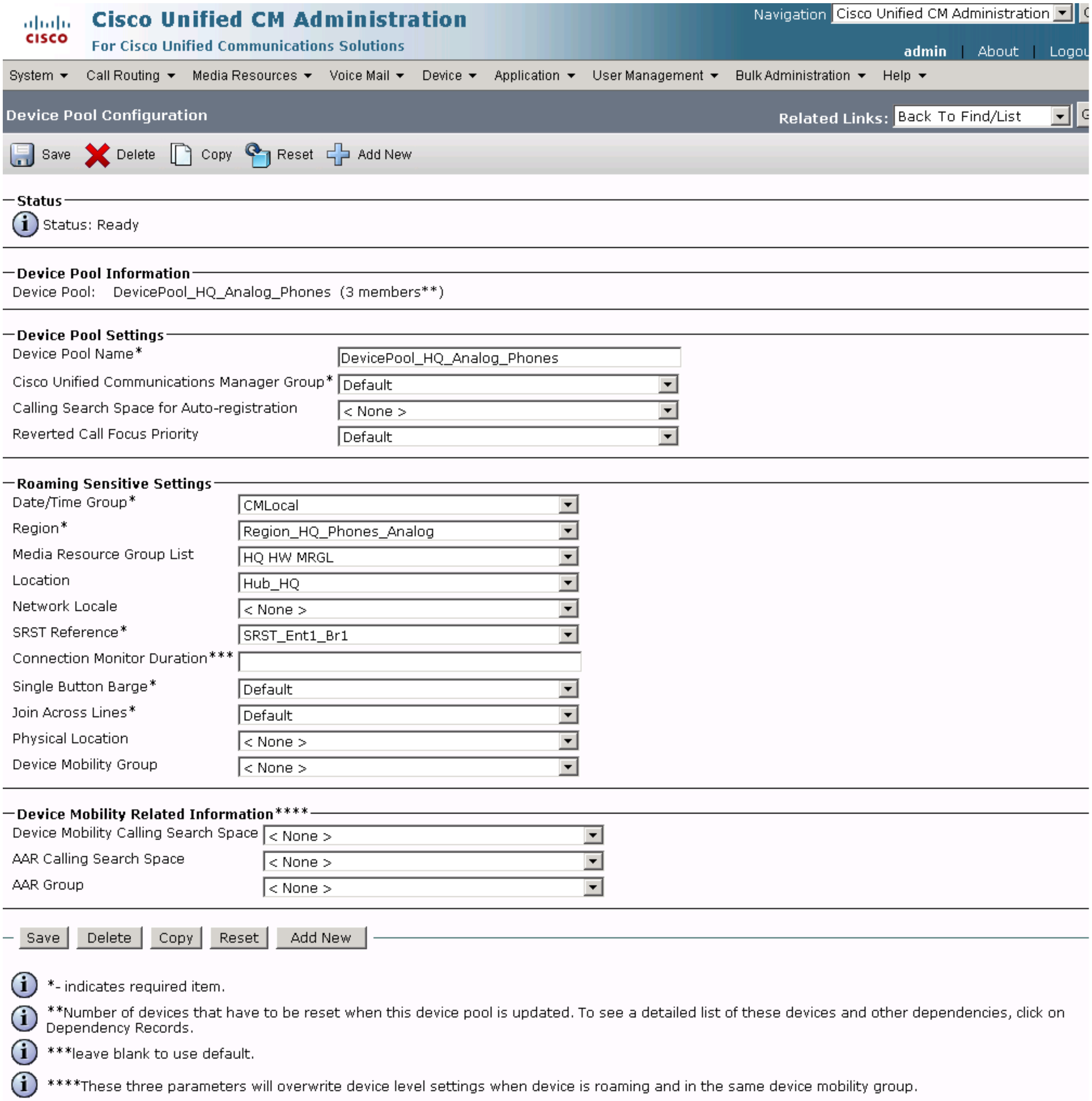
273768

Figure 27 System Device Pool-DevicePool Branch 1 IP Phones Cisco Unified CM Administration Window



273769

Figure 28 System Device Pool-DevicePool HQ Analog Phones Cisco Unified CM Administration Window



273770

Figure 29 System Device Pool-DevicePool HQ DSP Farm Cisco Unified CM Administration Window

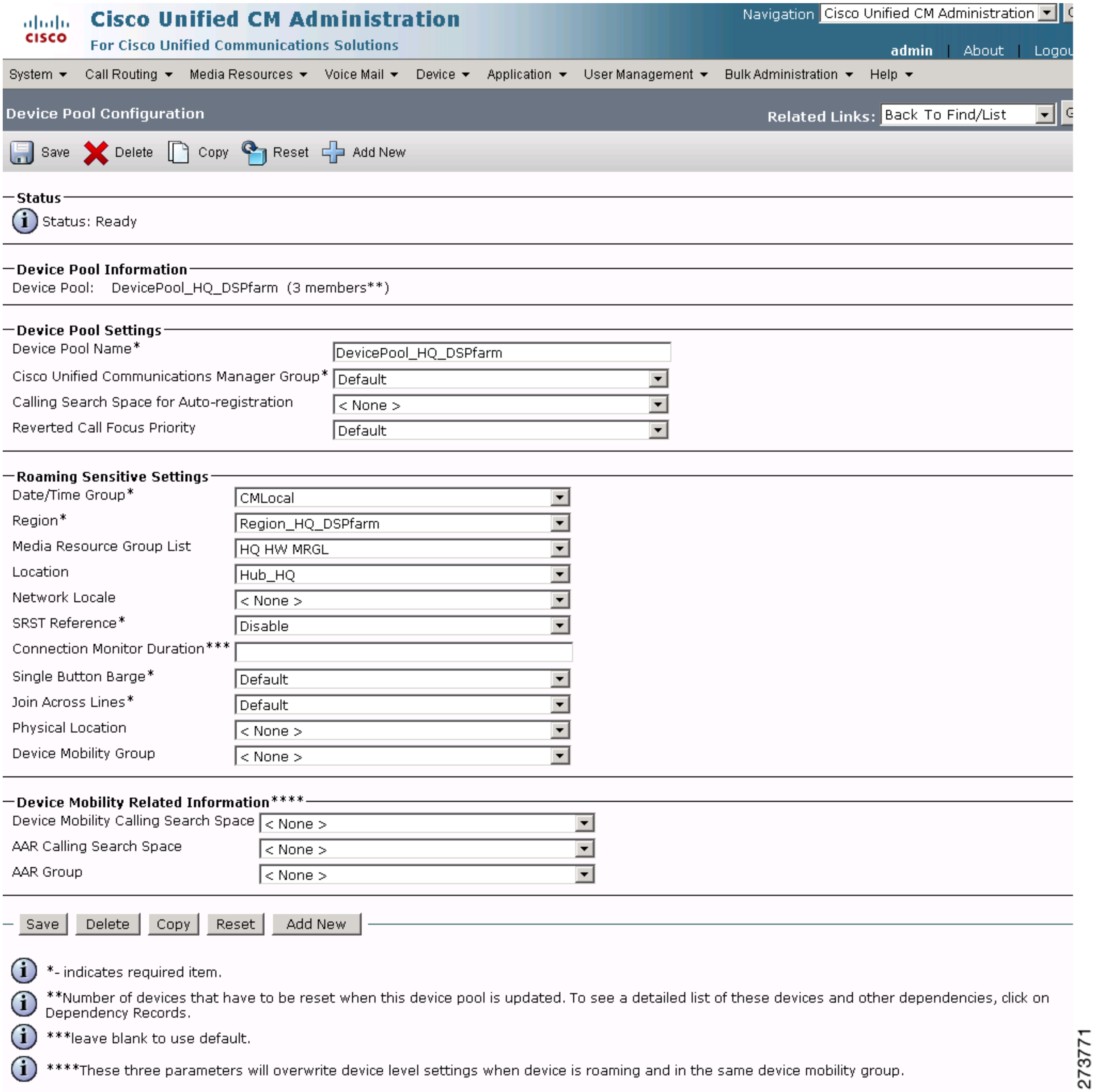
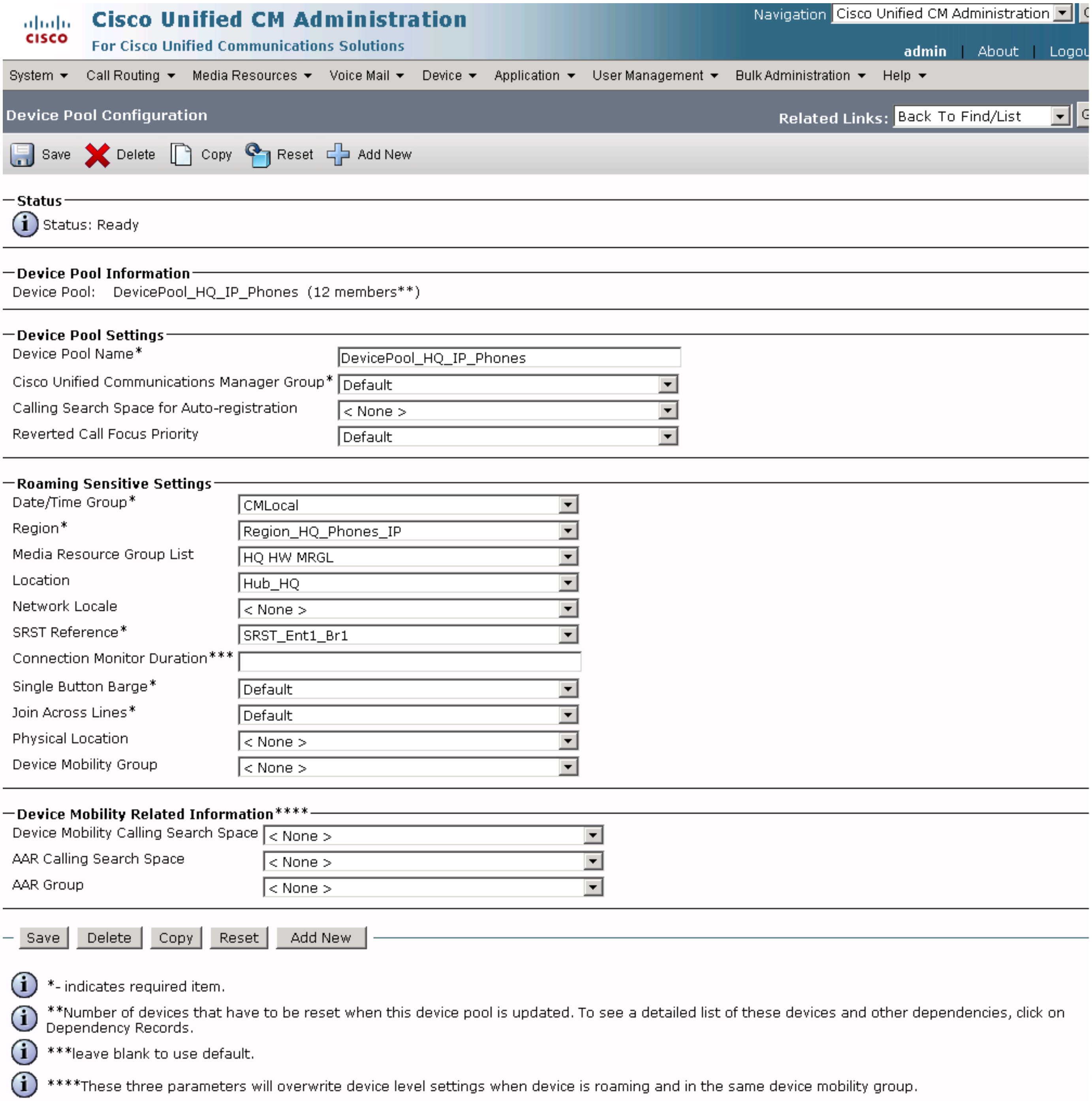
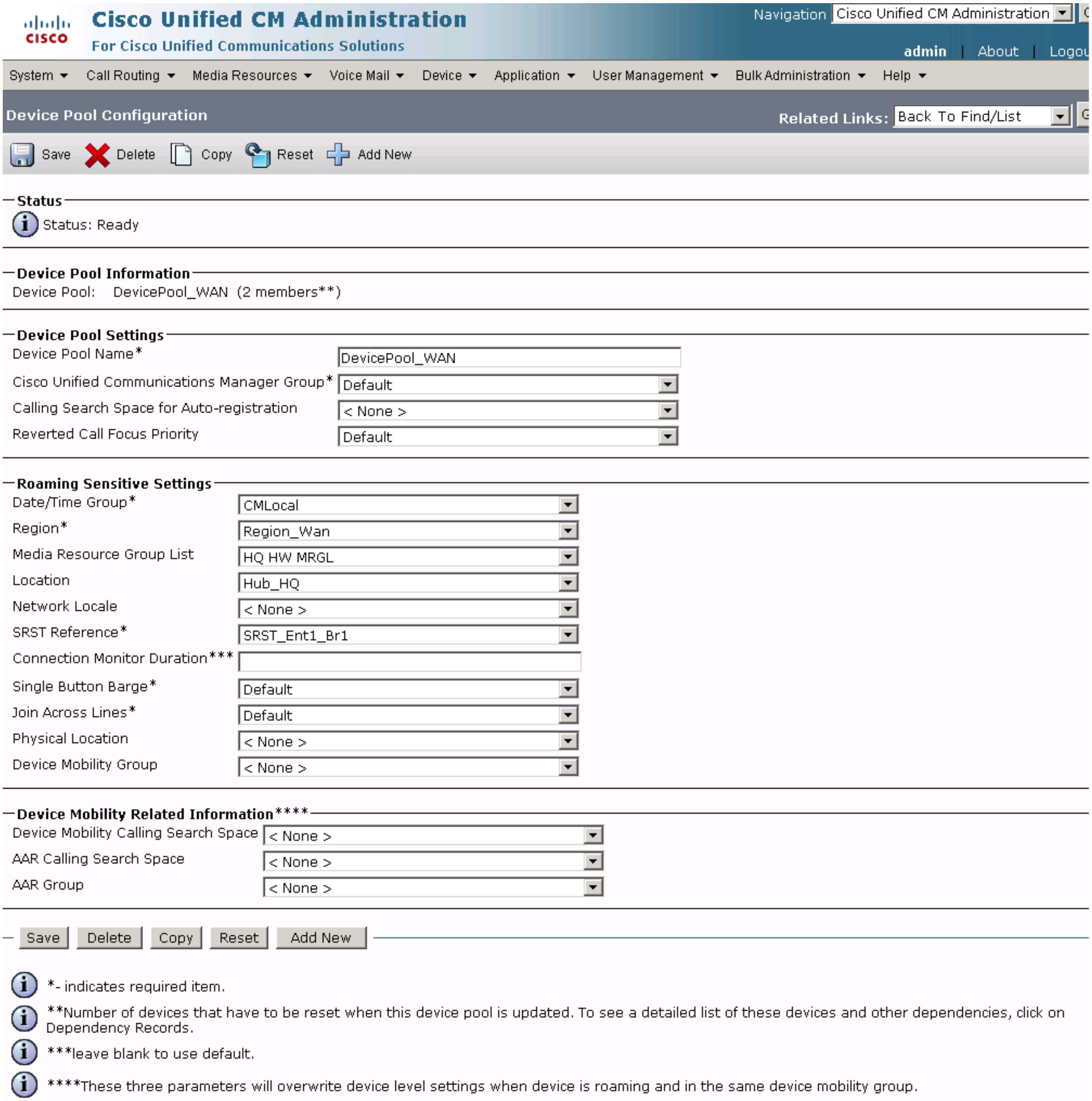


Figure 30 System Device Pool-DevicePool HQ IP Phones Cisco Unified CM Administration Window



273772

Figure 31 System DevicePool-DevicePool WAN Cisco Unified CM Administration Window



273773

System: Location Parameters

To configure the system location parameters for the Cisco Unified CM, click **System** > **Location** menu in the Cisco Unified CM Administration window.

Figure 32 System Location Cisco Unified CM Administration Window

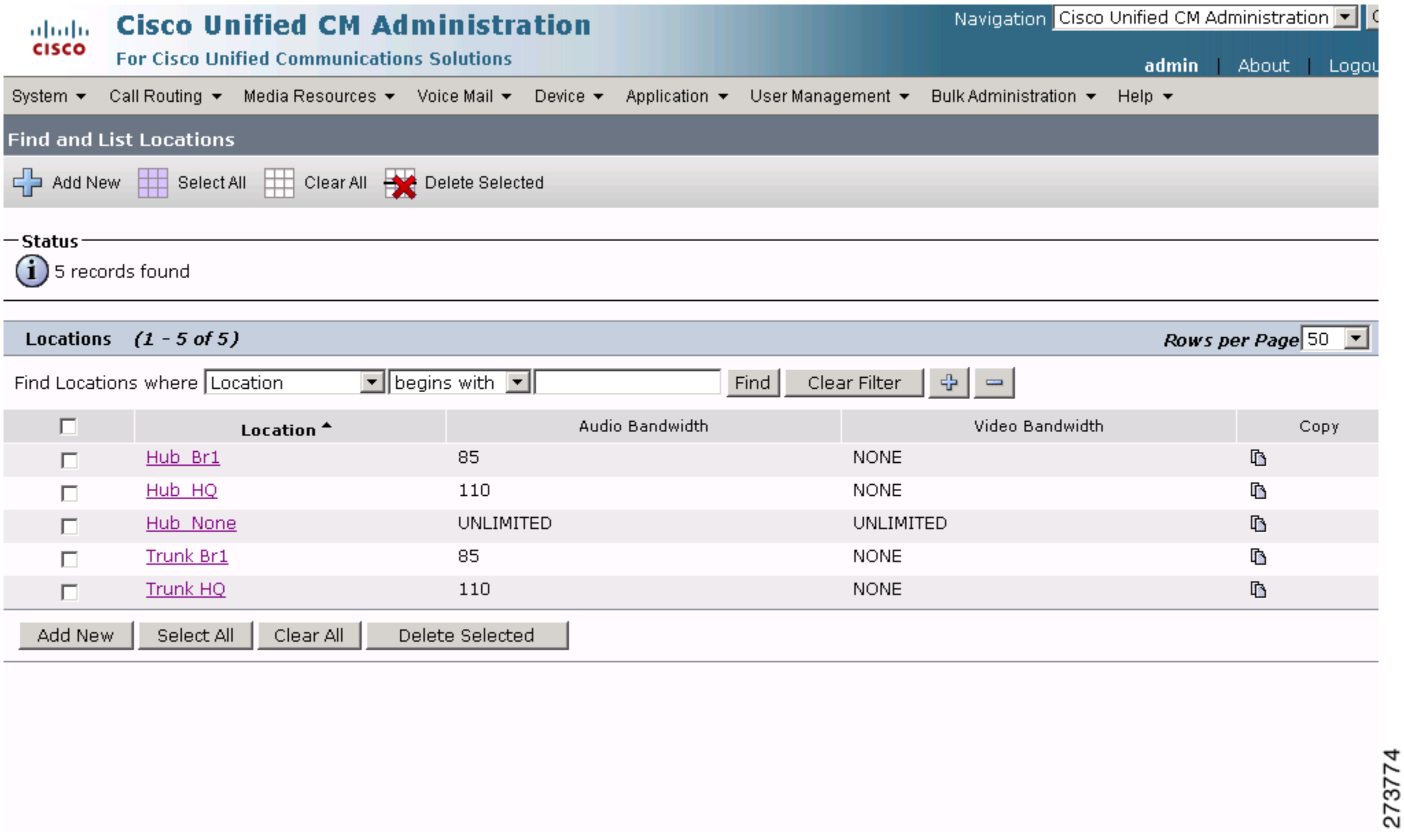


Figure 33 System Location Hub Branch 1 Cisco Unified CM Administration Window

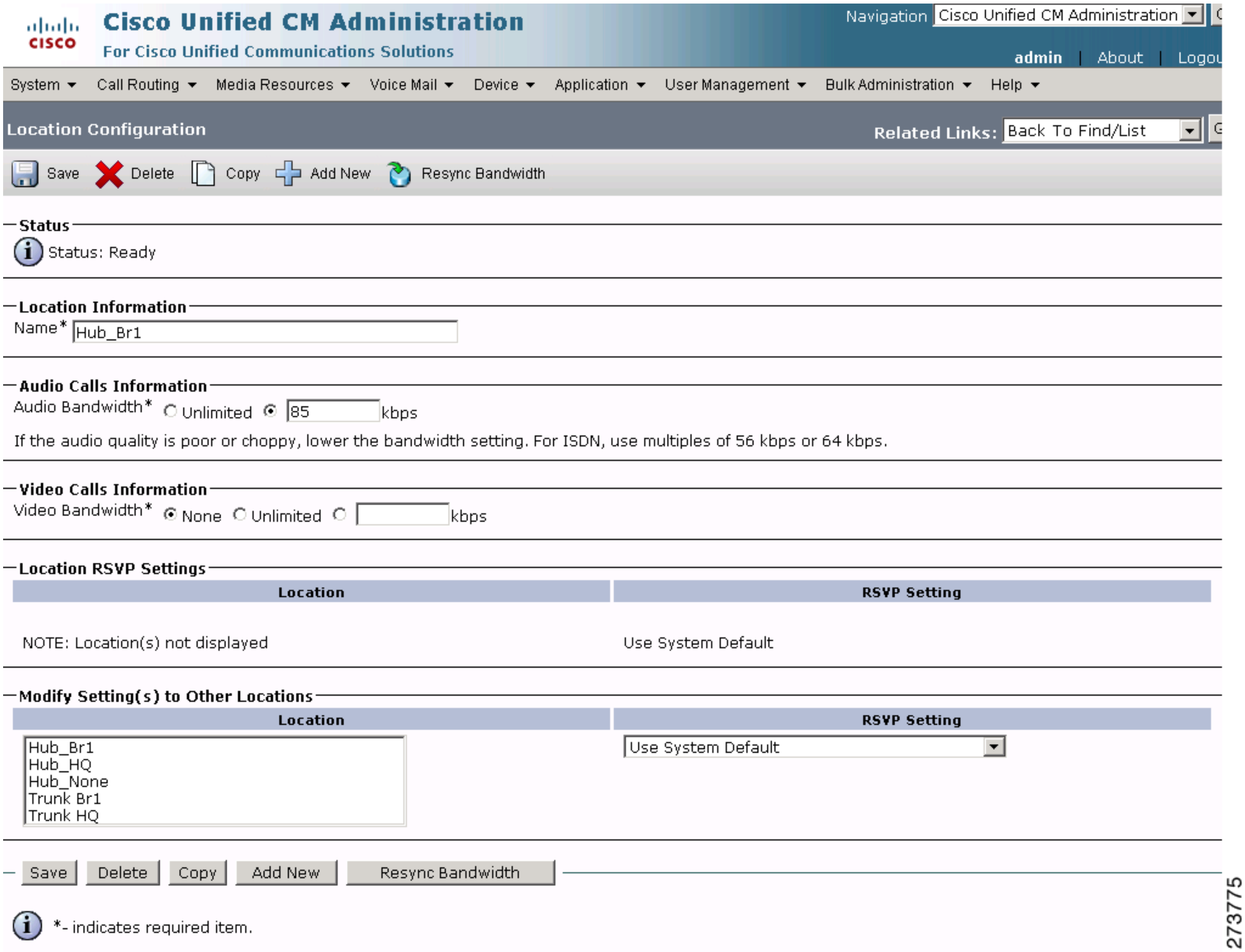


Figure 34 System Location Hub HQ Cisco Unified CM Administration Window

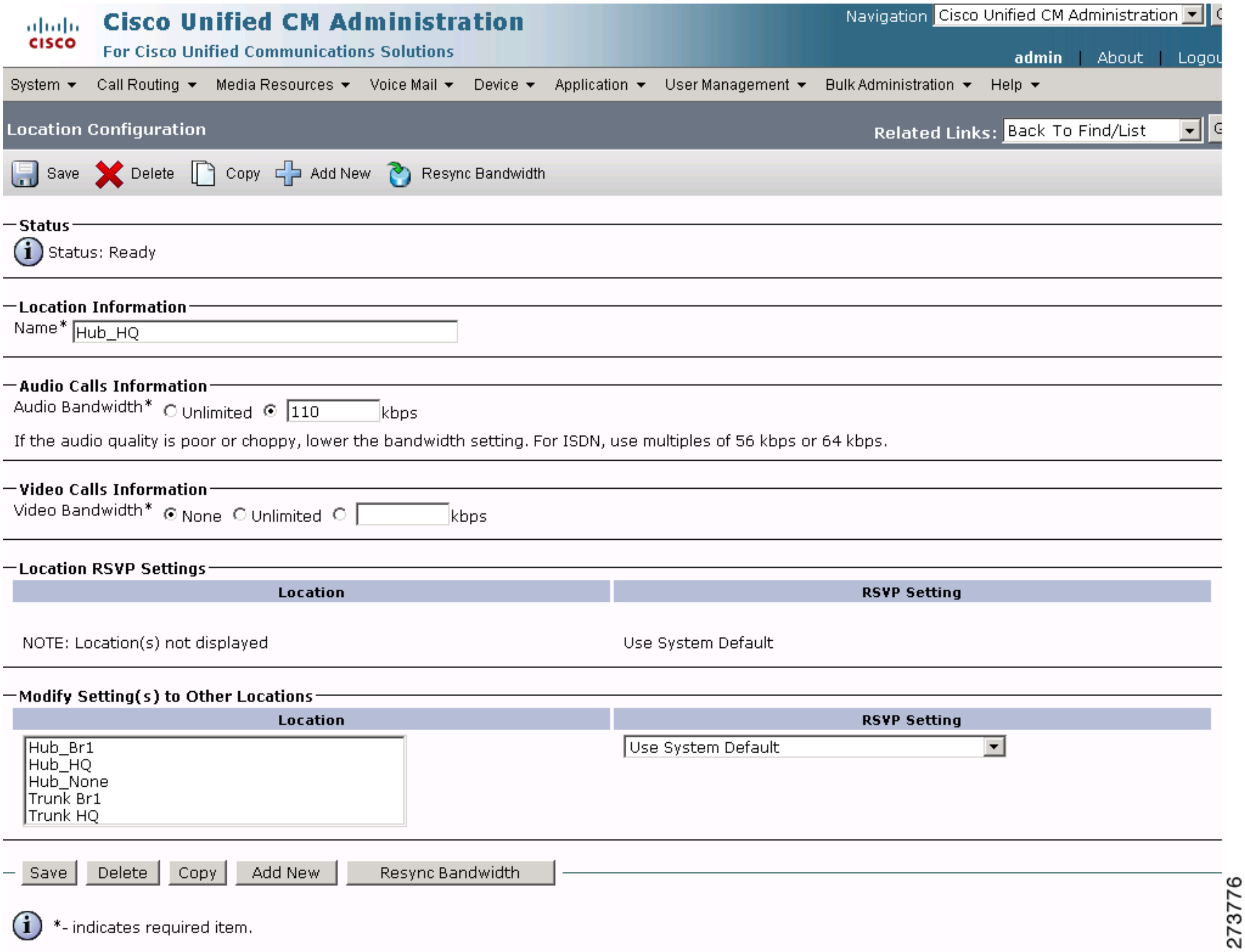


Figure 35 System Location Hub None Cisco Unified CM Administration Window

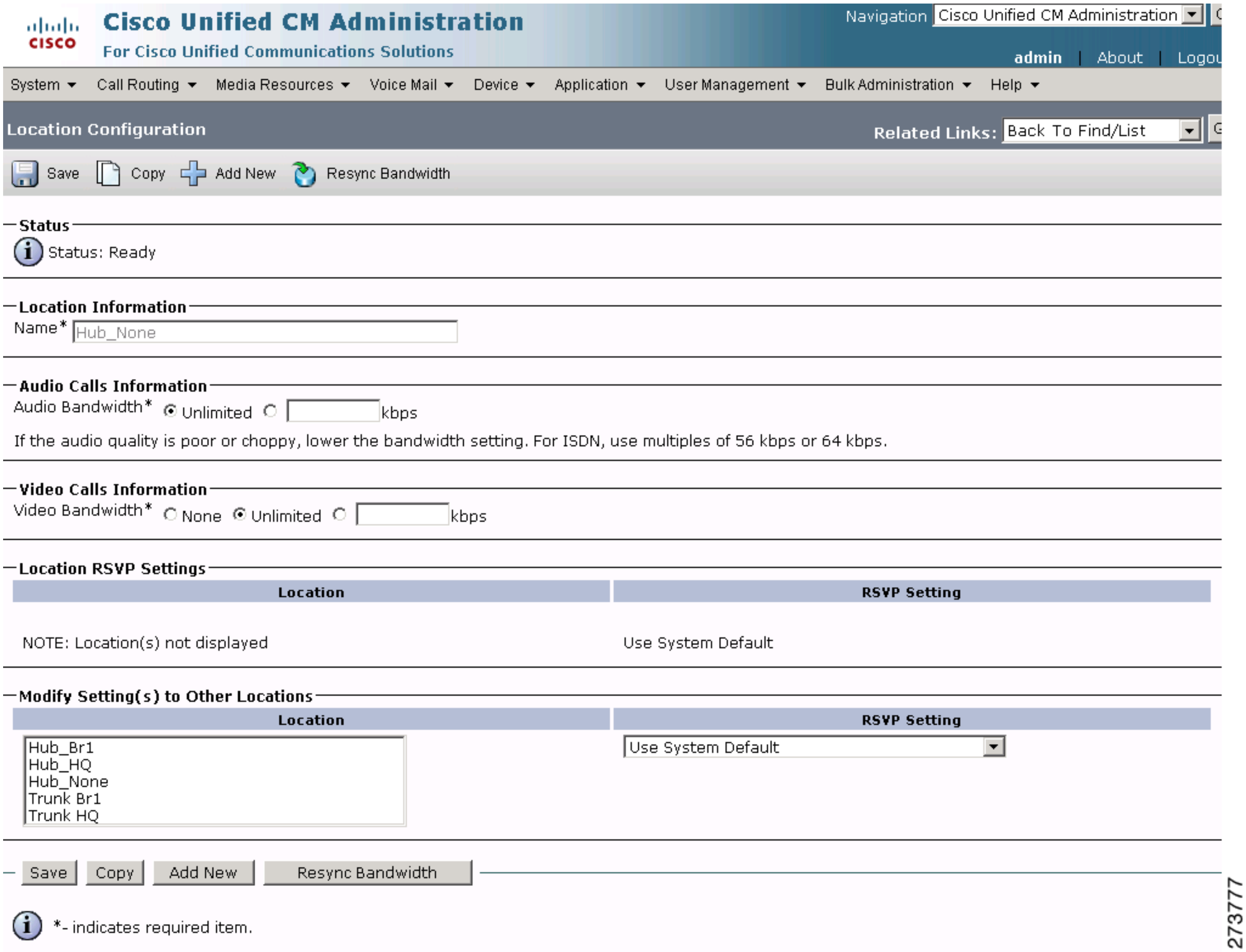
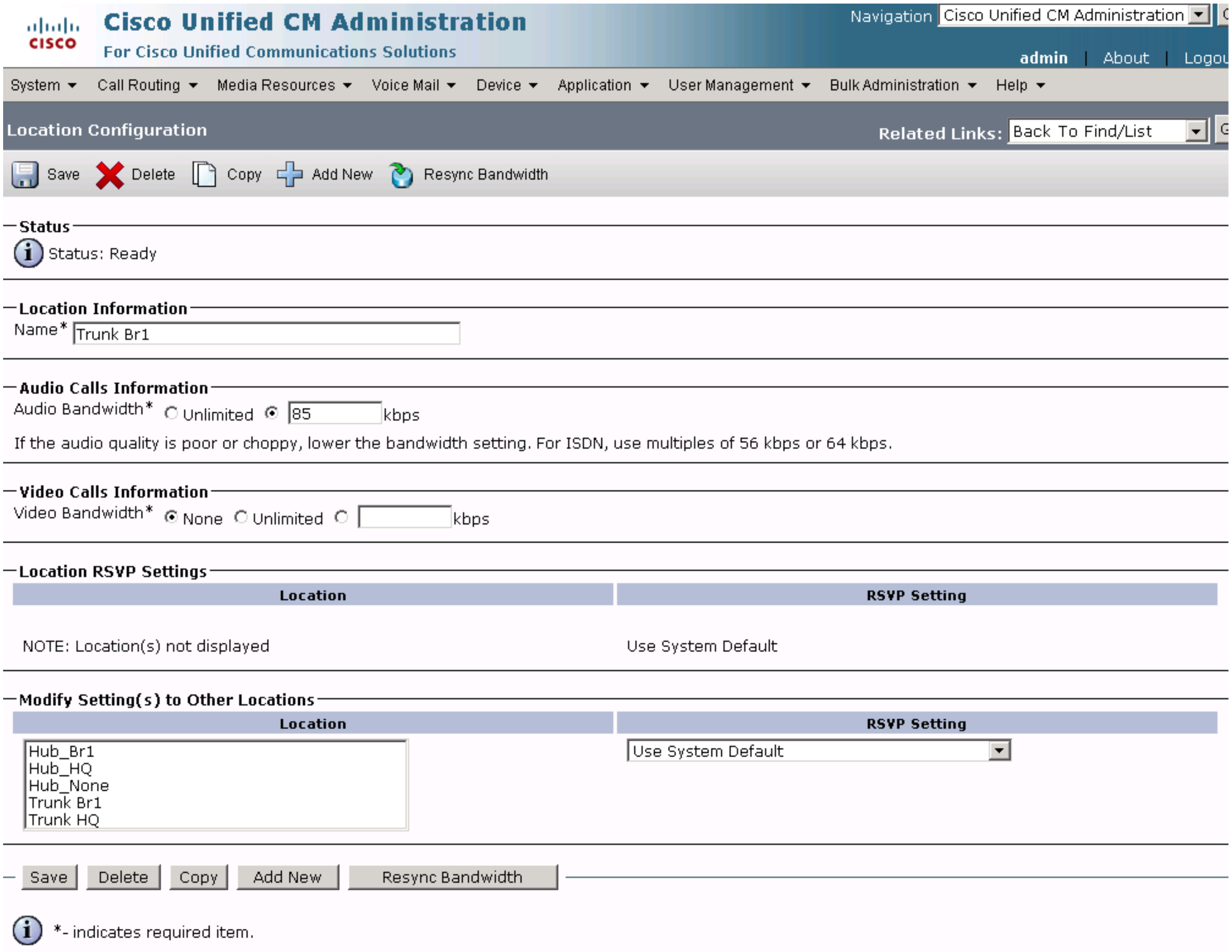
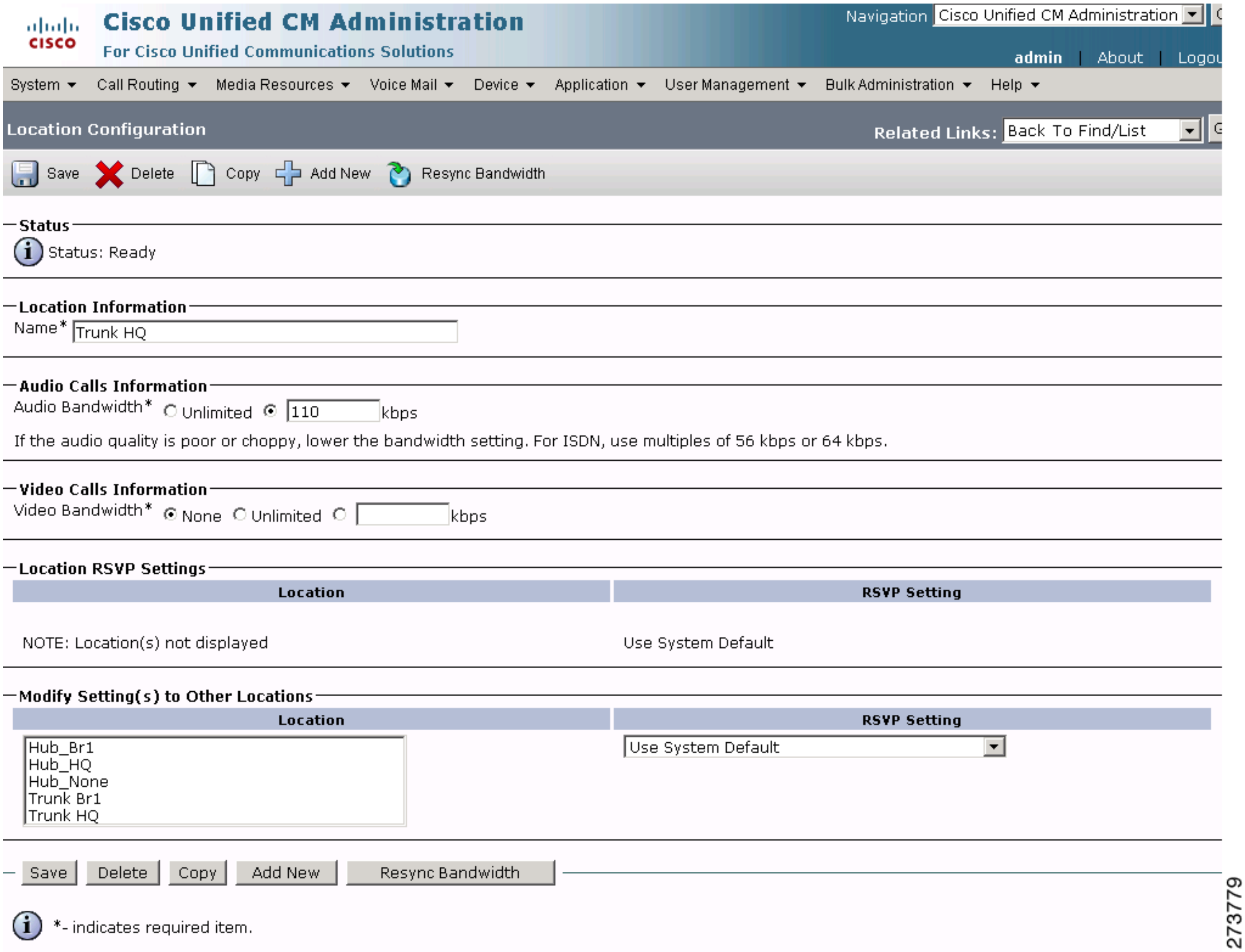


Figure 36 System Location-Location Trunk Branch 1 Cisco Unified CM Administration Window



273778

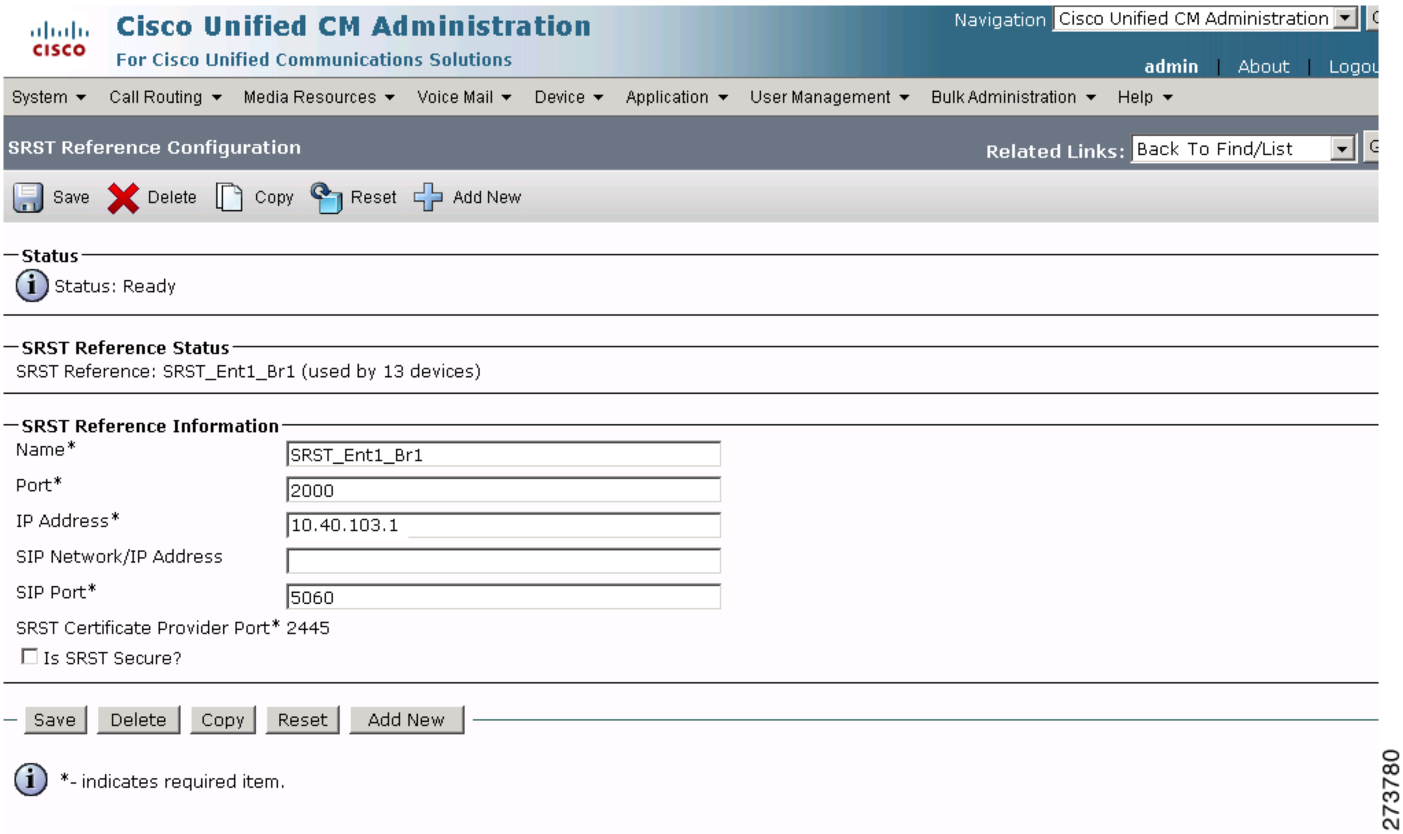
Figure 37 System Location-Location Trunk HQ Cisco Unified CM Administration Window



System: SRST Parameters

To configure the system SRST parameters for the Cisco Unified CM, click **System > SRST** menu in the Cisco Unified CM Administration window.

Figure 38 System SRST-SRST Enterprise 1 Branch 1 Cisco Unified CM Administration Window



Configuring the Cisco Unified CM Call Routing Parameters

Use the Cisco Unified Communications Manager Administration window to configure call routing parameters. Call routing parameter example configurations are shown in the following sections:

- Call Routing: Route/Hunt Parameters, page 63
- Call Routing: Class of Control Parameters, page 68

Call Routing: Route/Hunt Parameters

To configure call routing route/hunt parameters for the Cisco Unified CM, click **Call Routing** > **Route/Hunt** menu in the Cisco Unified CM Administration window.

Figure 39 Call Routing RouteHunt Route Pattern Cisco Unified CM Administration Window

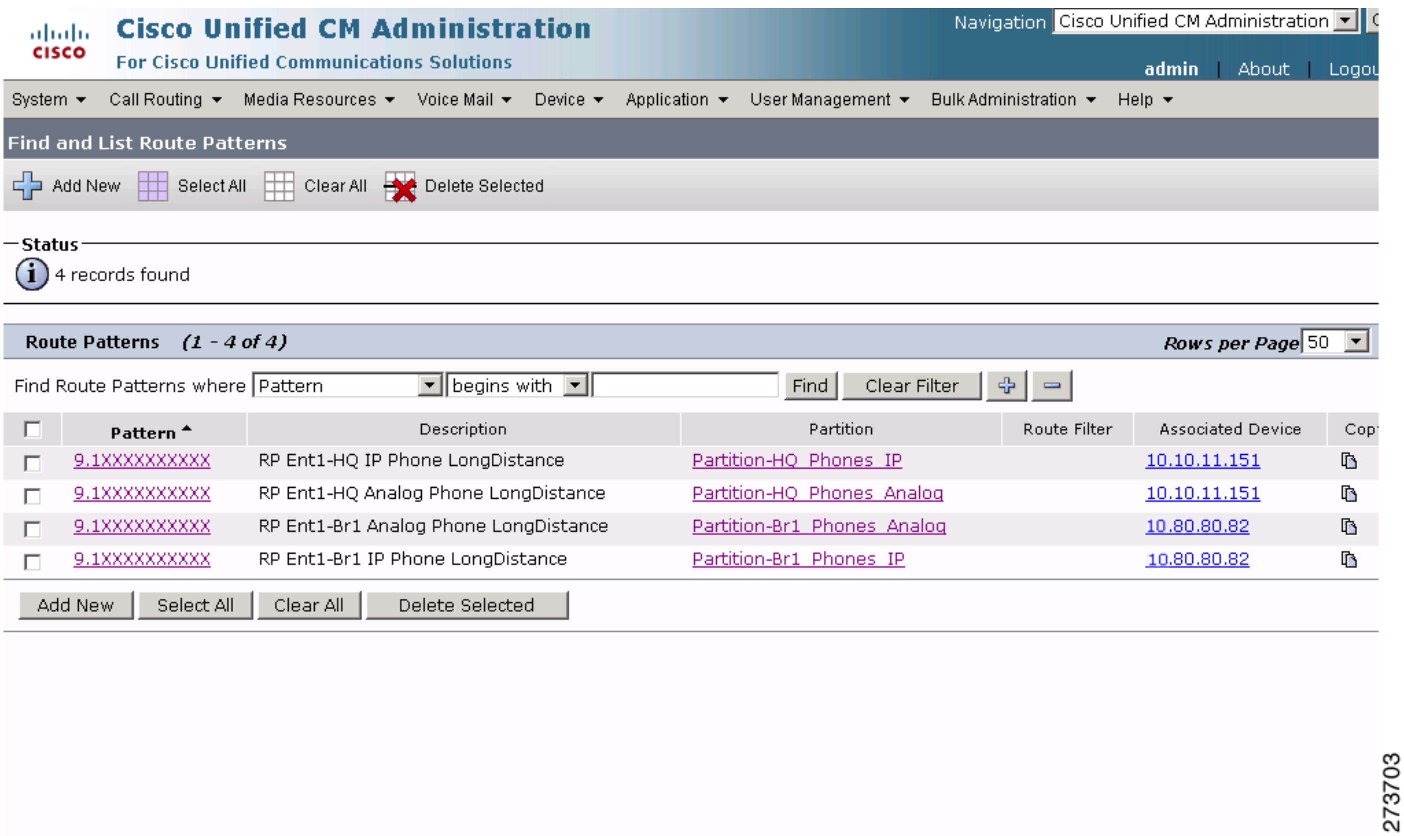
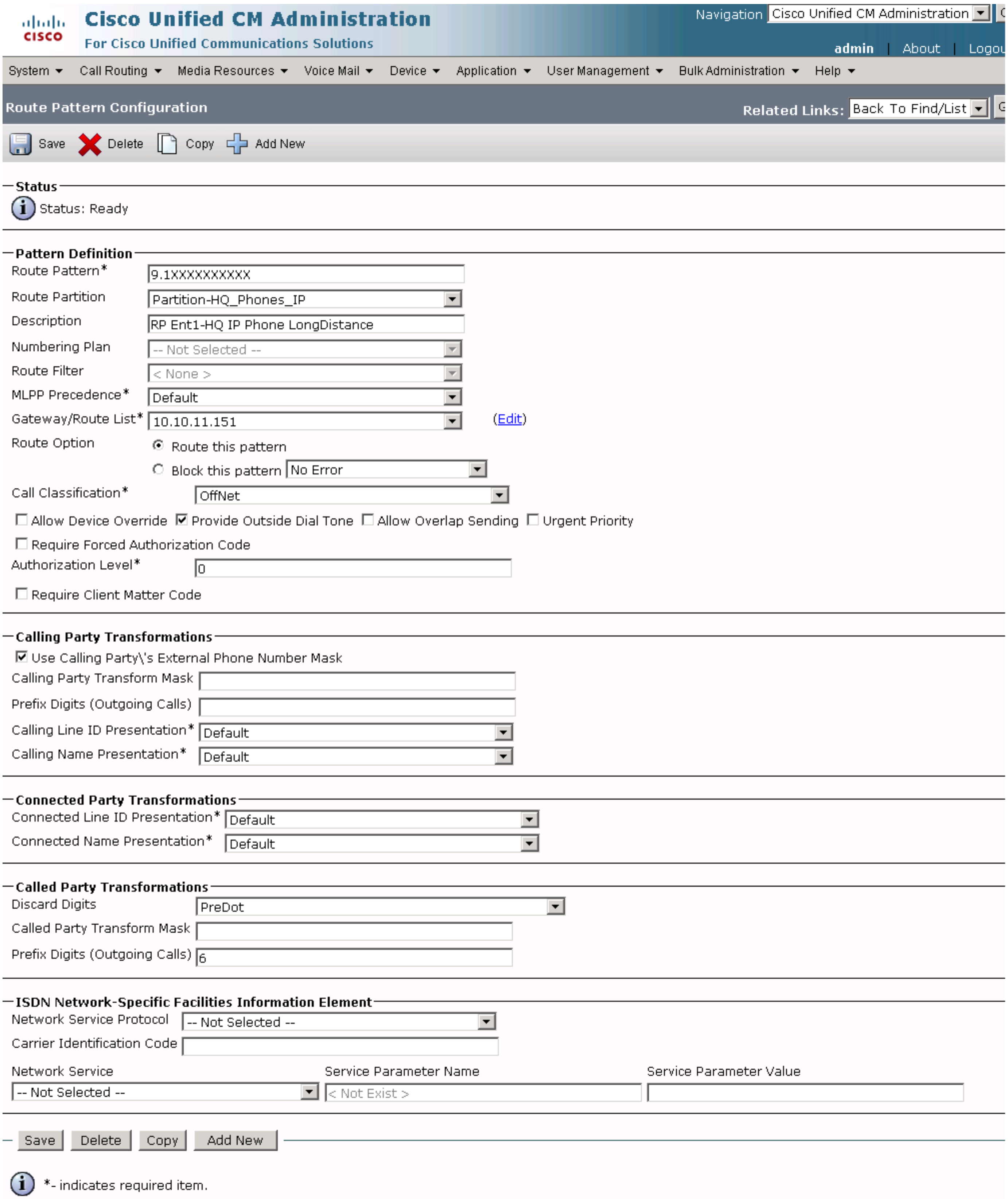
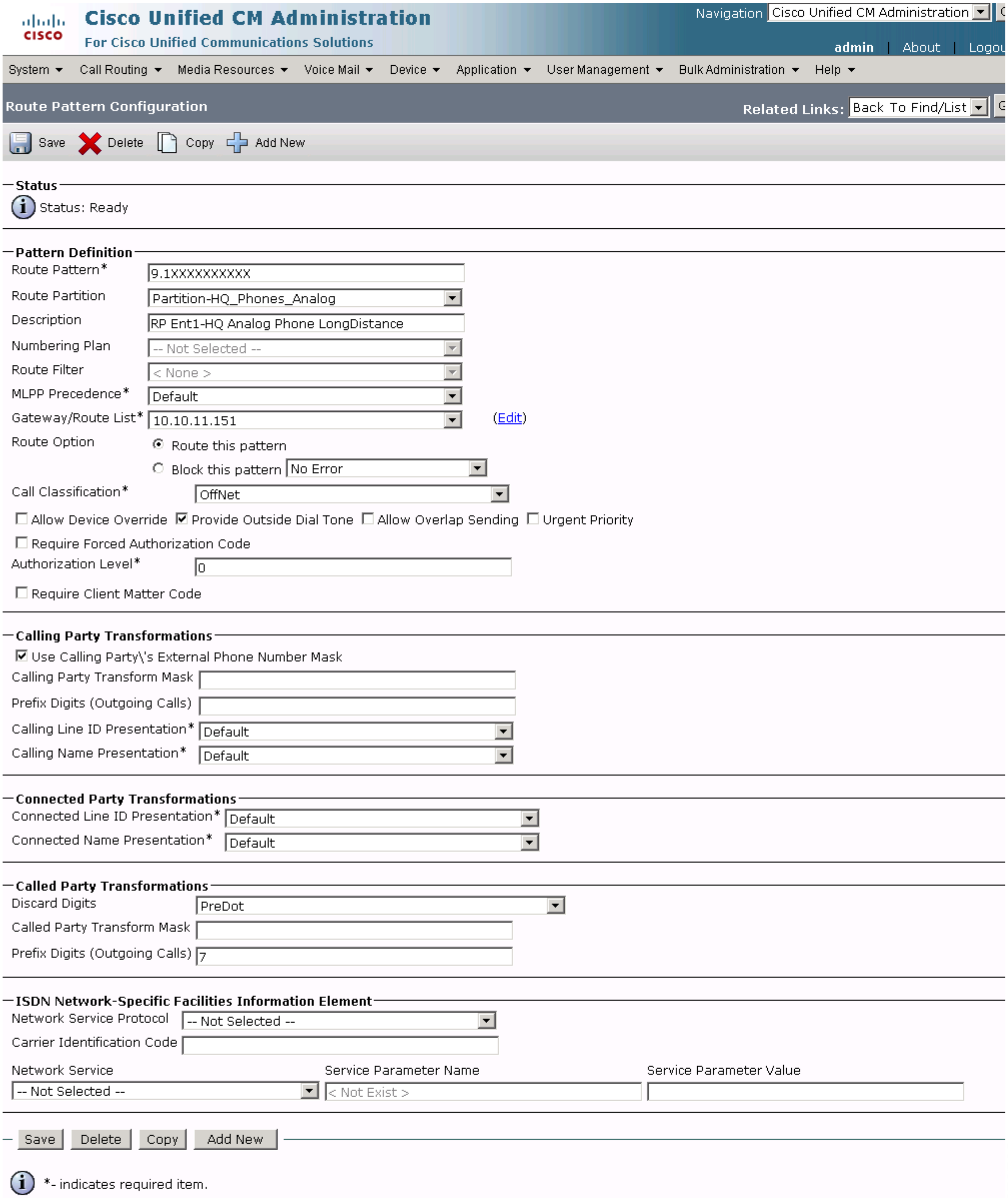


Figure 40 Call Routing RouteHunt Route Pattern RP Ent 1 HQ IP Phone LongDistance Cisco Unified CM Admin Window



273704

Figure 41 Call Routing RouteHunt Route Pattern RP Ent1 HQ Analog Phone LongDistance Administration Window



273705

Figure 42 Call Routing RouteHunt Route Pattern RP Ent1 Br1 Analog Phone LongDistance Administration Window

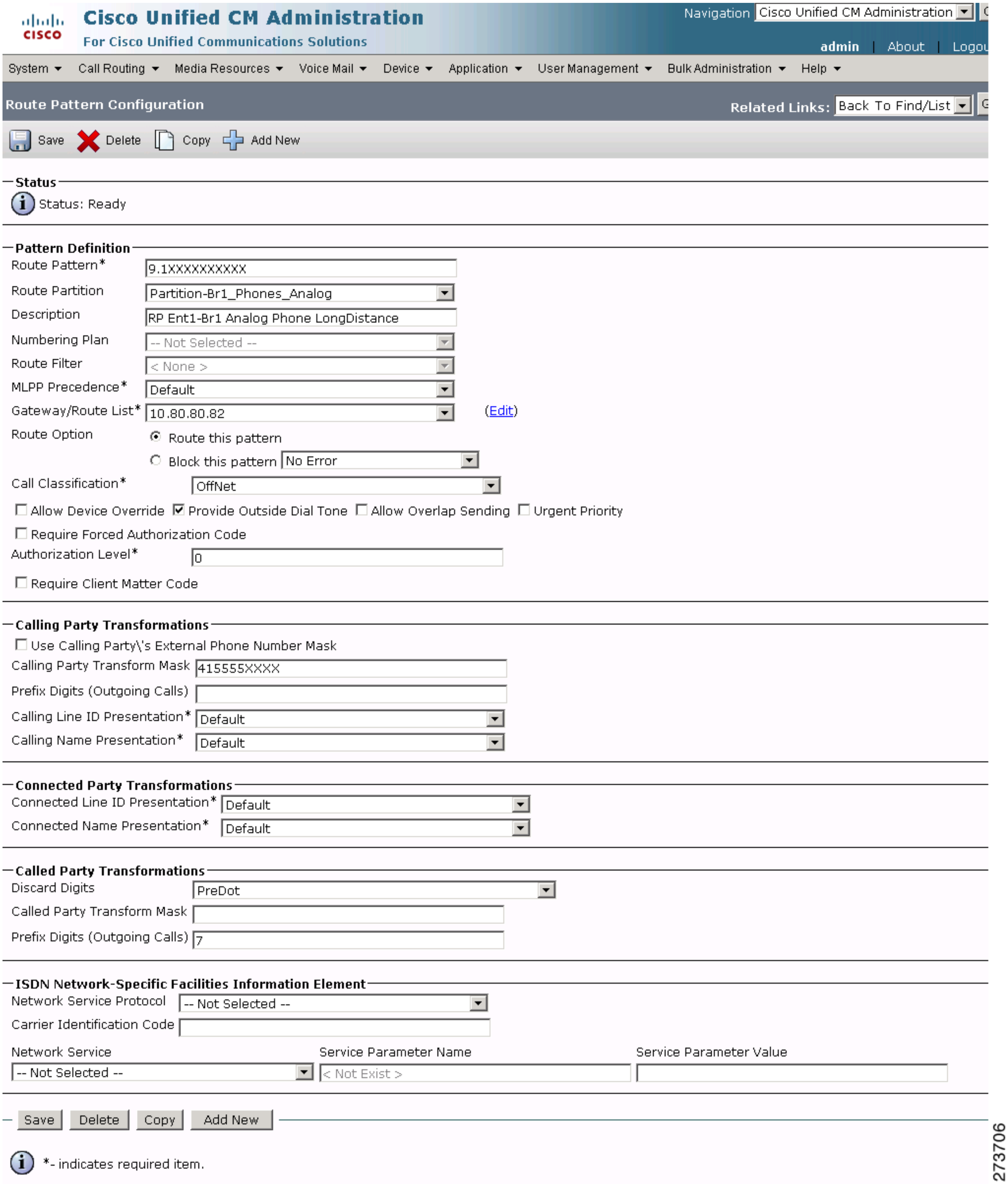
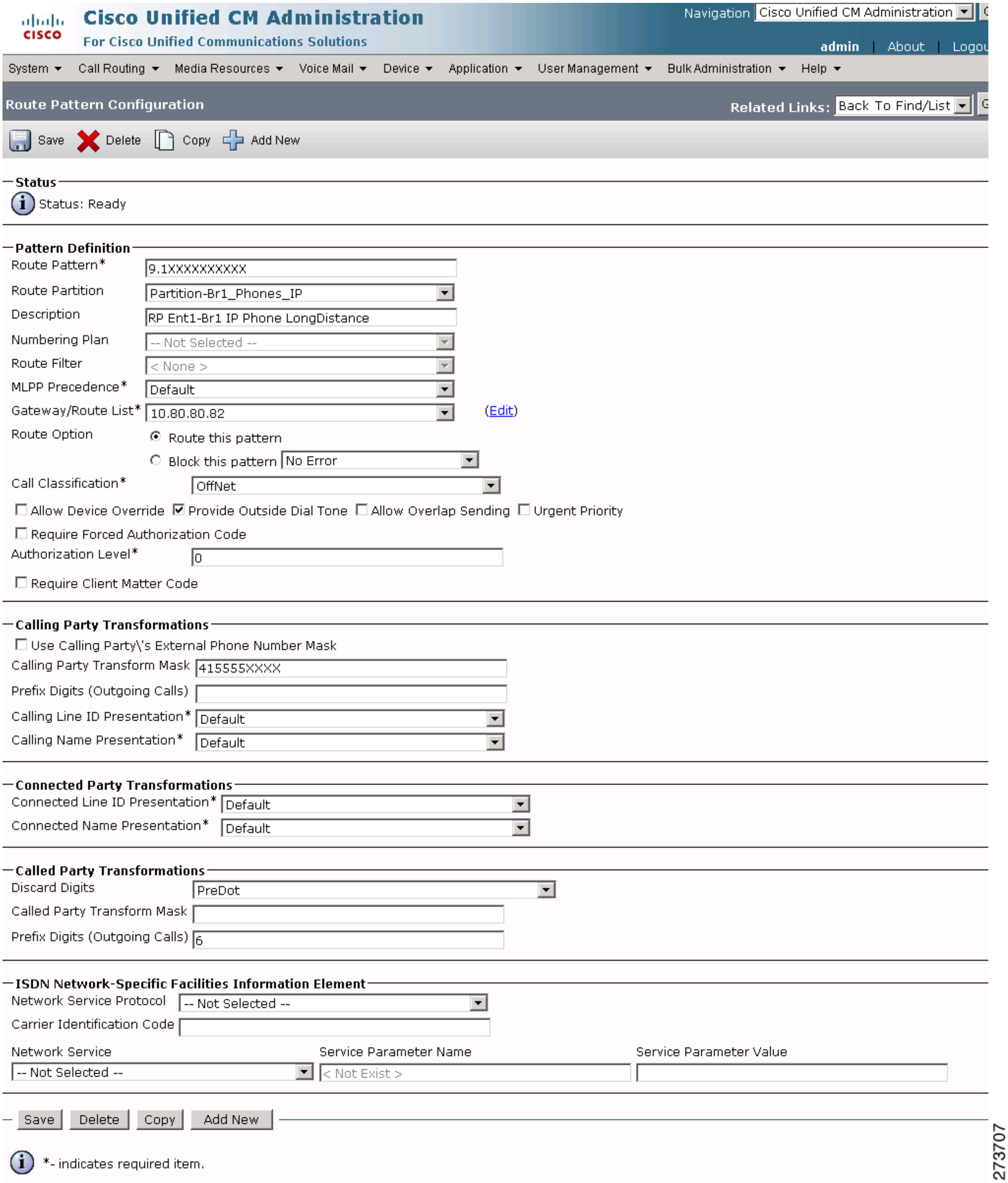


Figure 43 Call Routing RouteHunt Route Pattern RP Ent1 Br1 IP Phone LongDistance Administration Window



Call Routing: Class of Control Parameters

To configure the call routing class of control parameters for the Cisco Unified CM, click on **Call Routing** > **Class of Control** menu in the Cisco Unified CM Administration window.

Figure 44 Call Routing Class of Control Partition Cisco Unified CM Administration Window

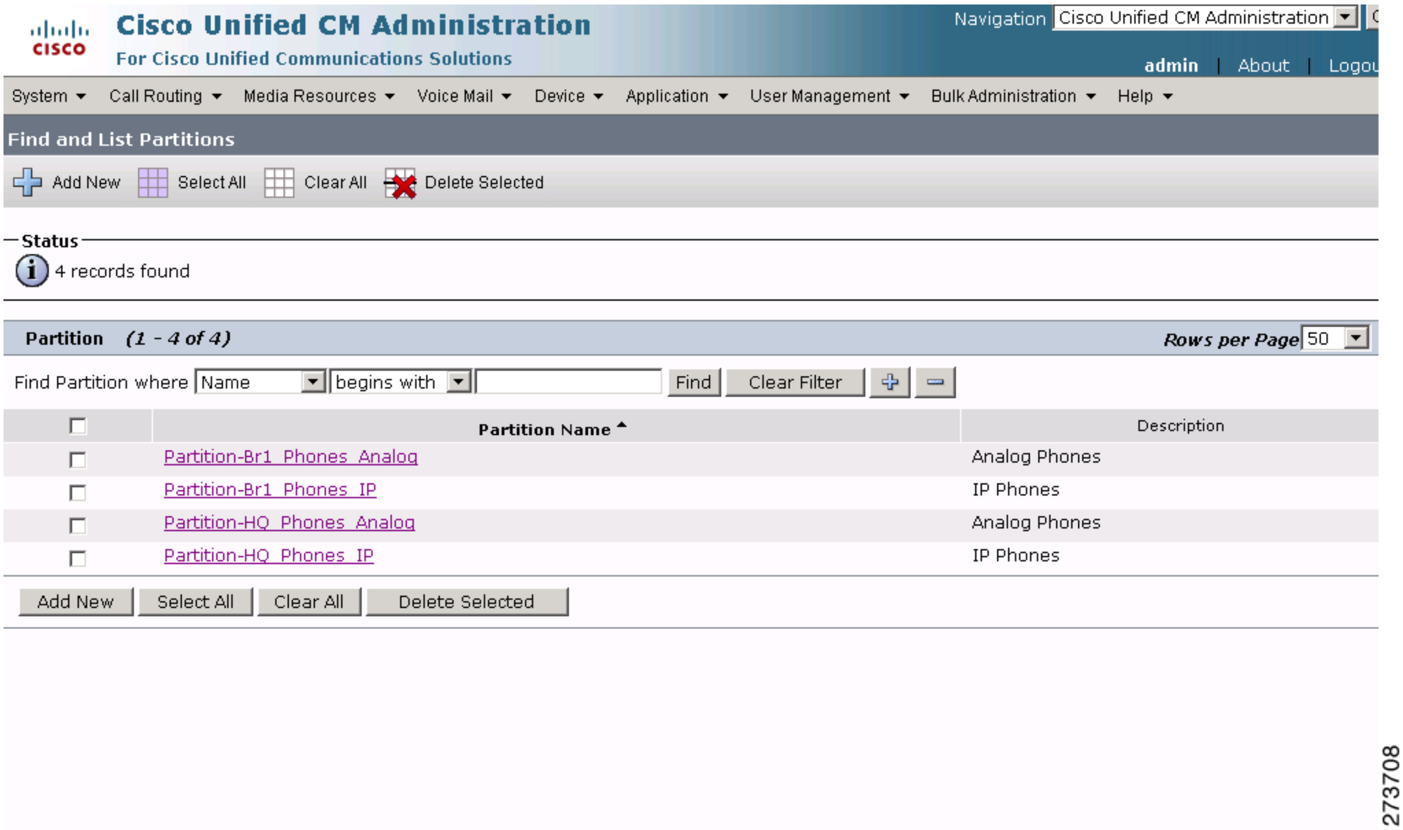


Figure 45 Call Routing Class of Control Partition-Partition Br1 Phones Analog Administration Window

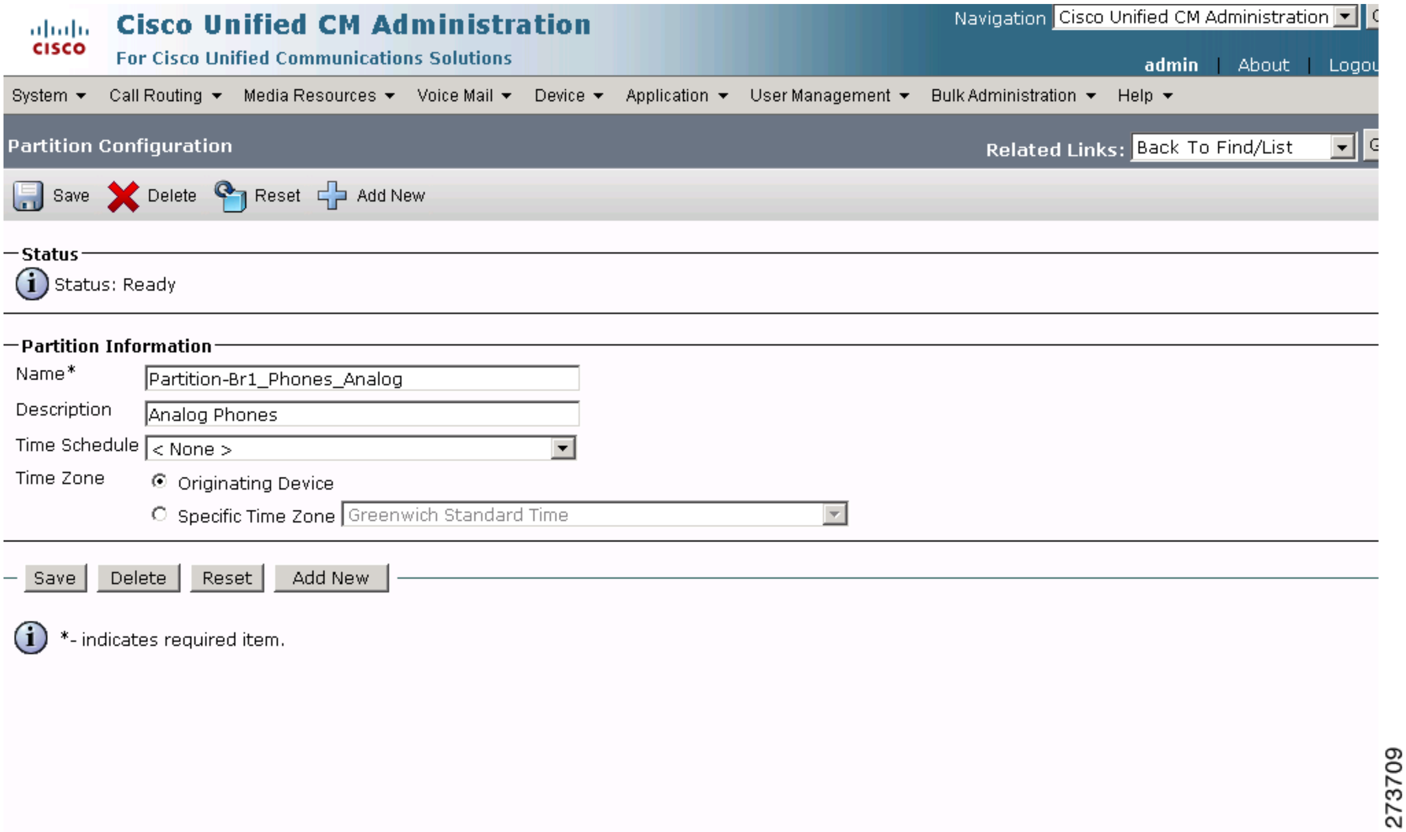


Figure 46 Call Routing Class of Control Partition-Partition Br1 Phones IP Cisco Unified CM Administration Window

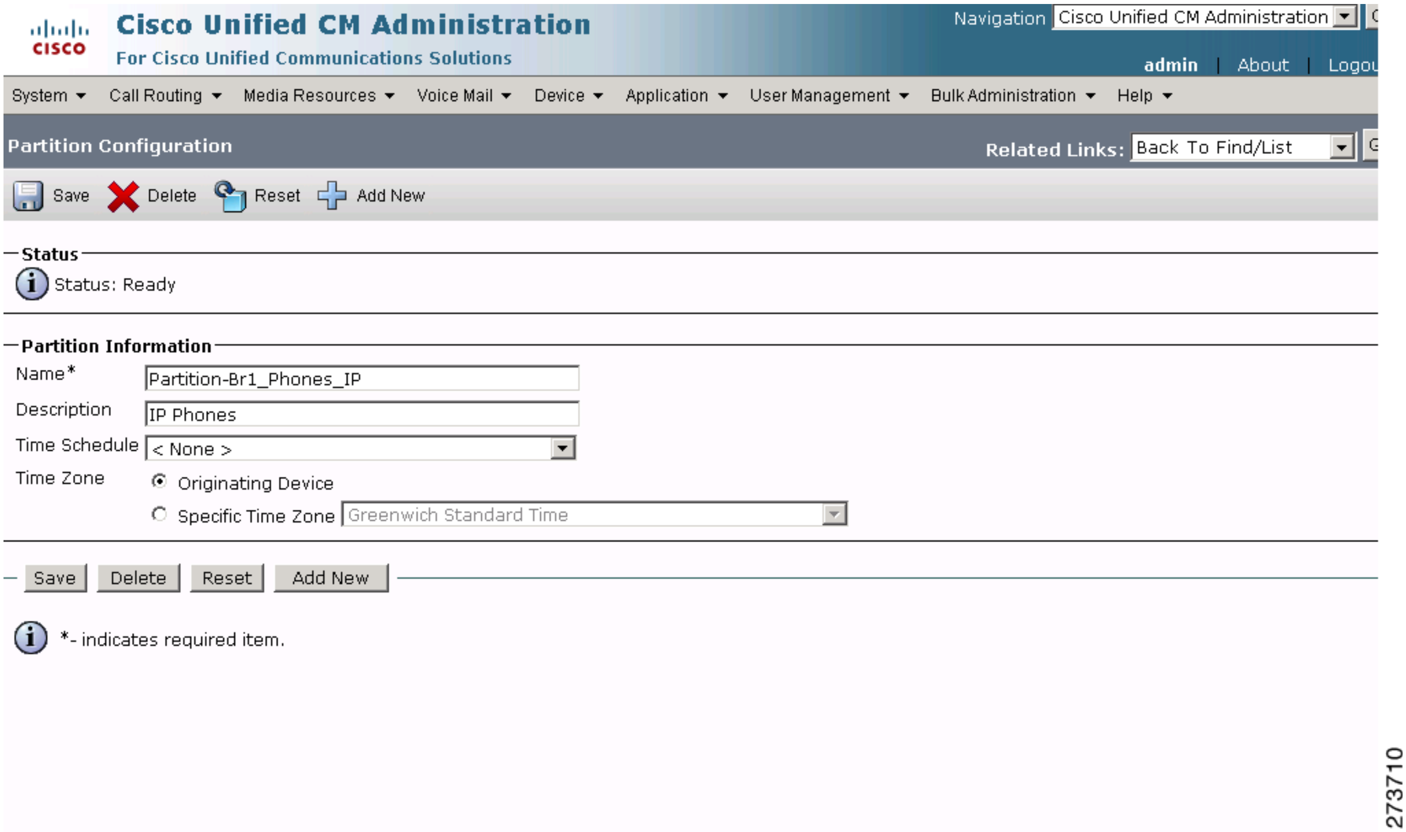


Figure 47 Call Routing Class of Control Partition-Partition HQ Phones Analog Administration Window

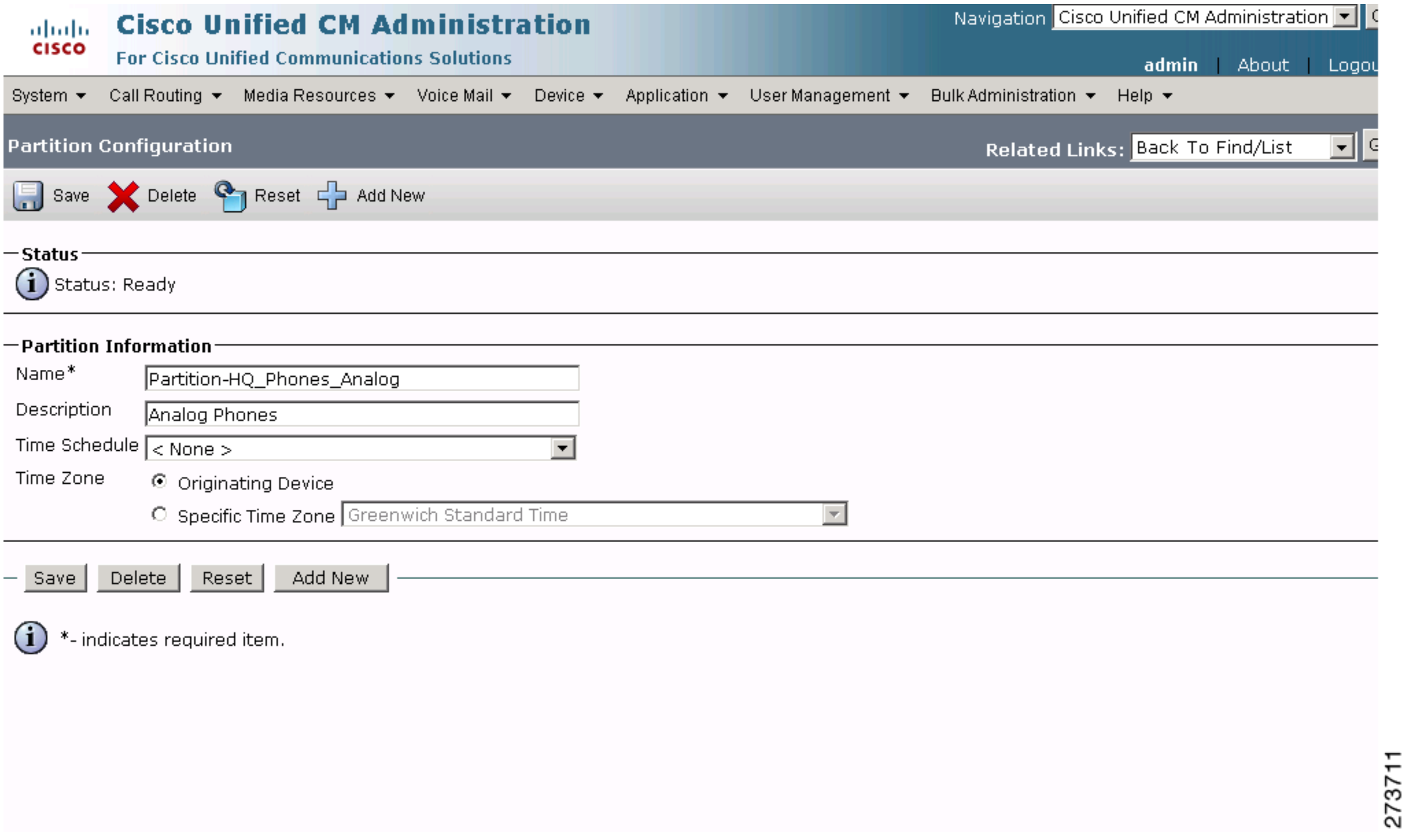


Figure 48 Call Routing Class of Control Partition-Partition HQ Phones IP Cisco Unified CM Administration Window

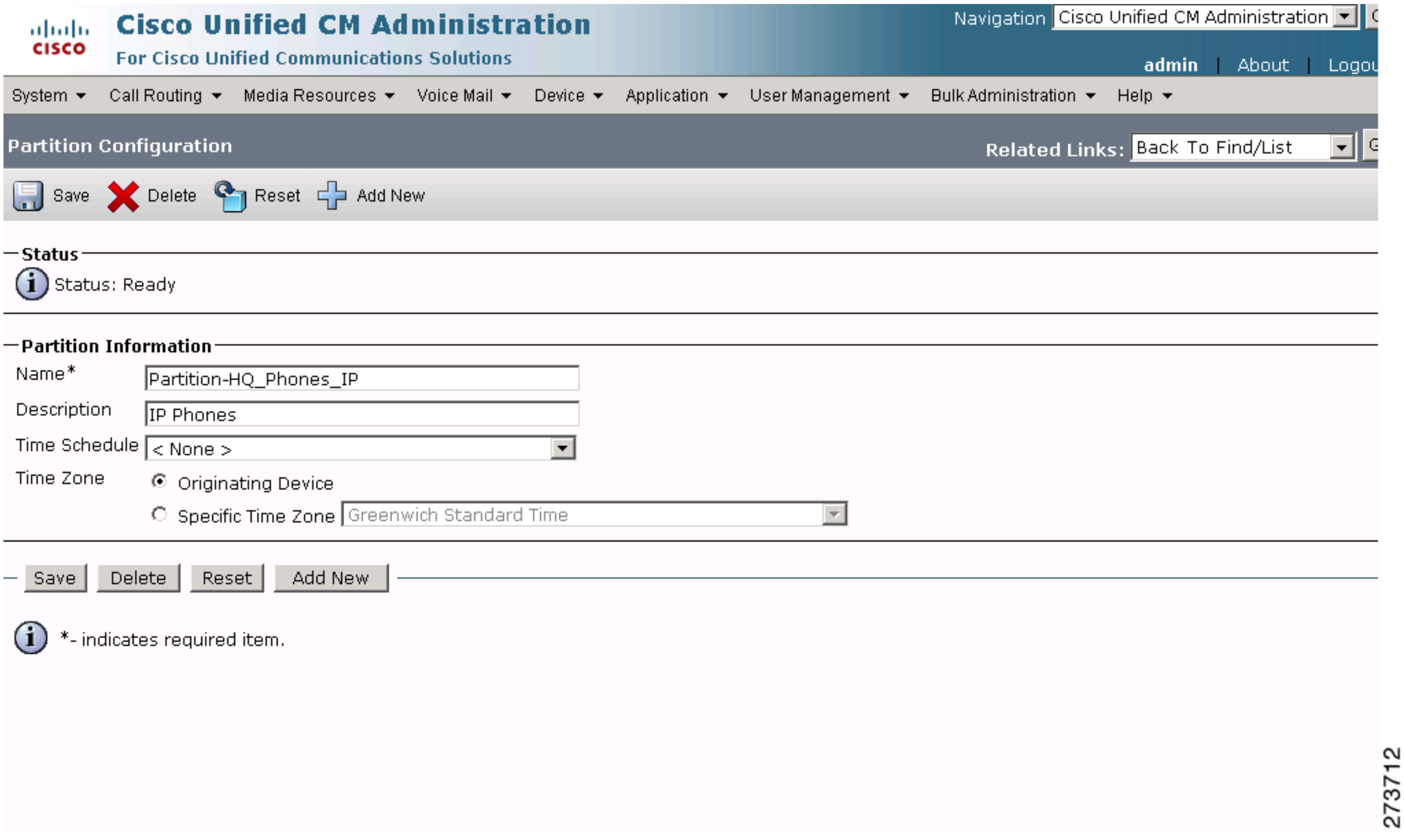


Figure 49 Call Routing Class of Control CSS Cisco Unified CM Administration Window

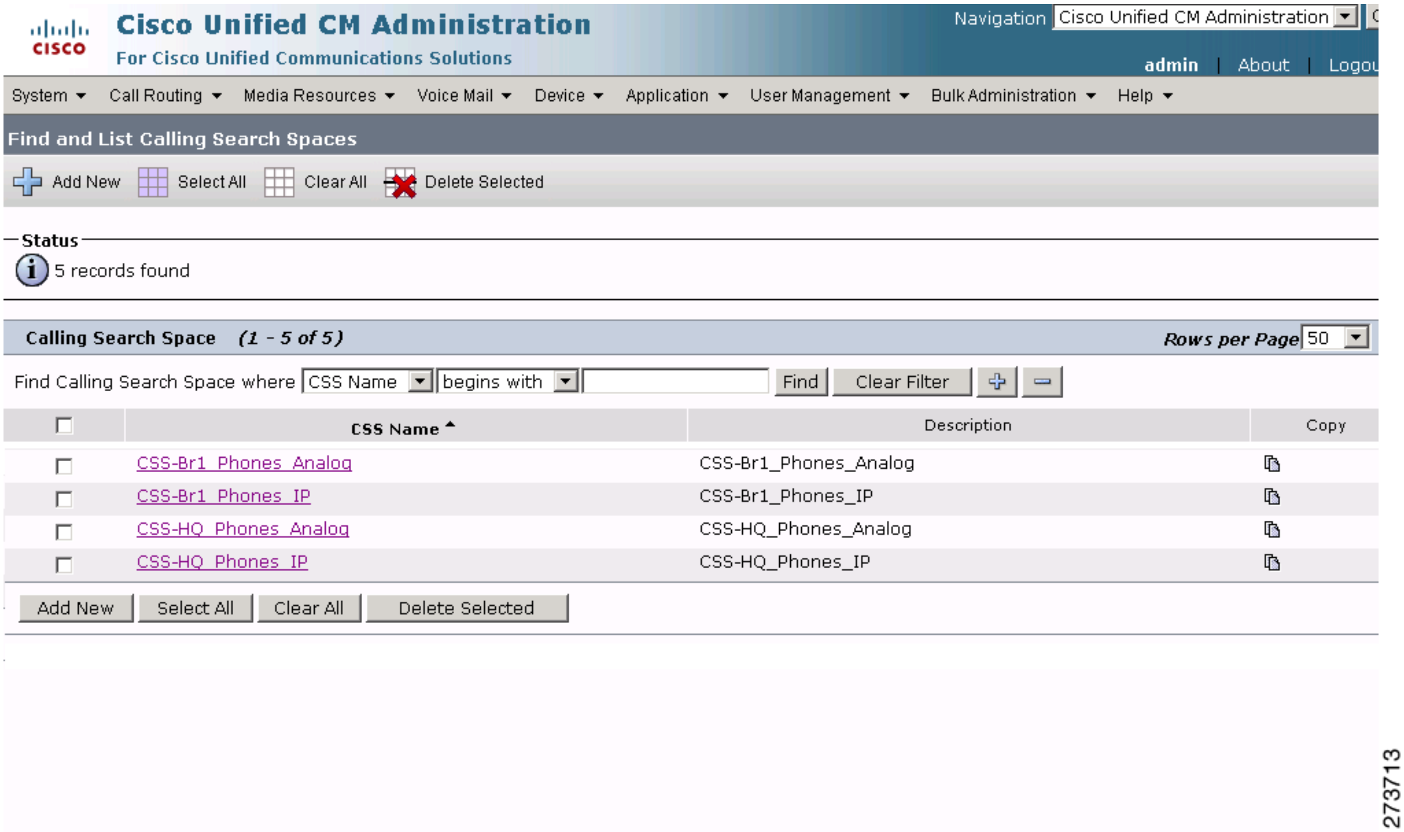


Figure 50 Call Routing Class of Control CSS-CSS Branch 1 Phones Analog Cisco Unified CM Administration Window

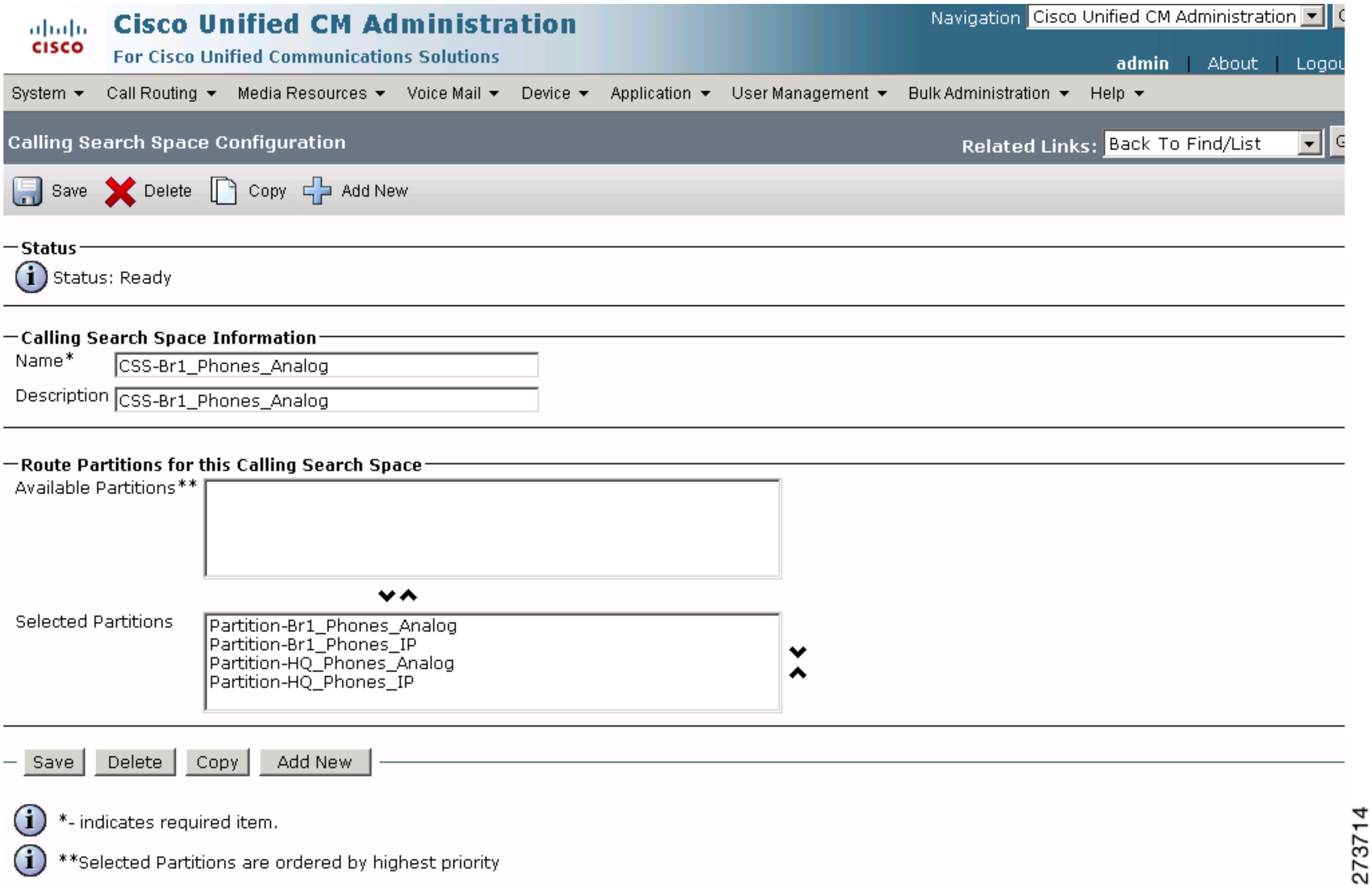


Figure 51 Call Routing Class of Control CSS-CSS Branch 1 Phones IP Cisco Unified CM Administration Window

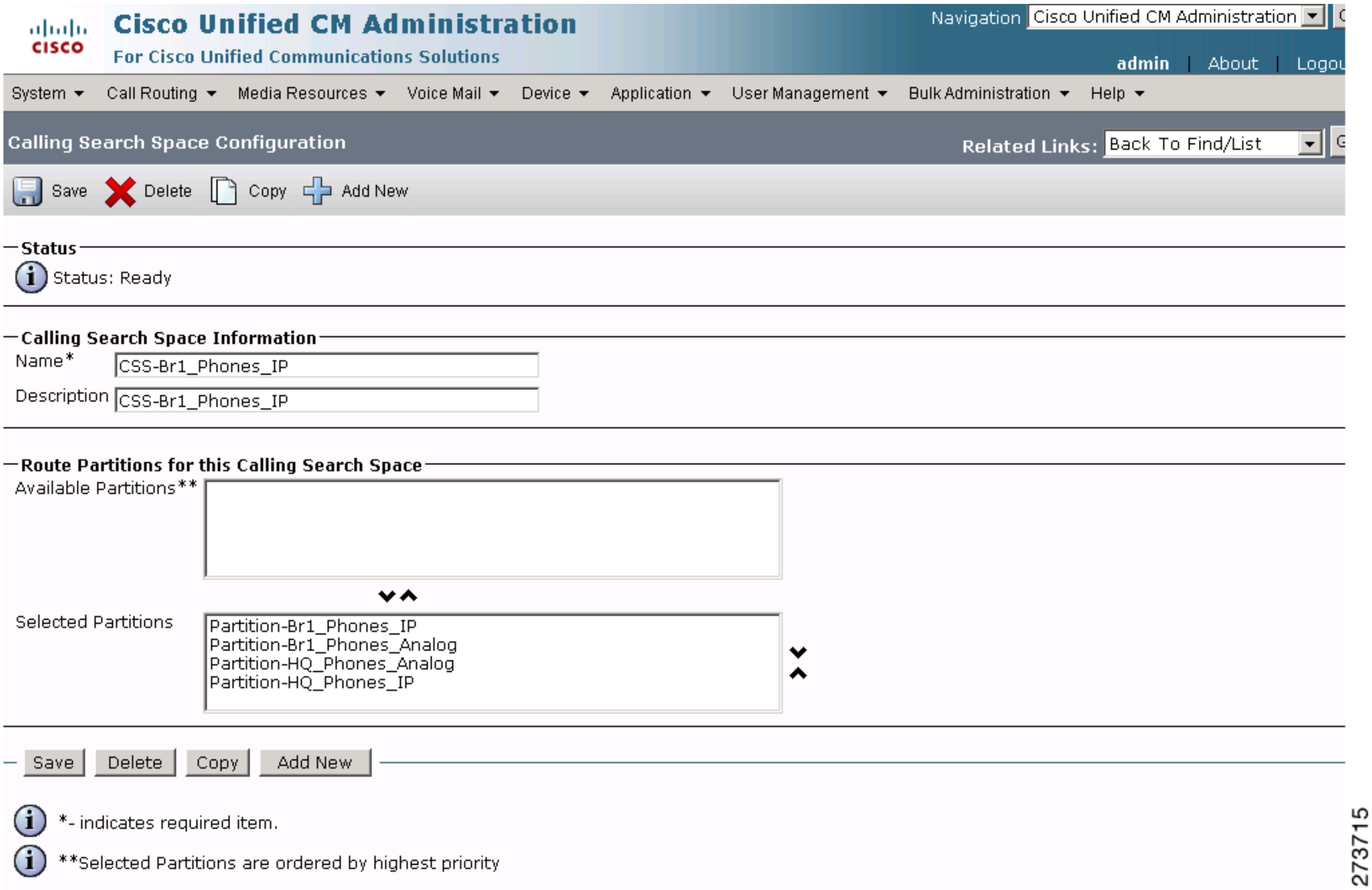
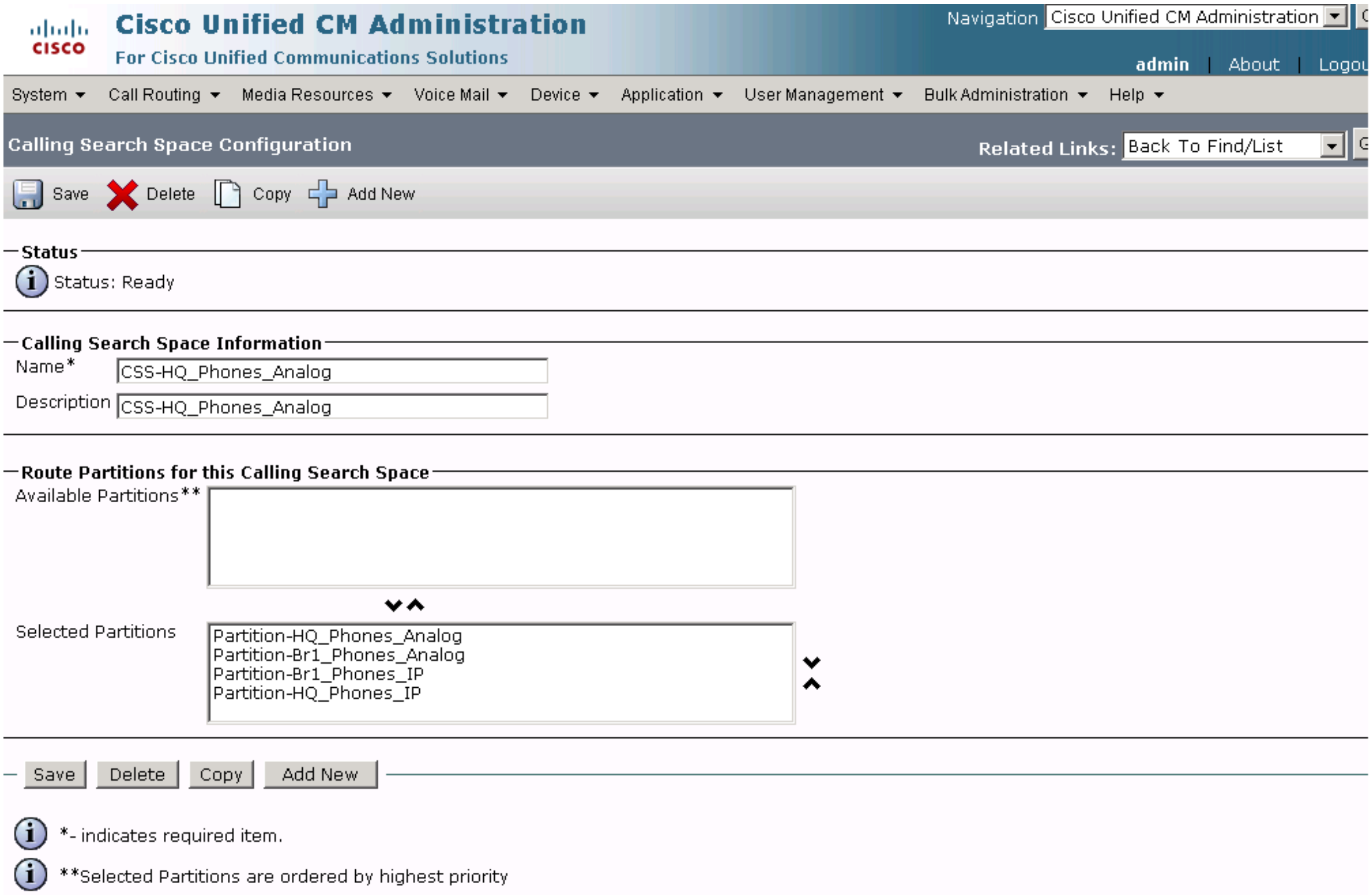
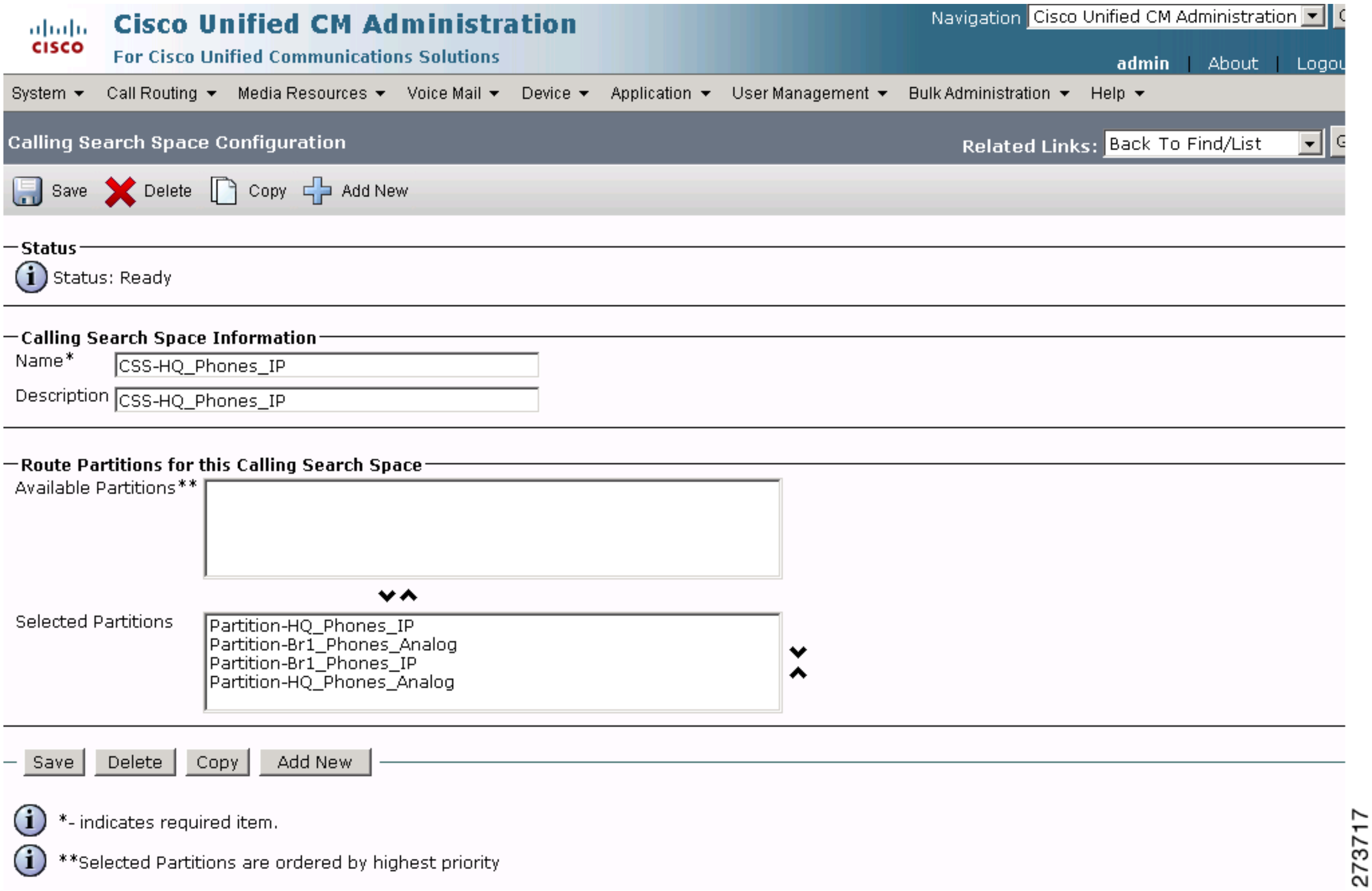


Figure 52 Call Routing Class of Control CSS-CSS HQ Phones Analog Cisco Unified CM Administration Window



273716

Figure 53 Call Routing Class of Control CSS-CSS HQ Phones IP Cisco Unified CM Administration Window



Configuring the Cisco Unified CM Media Resources Parameters

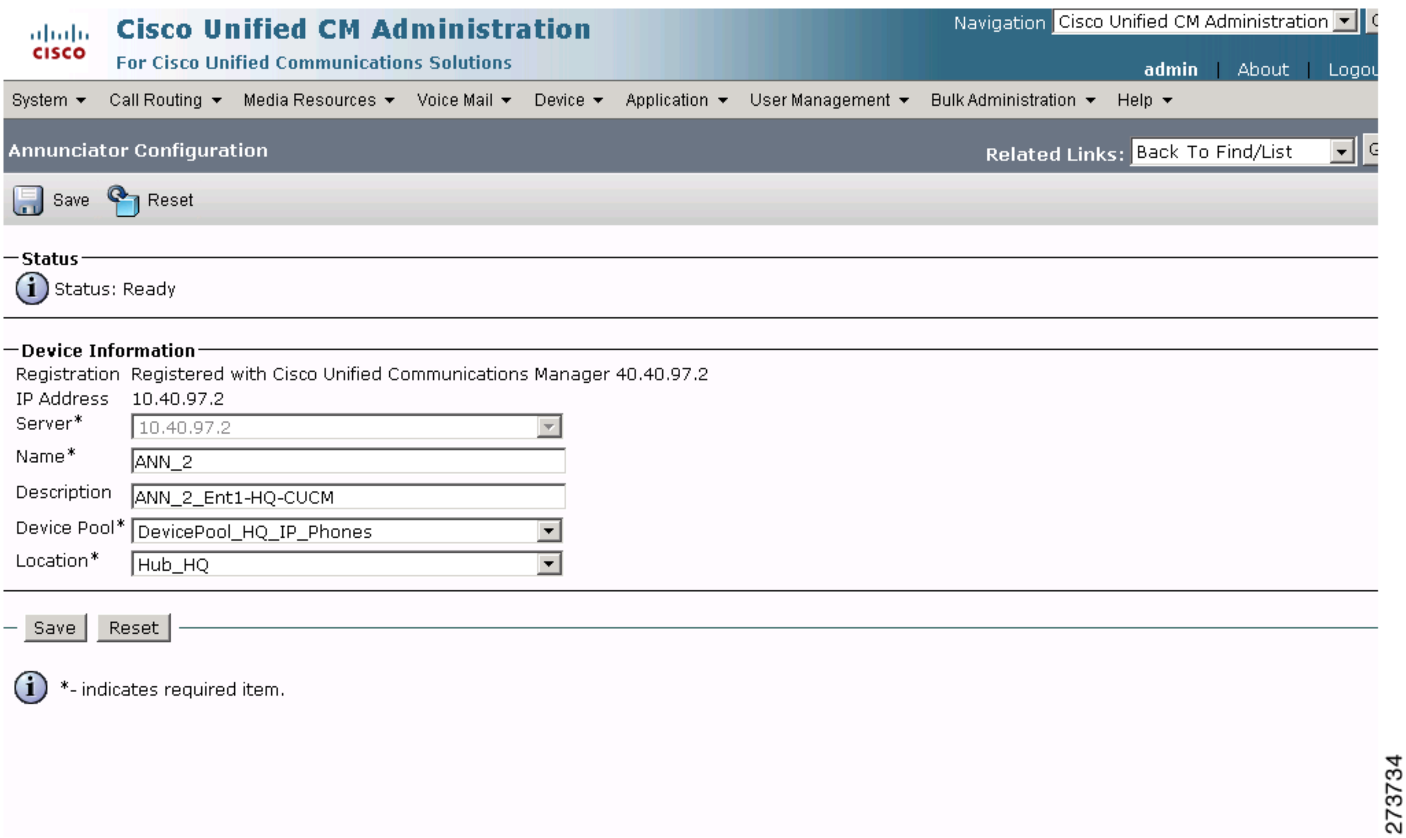
Use the Cisco Unified Communications Manager Administration window to configure the media resources parameters. The media resources parameter example configurations are shown in the following sections:

- Media Resources: Annunciator Parameters, page 78
- Media Resources: Conference Bridge Parameters, page 79
- Media Resources: Media Termination Point Parameters, page 82
- Media Resources: Music on Hold Server Parameters, page 85
- Media Resources: Transcoder Parameters, page 86
- Media Resources: Media Resource Group Parameters, page 89
- Media Resources: Media Resource Group List Parameters, page 92

Media Resources: Annunciator Parameters

To configure the media resources annunciator parameters for the Cisco Unified CM, click **Media Resources** > **Annunciator** menu in the Cisco Unified CM Administration window.

Figure 54 Media Resources Annunciator ANN 2 Cisco Unified CM Administration Window



Media Resources: Conference Bridge Parameters

To configure the media resources conference bridge parameters for the Cisco Unified CM, click **Media Resources** > **Conference Bridge** menu in the Cisco Unified CM Administration window.

Figure 55 Media Resources Conference Bridges Cisco Unified CM Administration Window

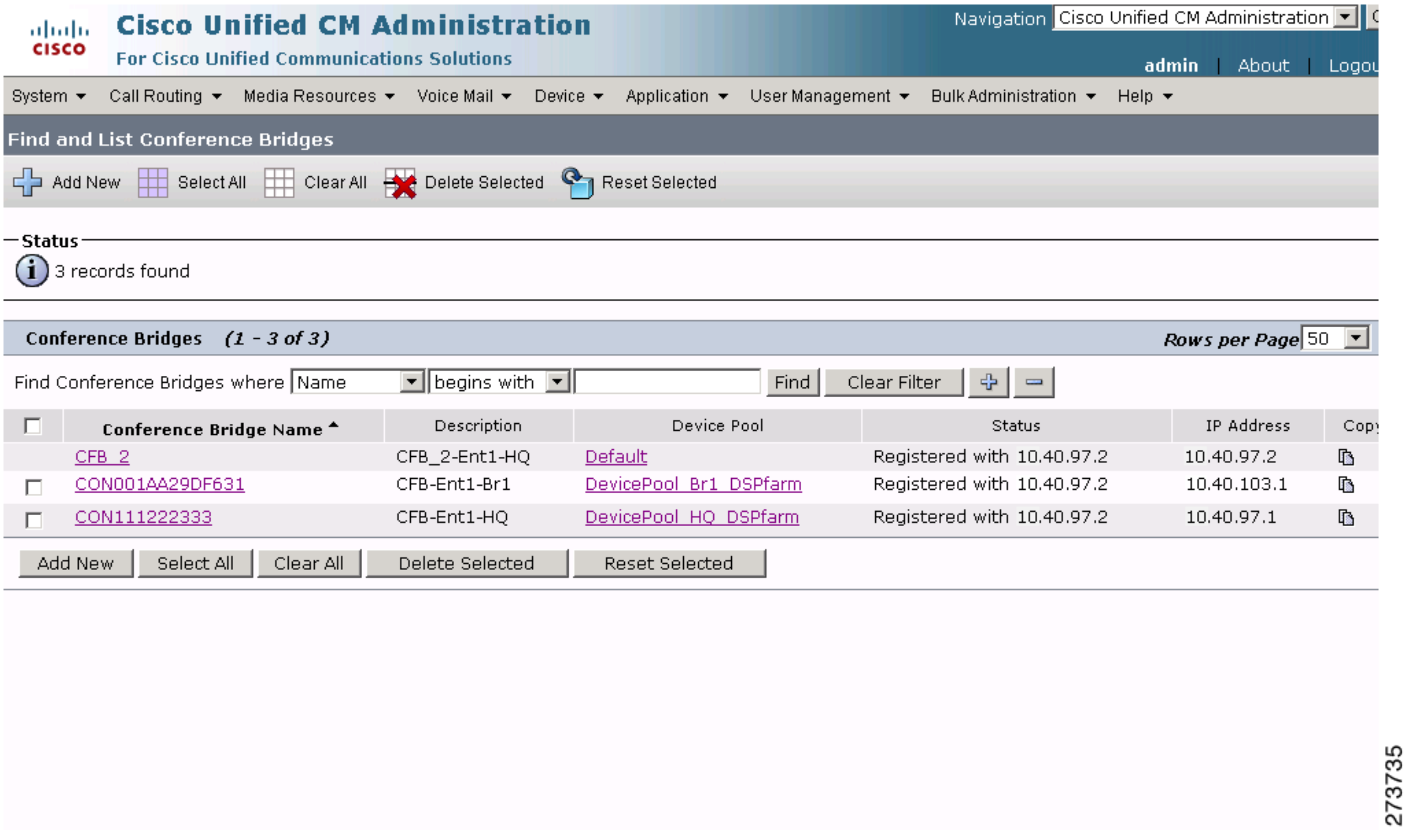


Figure 56 Media Resources Conference Bridges CFB Enterprise 1 Branch 1 Cisco Unified CM Administration Window

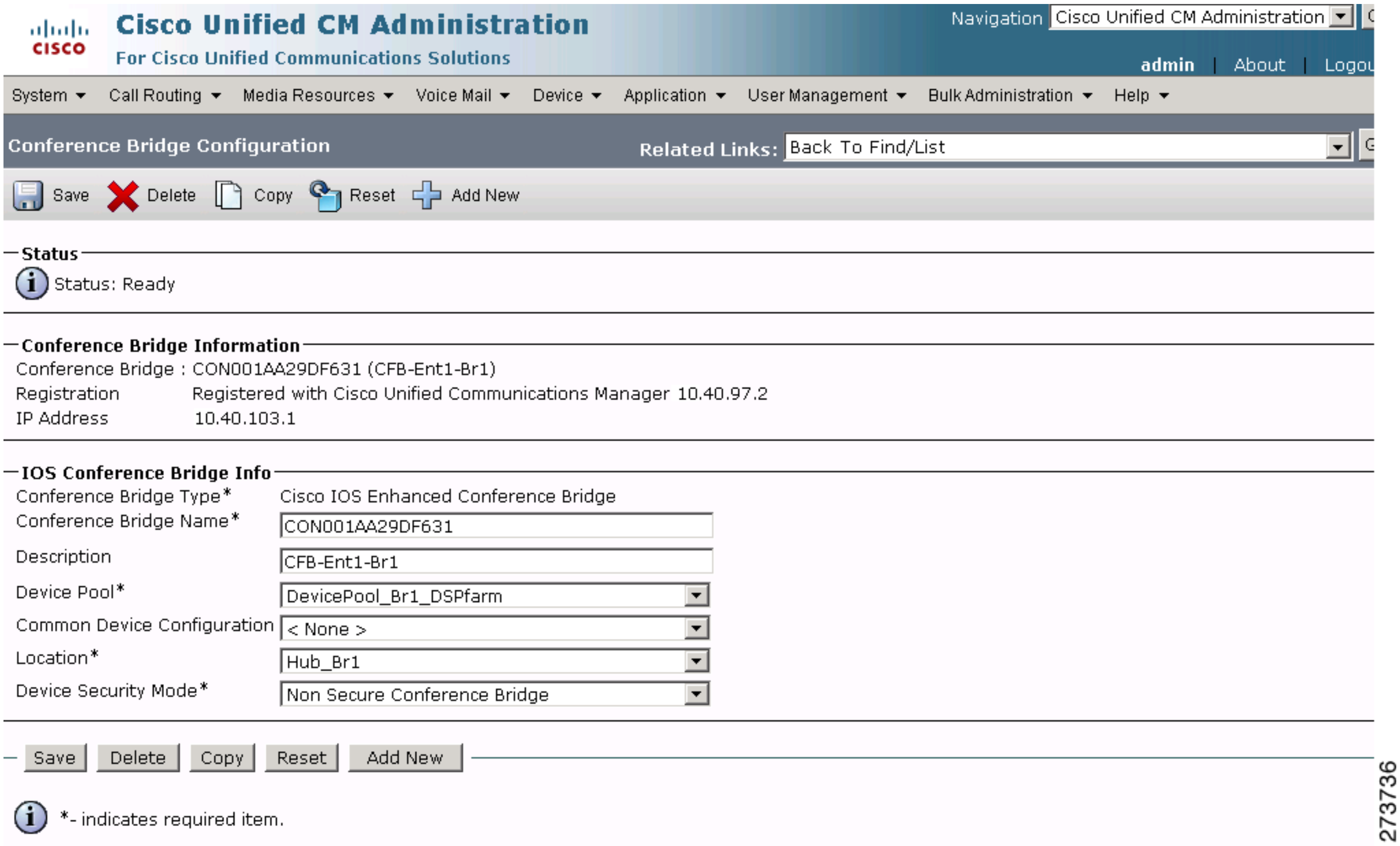
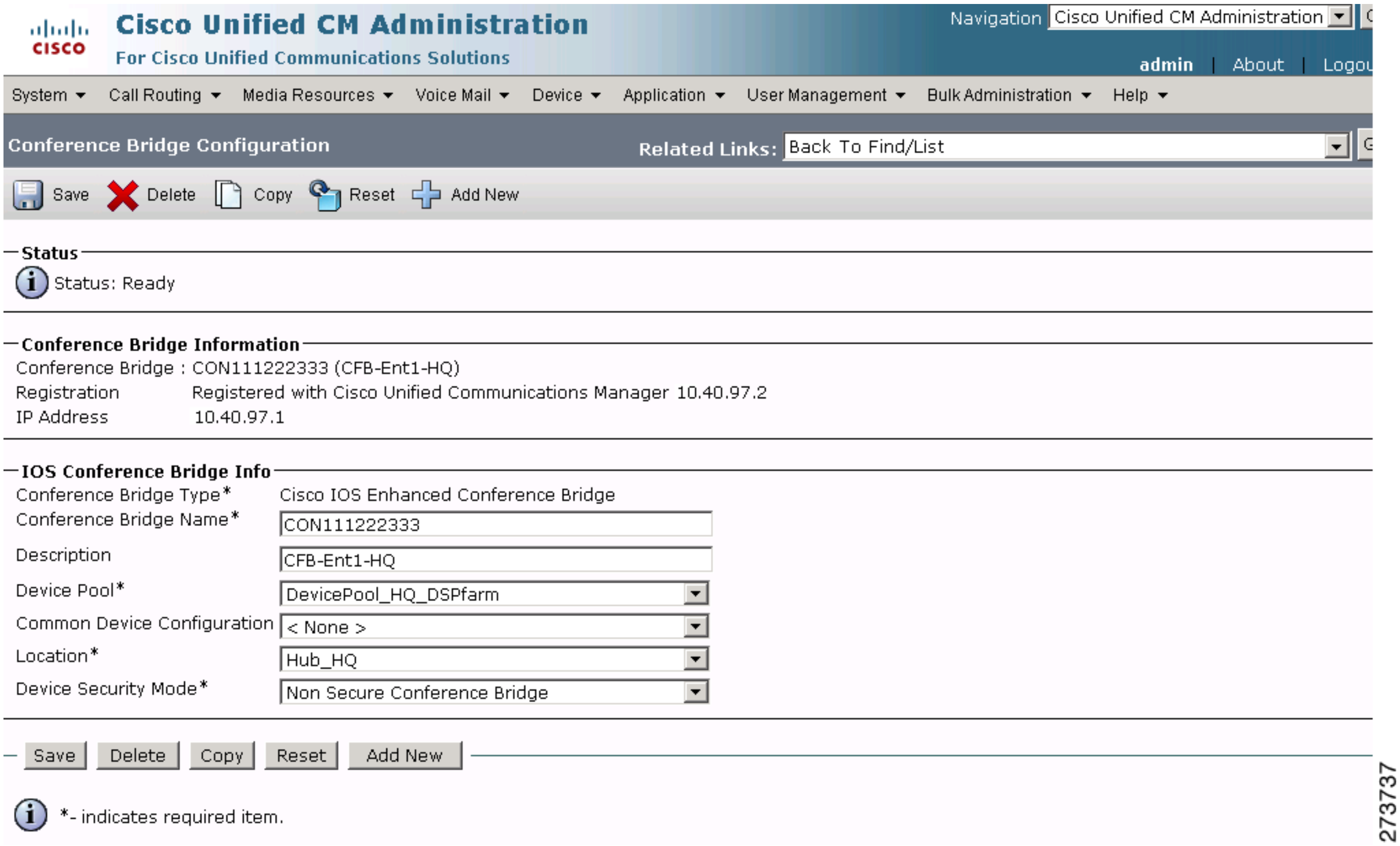


Figure 57 Media Resources Conference Bridges CFB Enterprise 1 HQ Cisco Unified CM Administration Window



Media Resources: Media Termination Point Parameters

To configure the media resources media termination point parameters for the Cisco Unified CM, click **Media Resources** > **Media Termination Point** menu in the Cisco Unified CM Administration window.

Figure 58 Media Resources Media Termination Point Cisco Unified CM Administration Window

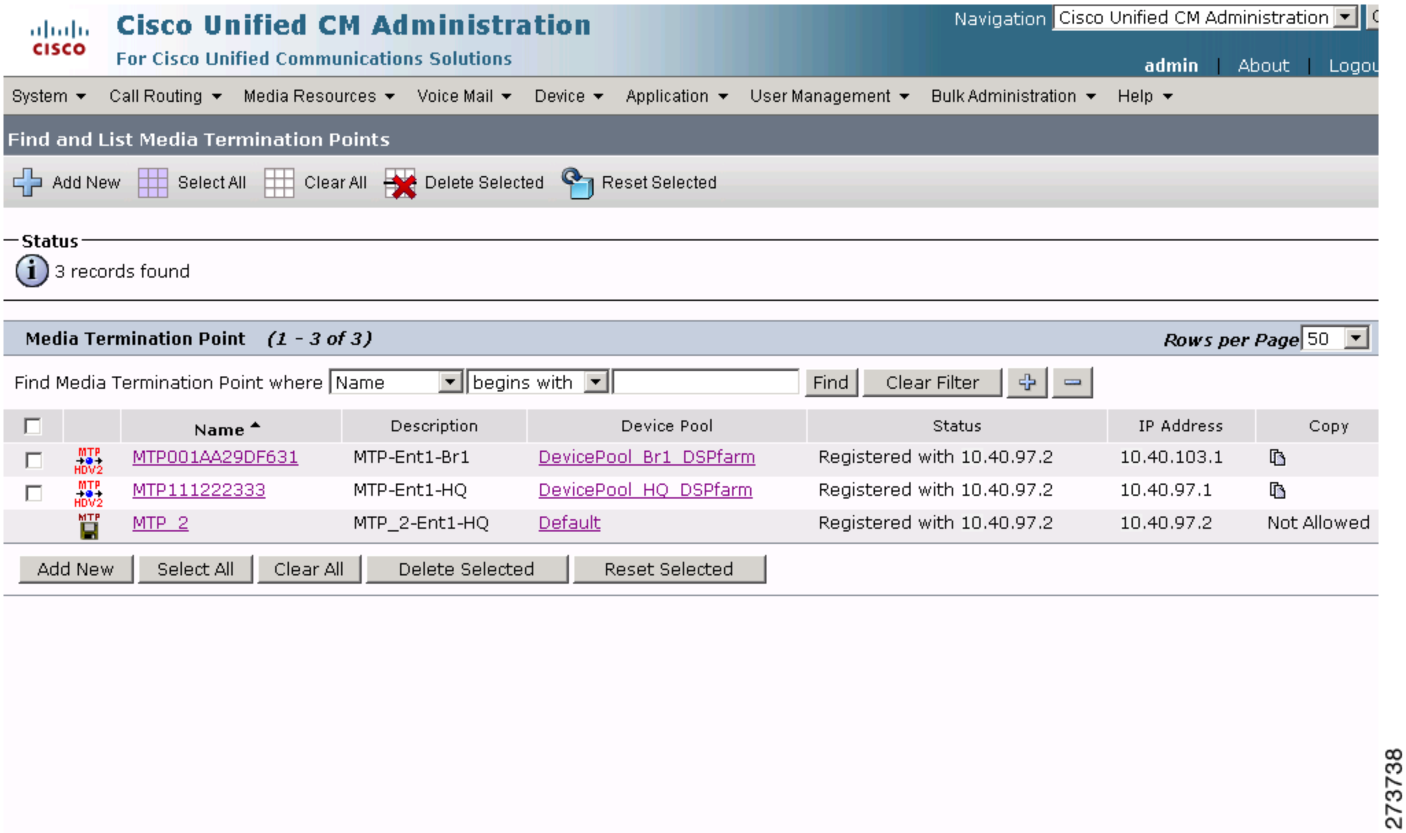


Figure 59 Media Resources Media Termination Point MTP Enterprise 1 Branch 1 Administration Window

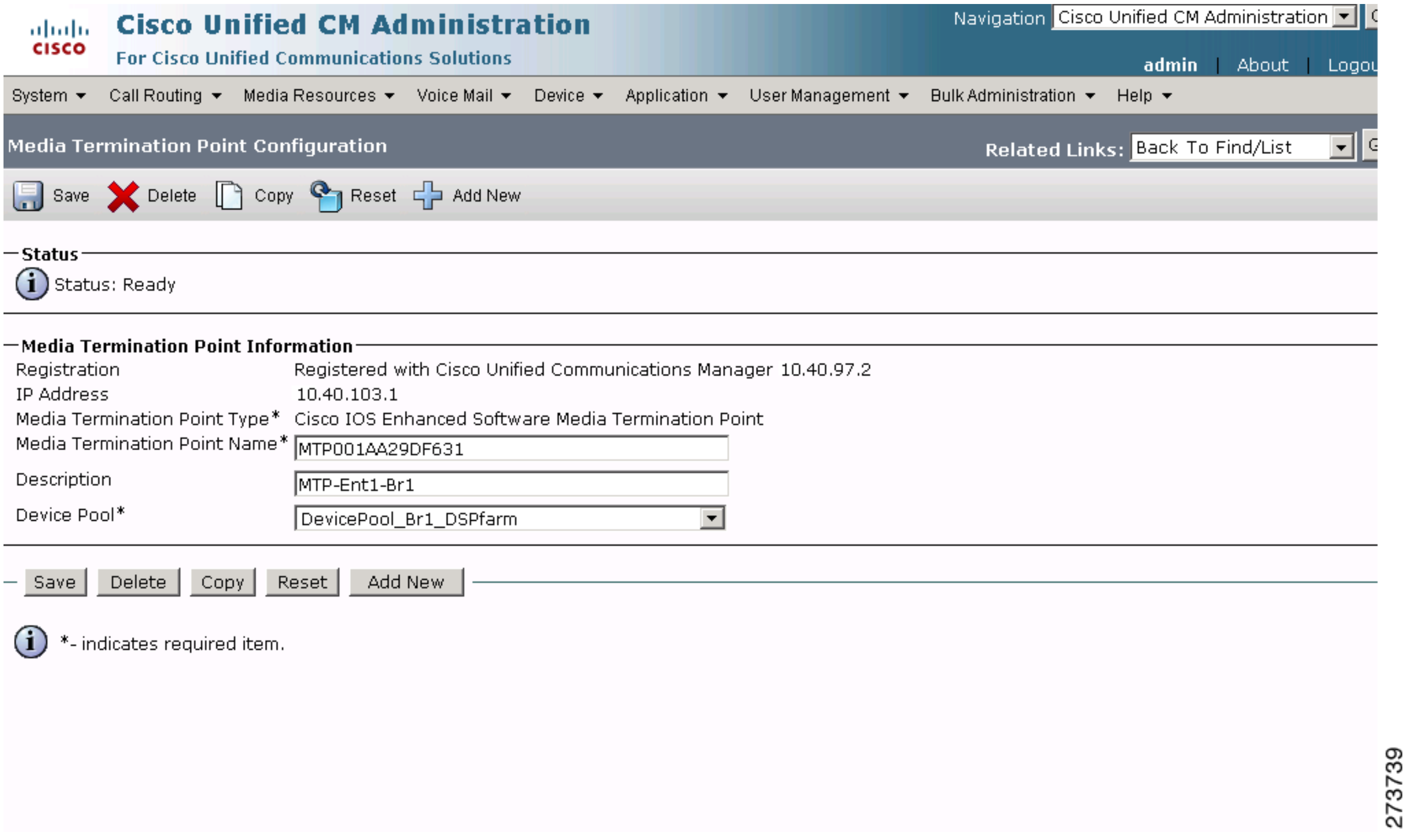
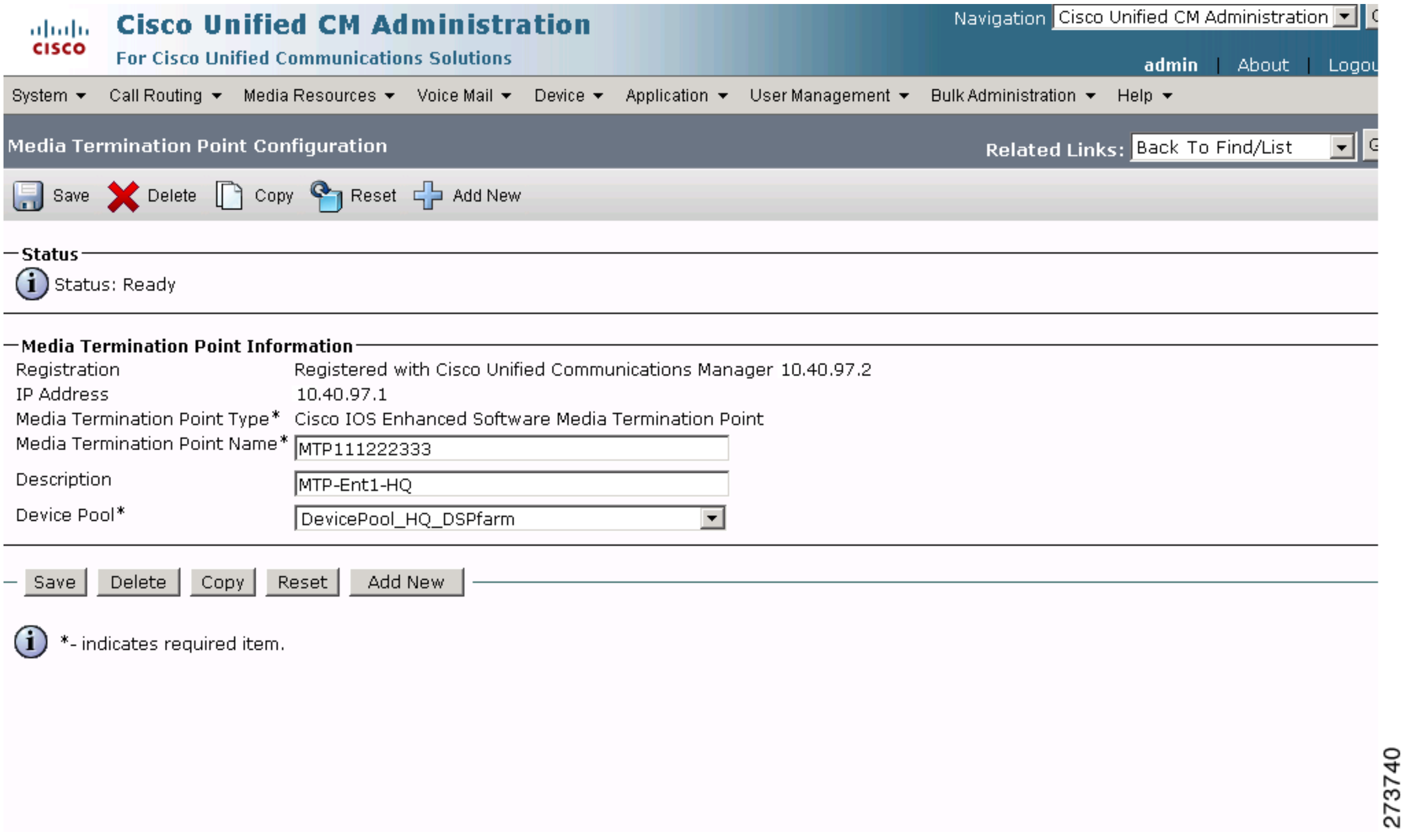


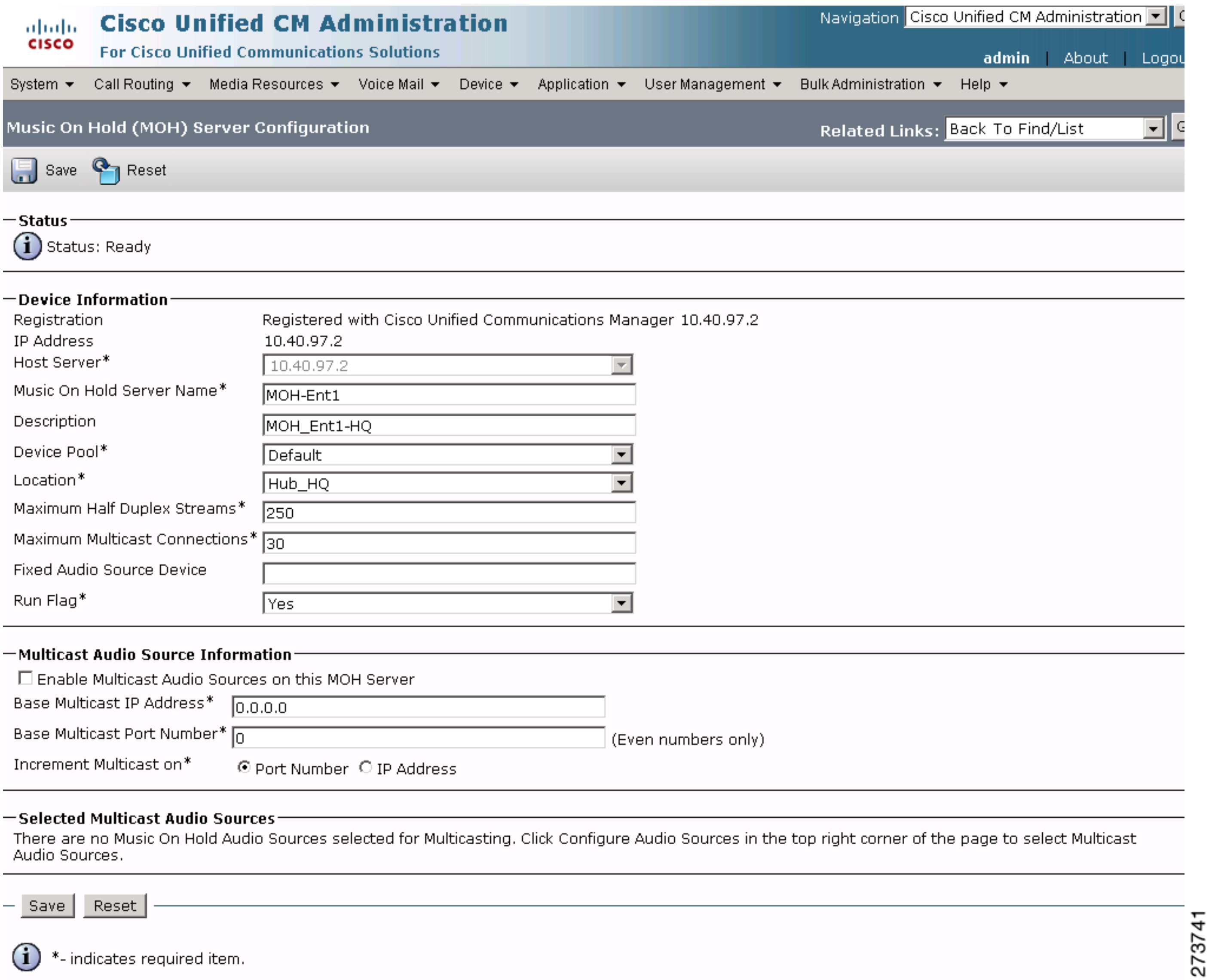
Figure 60 Media Resources Media Termination Point MTP Enterprise 1 HQ Cisco Unified CM Administration Window



Media Resources: Music on Hold Server Parameters

To configure the media resources music on hold server parameters for the Cisco Unified CM, click **Media Resources** > **Music On Hold Server** menu in the Cisco Unified CM Administration window.

Figure 61 Media Resources Music on Hold Server MOH Enterprise 1 HQ Cisco Unified CM Administration Window



Media Resources: Transcoder Parameters

To configure the media resources transcoder parameters for the Cisco Unified CM, click **Media Resources** > **Transcoder** menu in the Cisco Unified CM Administration window.

Figure 62 Media Resources Transcoder Cisco Unified CM Administration Window

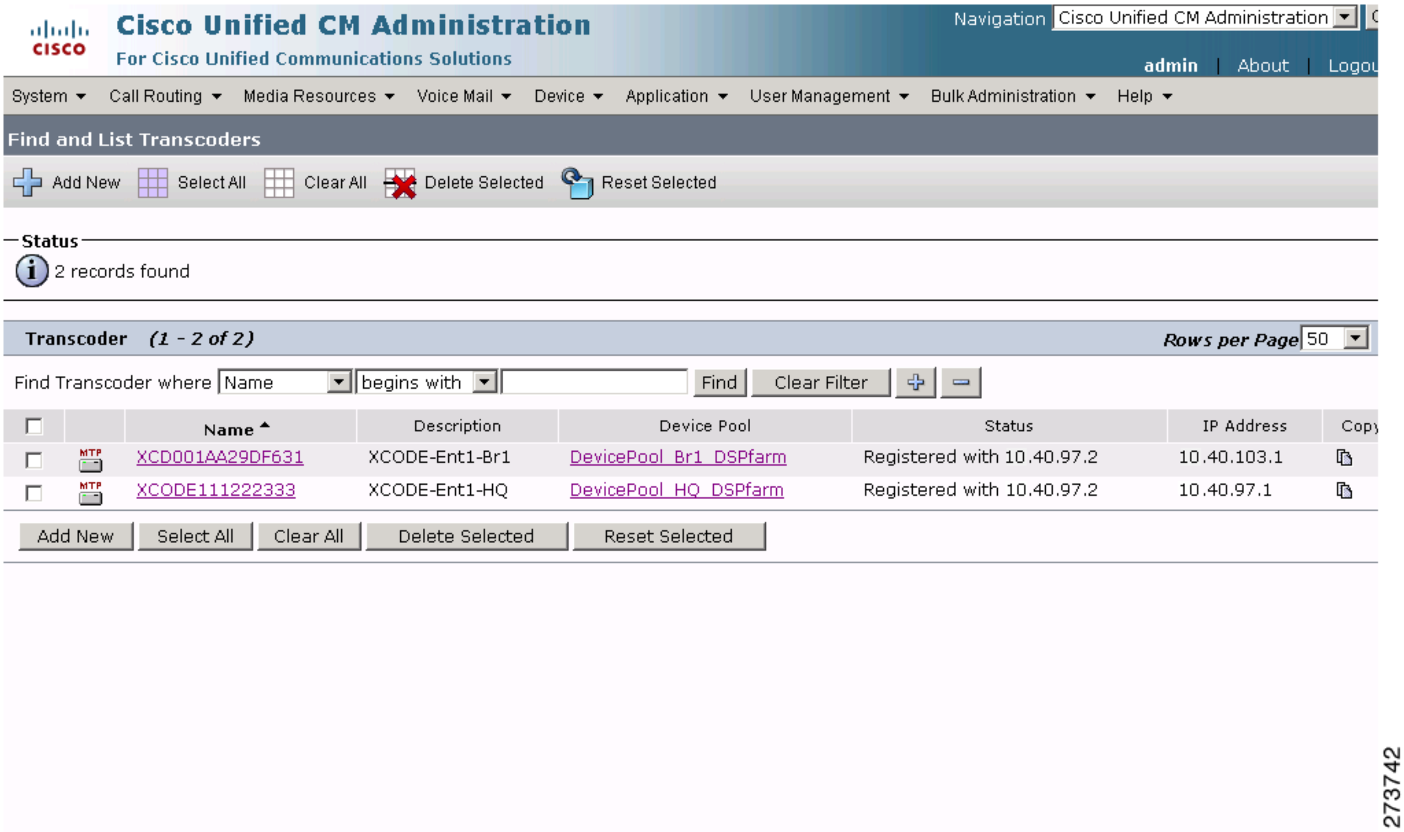


Figure 63 Media Resources Transcoder XCODE Enterprise 1 Branch 1 Cisco Unified CM Administration Window

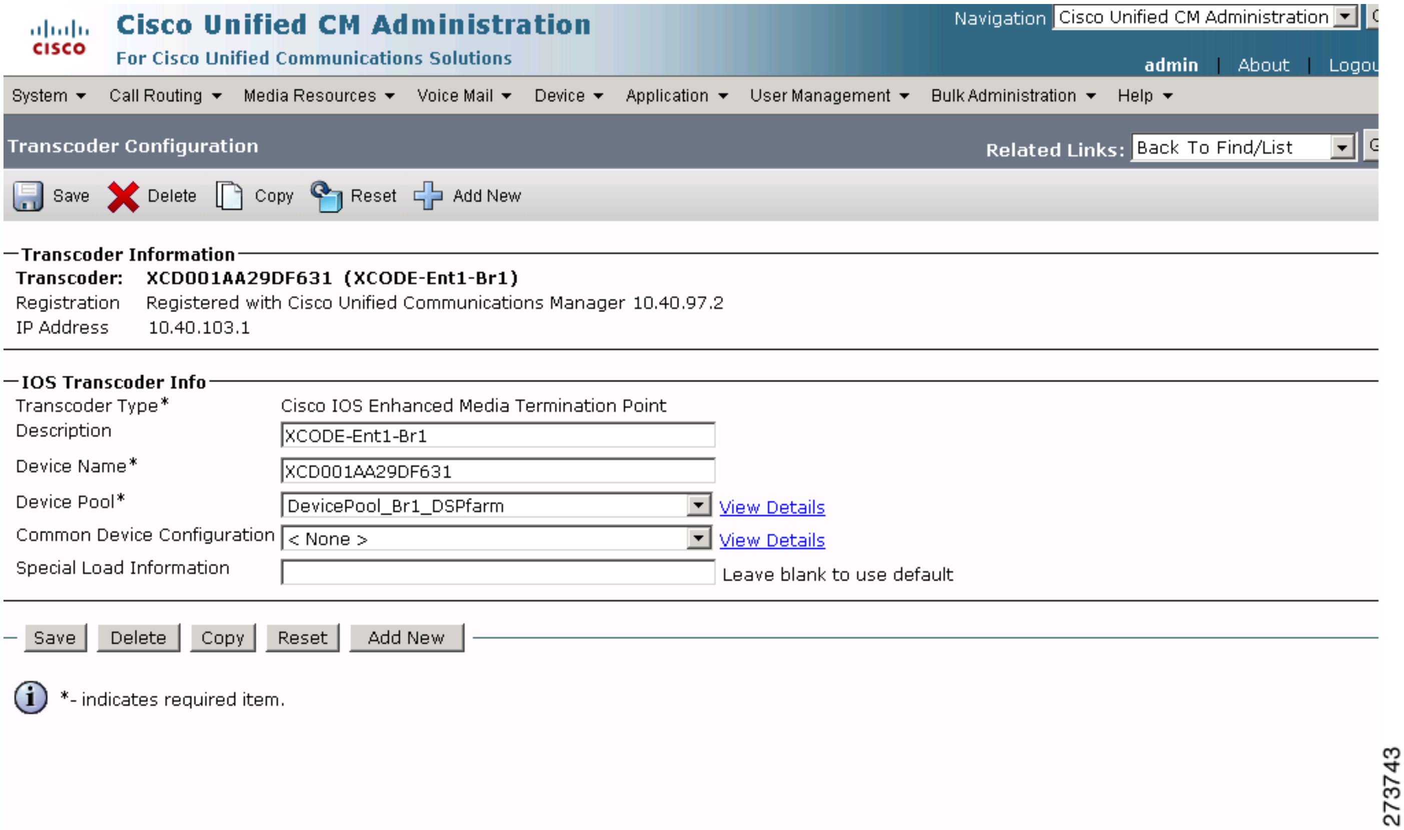
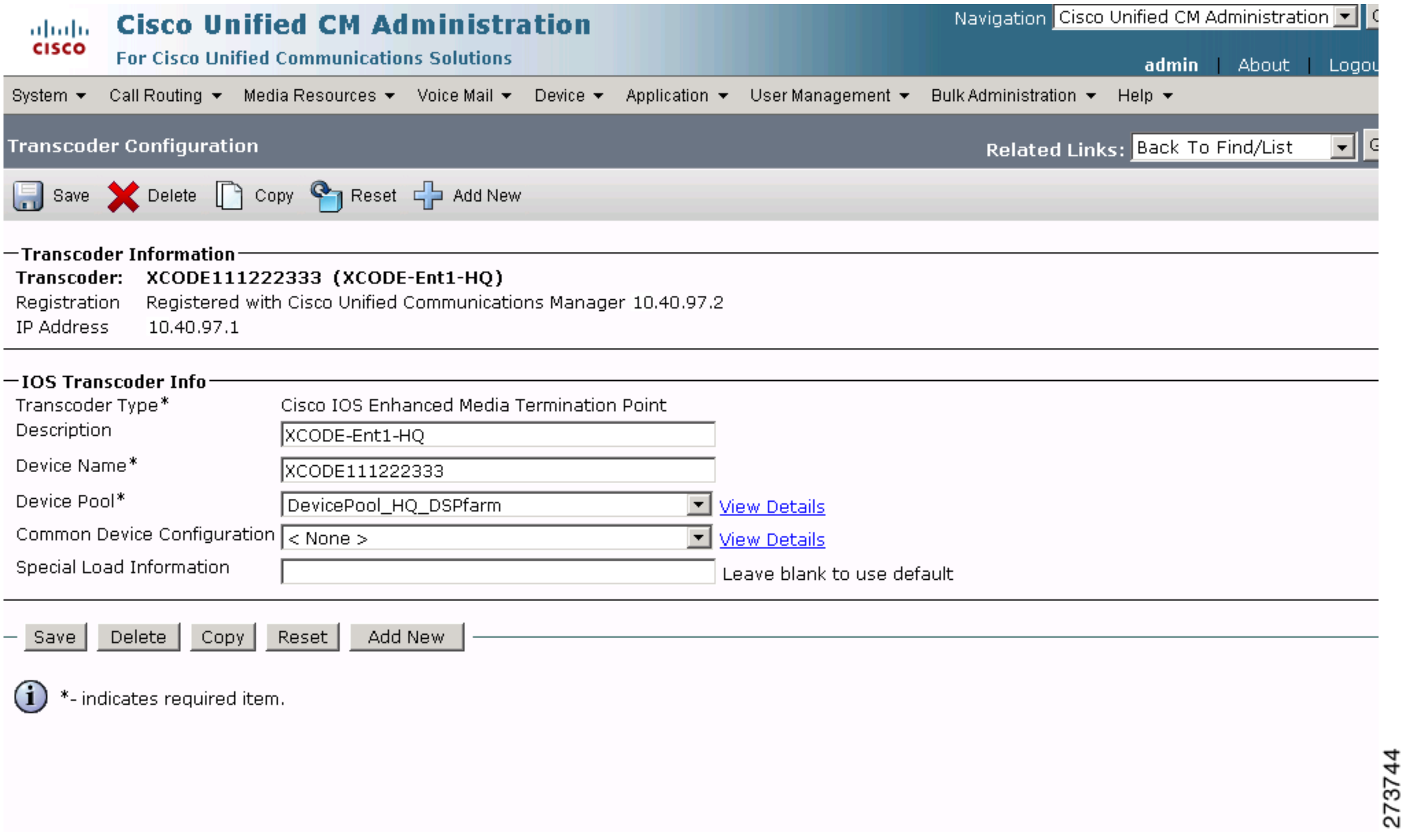


Figure 64 Media Resources Transcoder XCODE Enterprise 1 HQ Cisco Unified CM Administration Window



Media Resources: Media Resource Group Parameters

To configure the media resources media resource group parameters for the Cisco Unified CM, click **Media Resources** > **Media Resource Group** menu in the Cisco Unified CM Administration window.

Figure 65 Media Resources-Media Resource Group Cisco Unified CM Administration Window

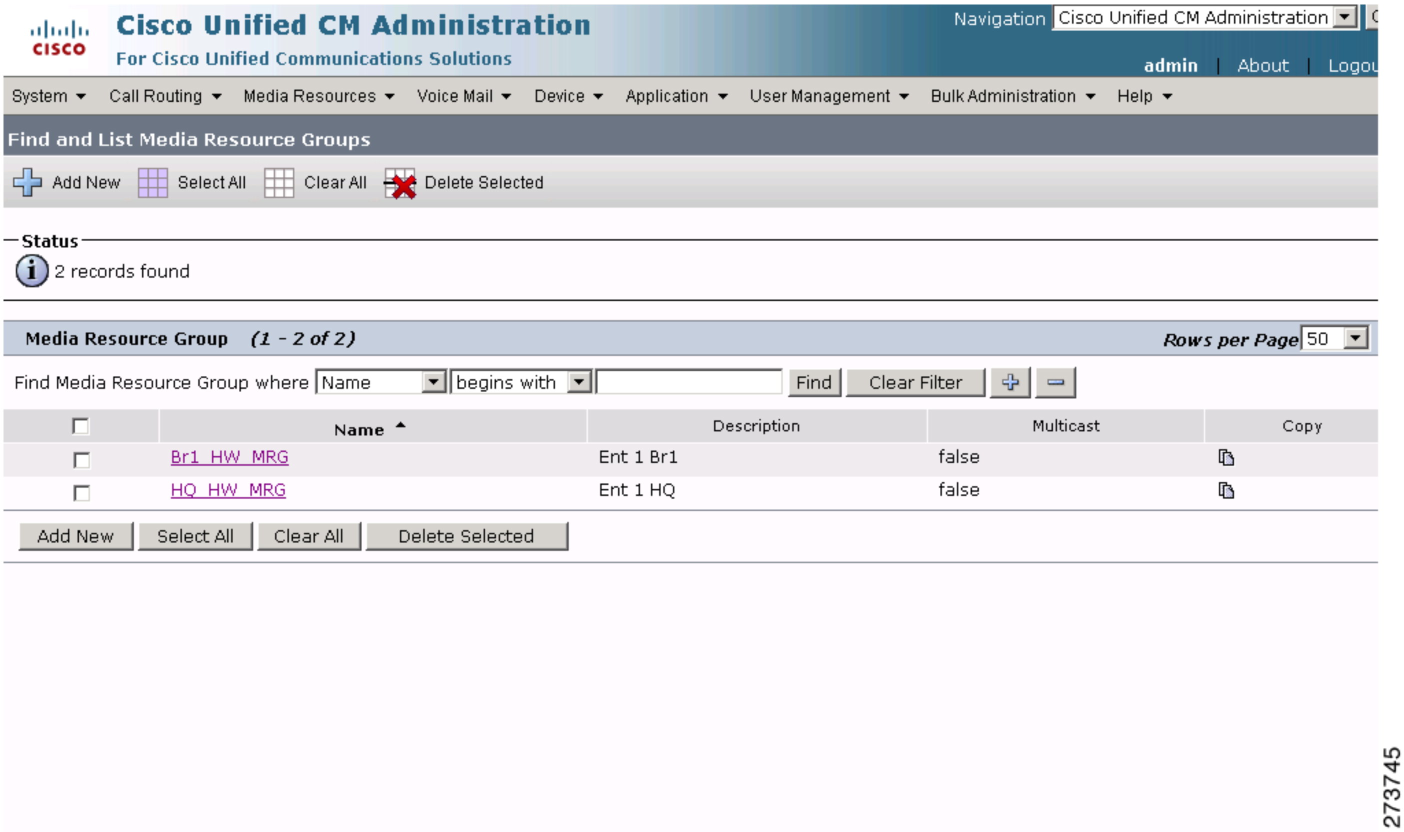


Figure 66 Media Resources-Media Resource Group Enterprise 1 Branch 1 Cisco Unified CM Administration Window

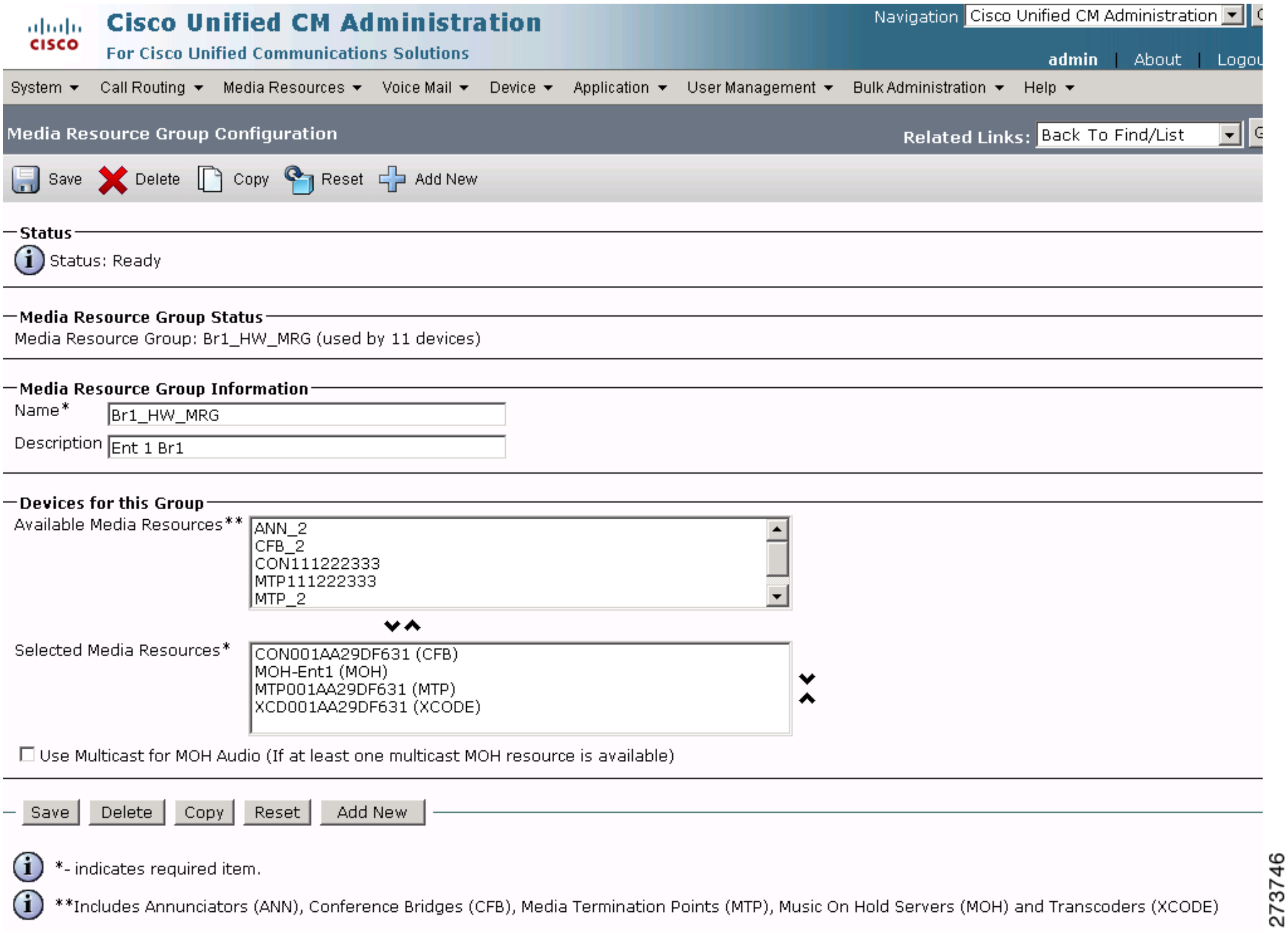
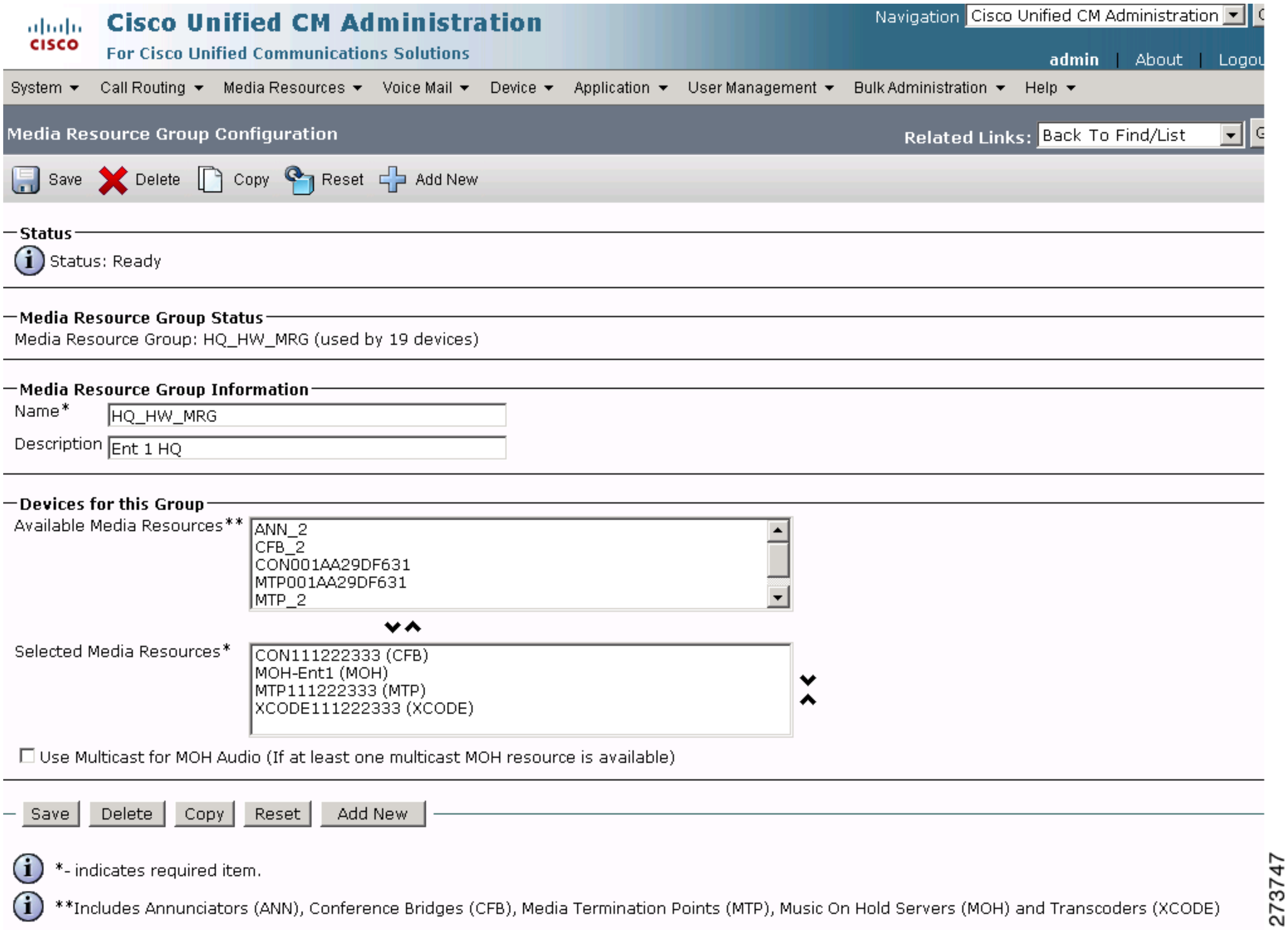


Figure 67 Media Resources-Media Resource Group Enterprise 1 HQ Cisco Unified CM Administration Window



Media Resources: Media Resource Group List Parameters

To configure the media resources media resource group list parameters for the Cisco Unified CM, click **Media Resources** > **Media Resource Group List** menu in the Cisco Unified CM Administration window.

Figure 68 Media Resources-Media Resource Group List Cisco Unified CM Administration Window

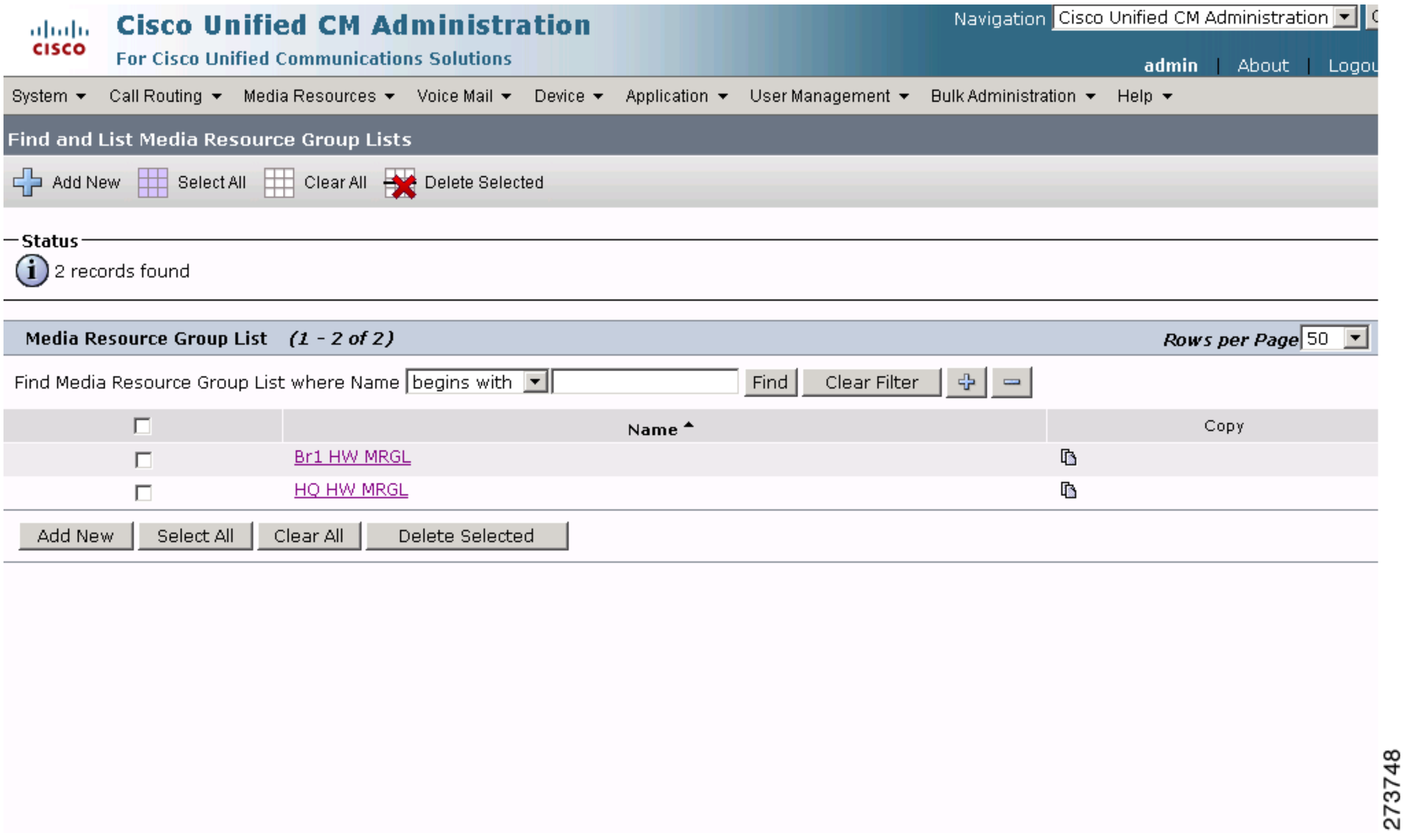


Figure 69 Media Resources-Media Resource Group List Branch 1 HW MRGL Cisco Unified CM Administration Window

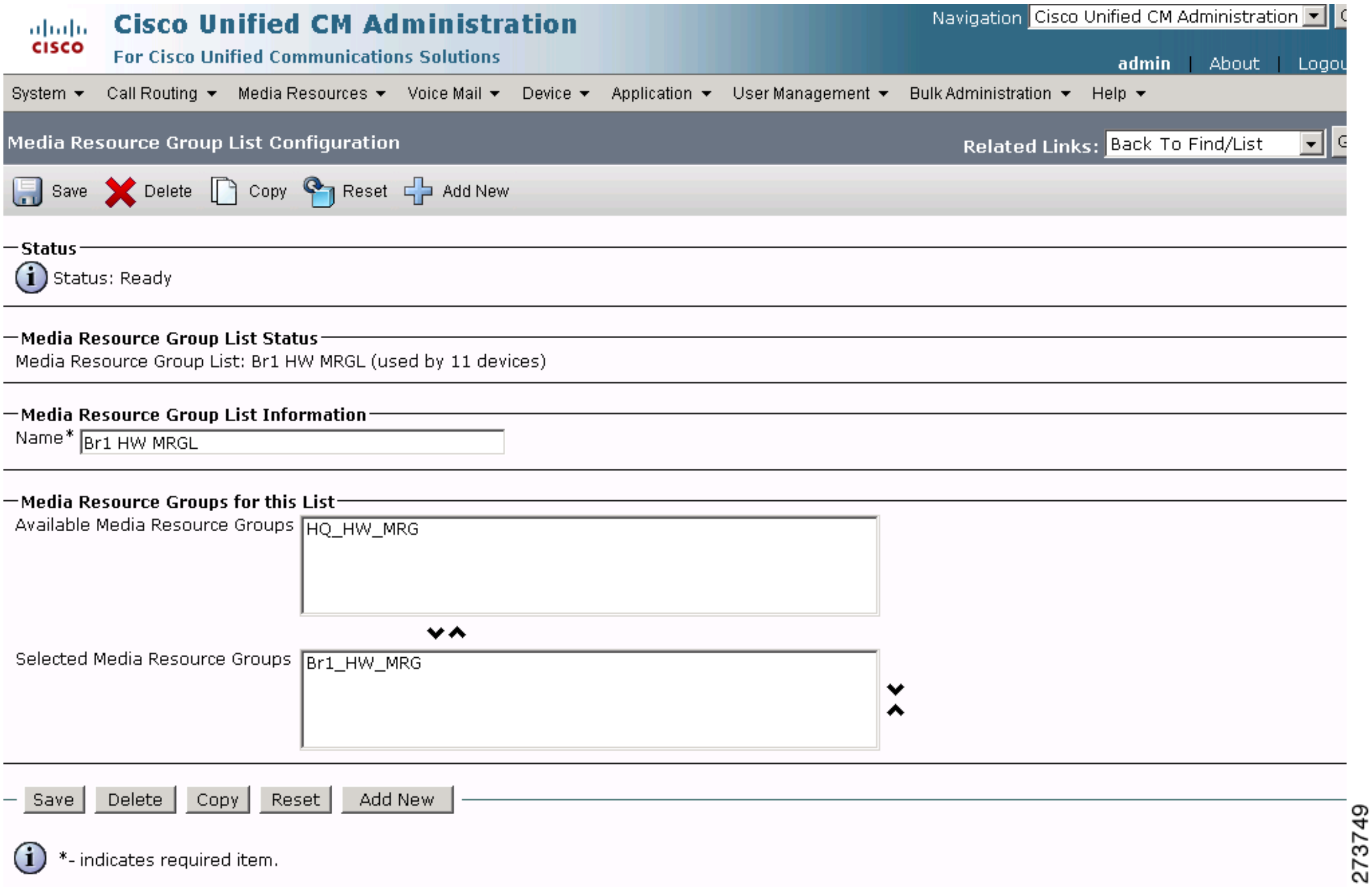
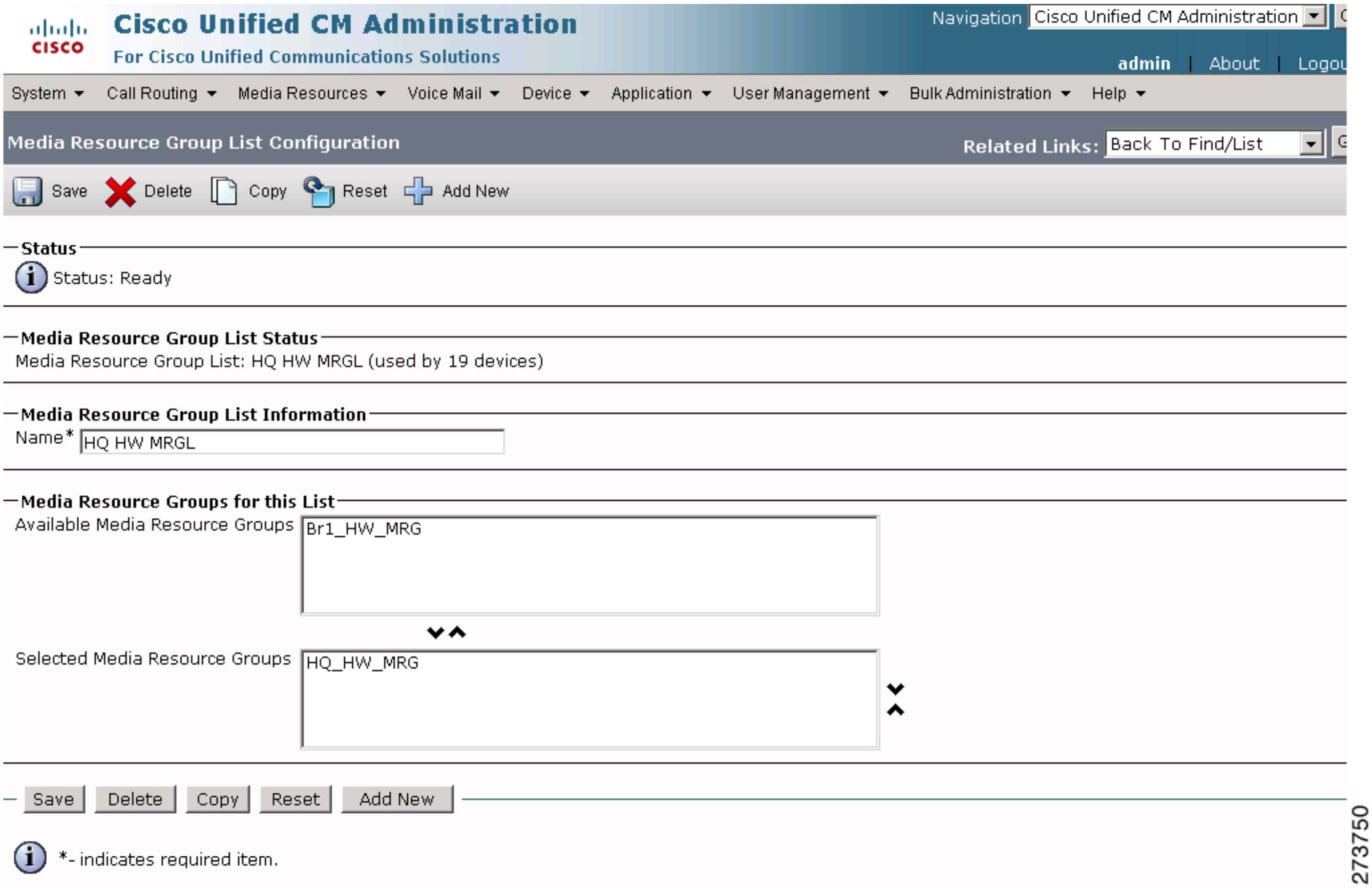


Figure 70 Media Resources-Media Resource Group List HQ HW MRGL Cisco Unified CM Administration Window



Configuring the Cisco Unified CM Voice Mail Parameters

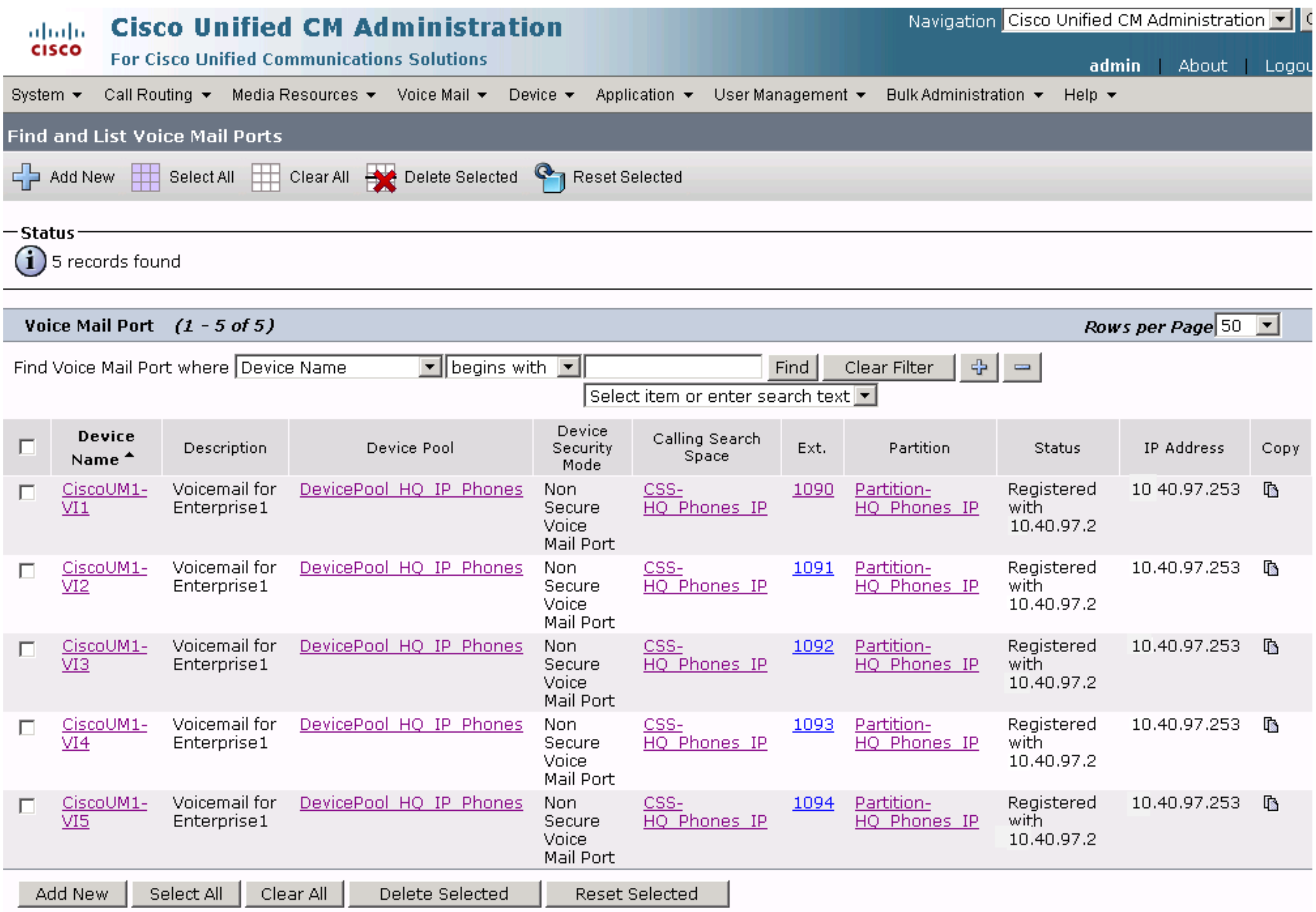
Use the Cisco Unified Communications Manager Administration window to configure the voice mail parameters. The voice mail parameter example configurations are shown in the following sections:

- Voice Mail: Cisco Voice Mail Port Parameters, page 95
- Voice Mail: Message Waiting Parameters, page 97
- Voice Mail: Voice Mail Pilot Parameters, page 100
- Voice Mail: Voice Mail Profile Parameters, page 101

Voice Mail: Cisco Voice Mail Port Parameters

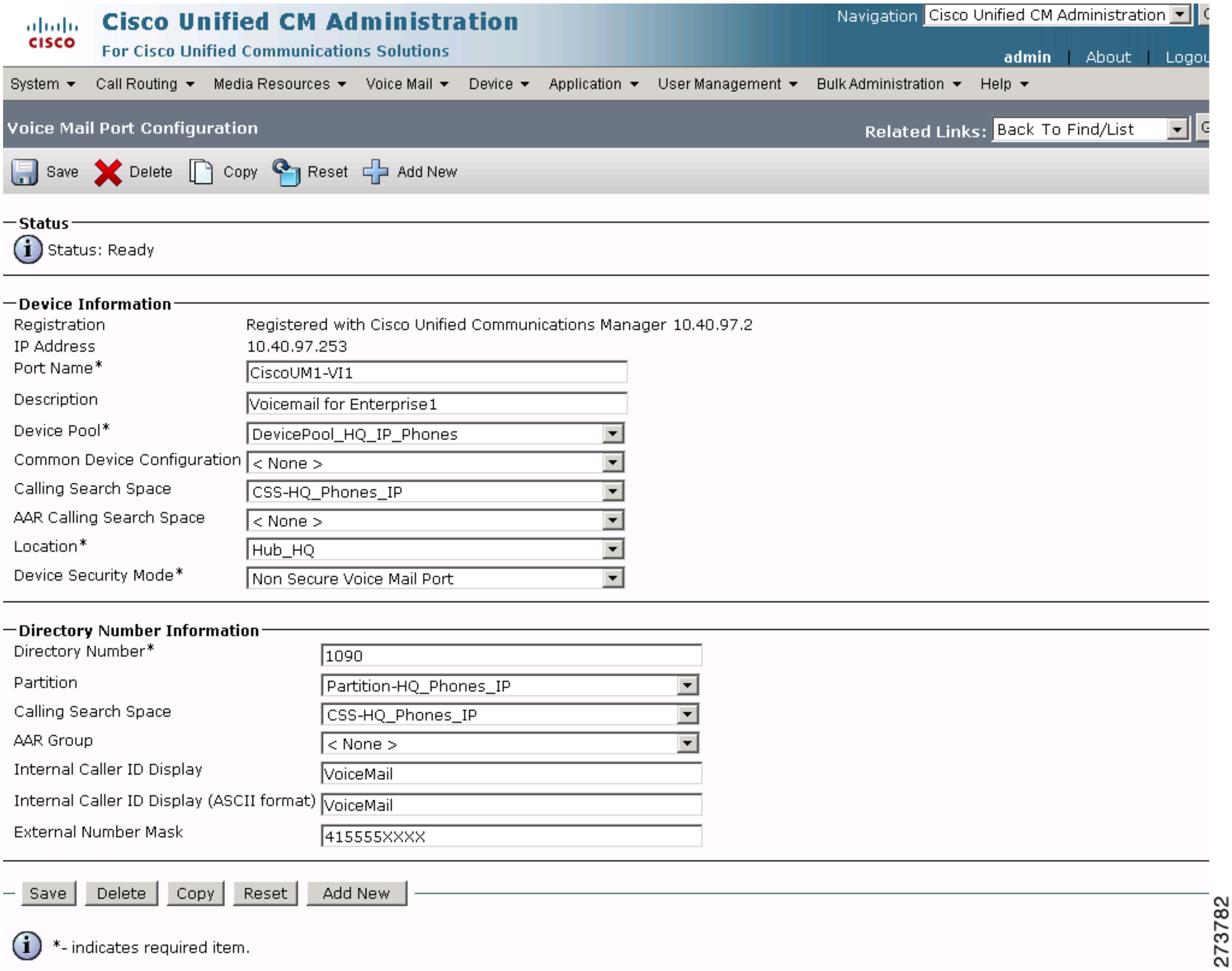
To configure the voice mail Cisco voice mail port parameters for the Cisco Unified CM, click **Voice Mail > Cisco Voice Mail Port** menu in the Cisco Unified CM Administration window.

Figure 71 Voice Mail Cisco Voice Mail Port Cisco Unified CM Administration Window



273781

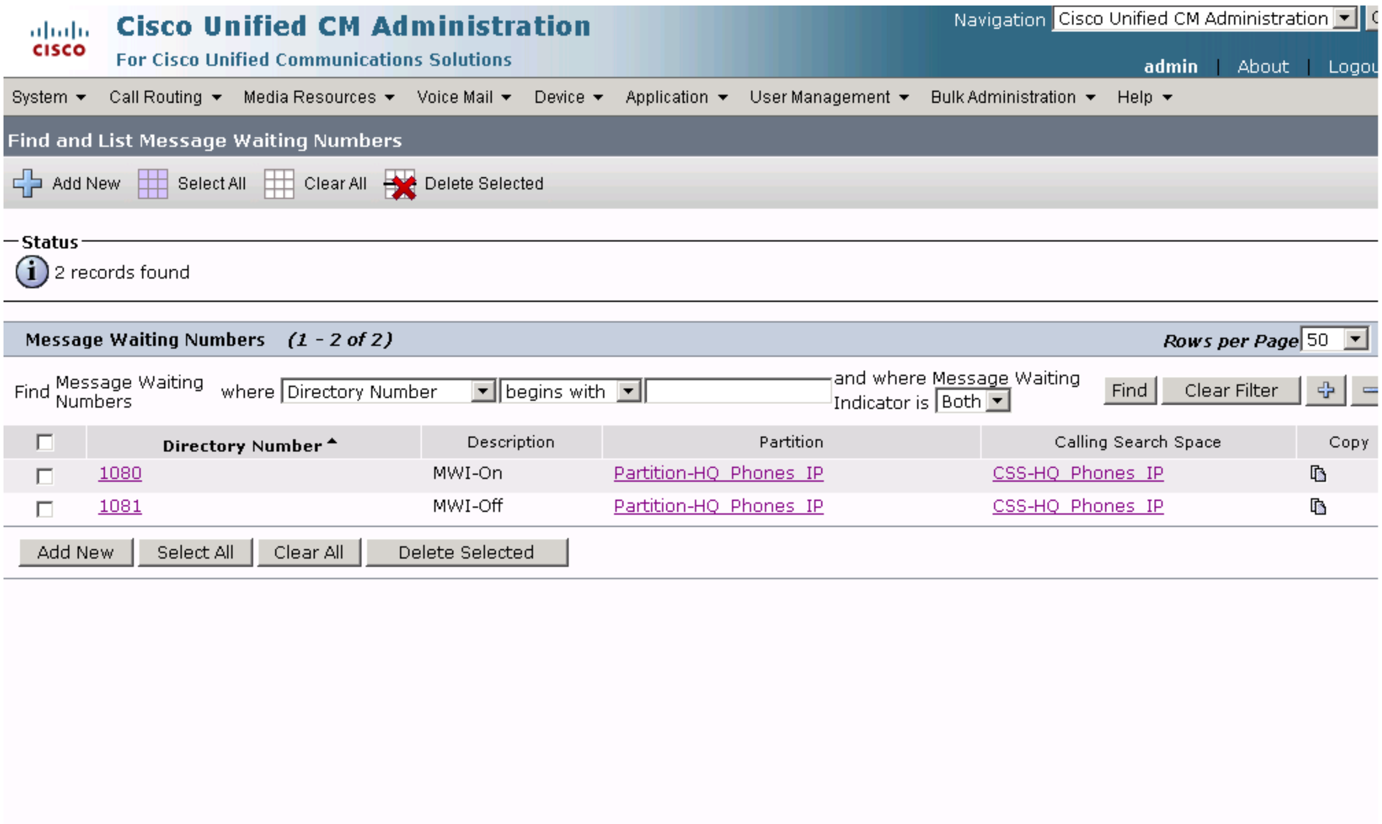
Figure 72 Voice Mail-Voice Mail Port CiscoUM1 VI1 Cisco Unified CM Administration Window



Voice Mail: Message Waiting Parameters

To configure the voice mail message waiting parameters for the Cisco Unified CM, click **Voice Mail** > **Message Waiting** menu in the Cisco Unified CM Administration window.

Figure 73 Voice Mail Message Waiting Cisco Unified CM Administration Window



273783

Figure 74 Voice Mail Message Waiting MWI ON Cisco Unified CM Administration Window

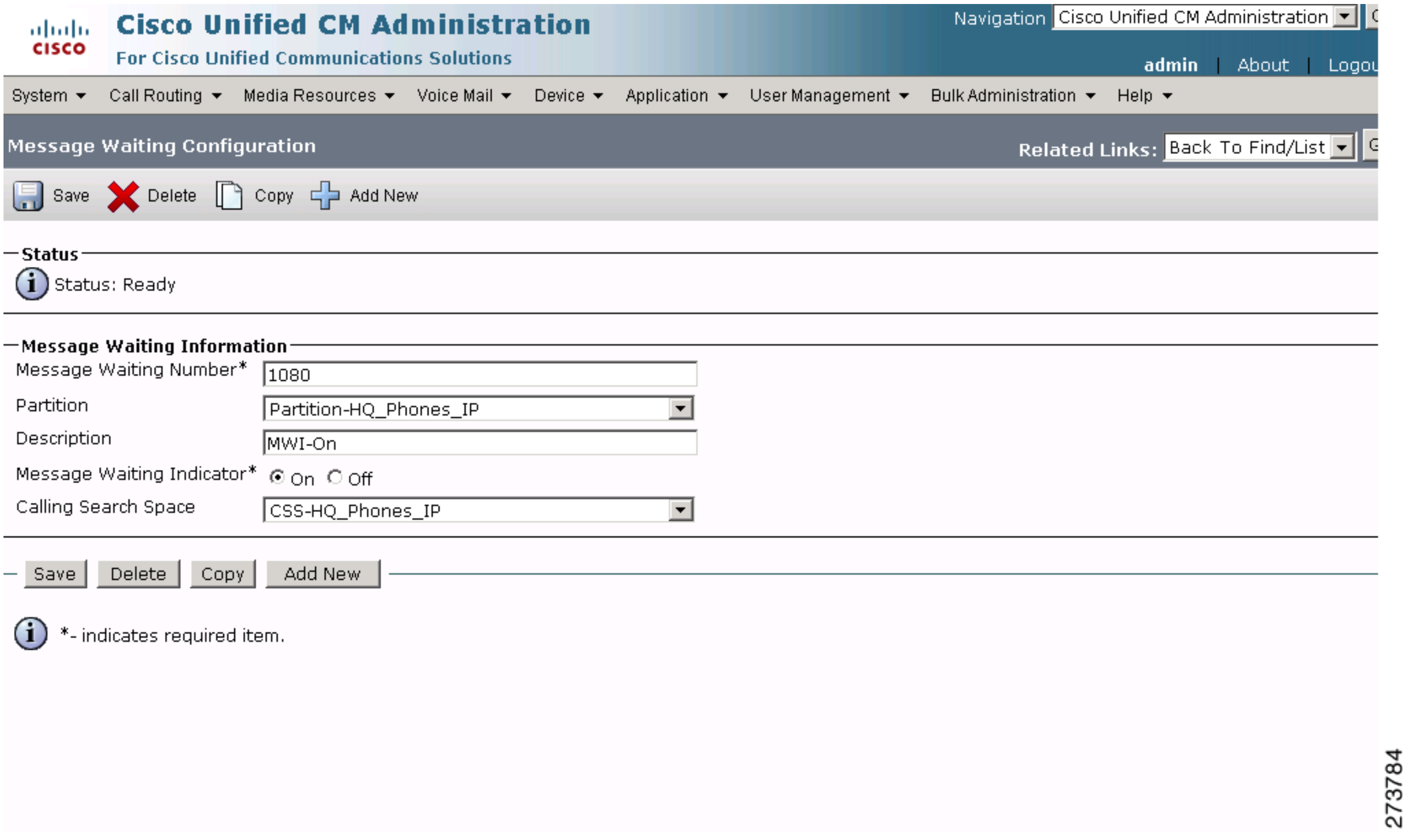
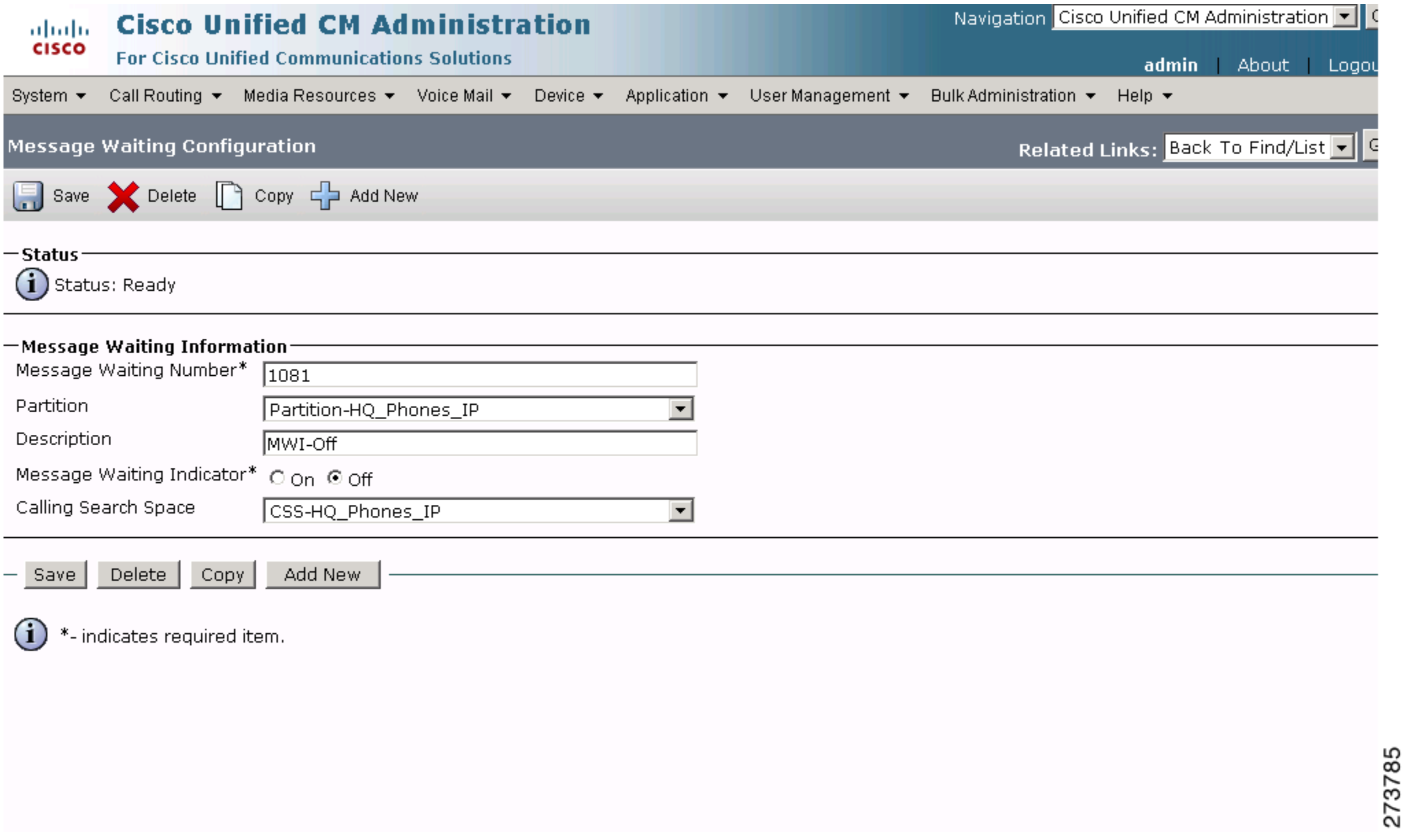


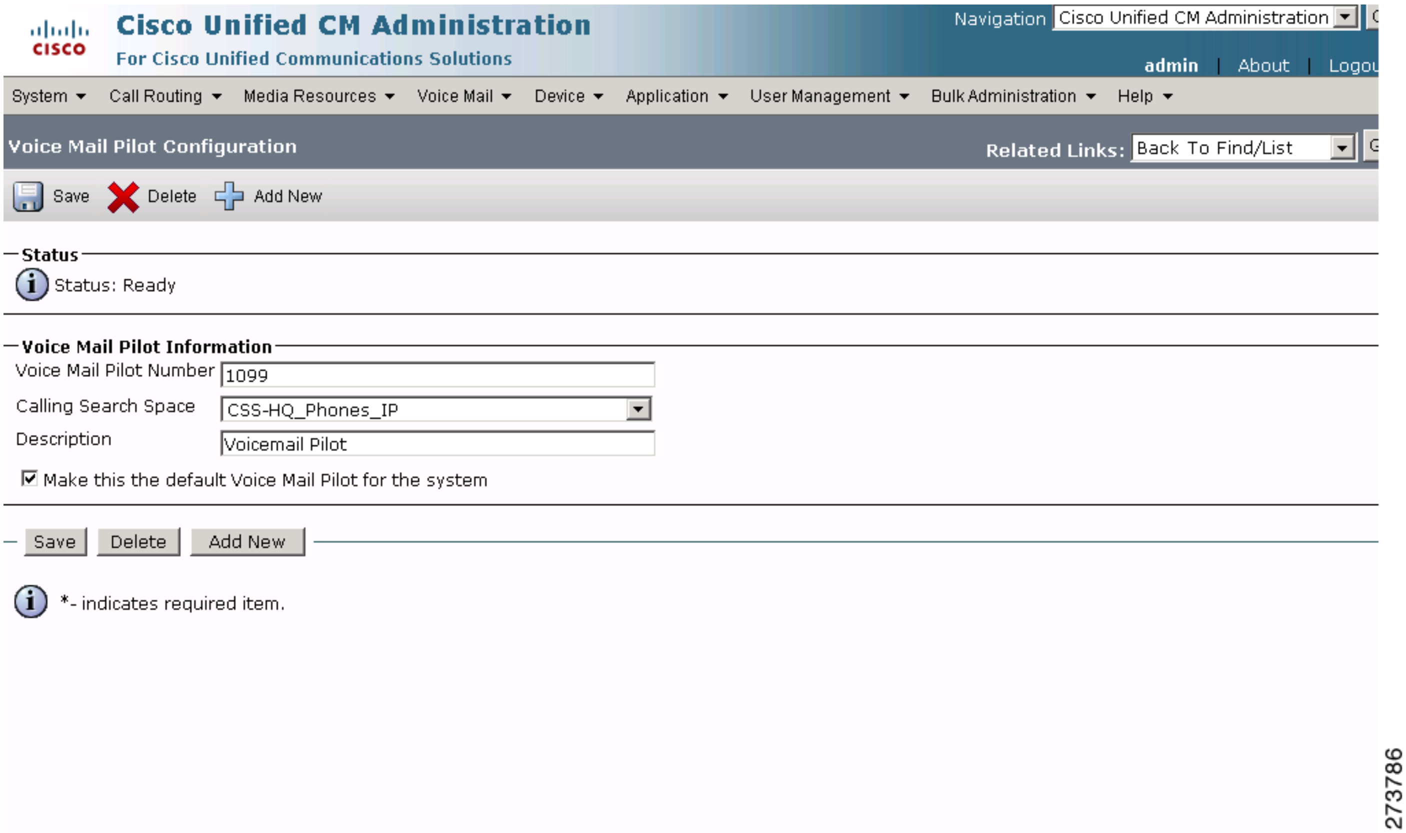
Figure 75 Voice Mail Message Waiting MWI Off Cisco Unified CM Administration Window



Voice Mail: Voice Mail Pilot Parameters

To configure the voice mail voice mail pilot parameters for the Cisco Unified CM, click **Voice Mail** > **Voice Mail Pilot** menu in the Cisco Unified CM Administration window.

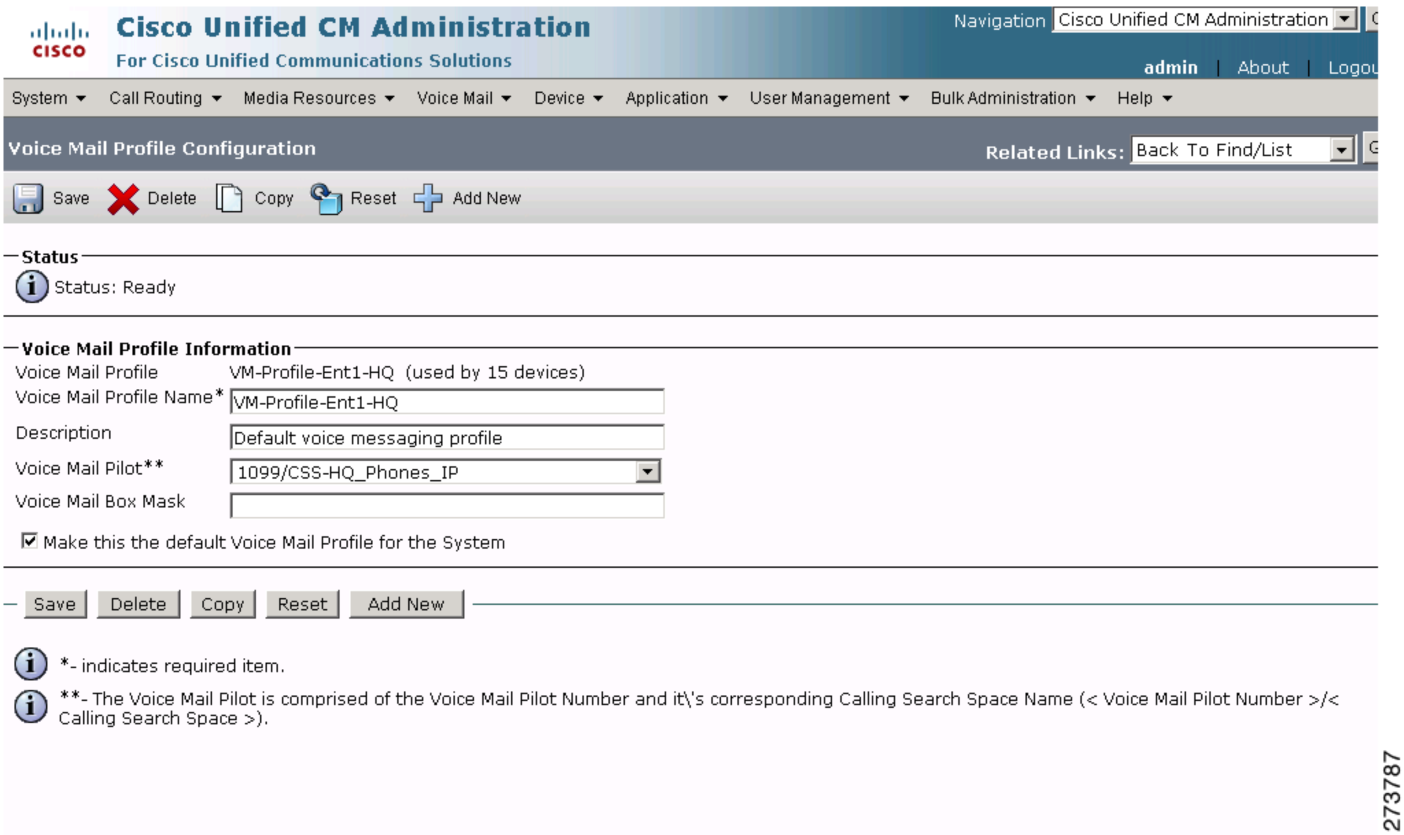
Figure 76 Voice Mail-Voice Mail Pilot 1099 Cisco Unified CM Administration Window



Voice Mail: Voice Mail Profile Parameters

To configure the voice mail voice mail profile parameters for the Cisco Unified CM, click **Voice Mail** > **Voice Mail Profile** menu in the Cisco Unified CM Administration window.

Figure 77 Voice Mail-Voice Mail Profile VM Profile Enterprise 1 HQ Cisco Unified CM Administration Window



Configuring the Cisco Unified CM Device Parameters

Use the Cisco Unified Communications Manager Administration window to configure the device parameters. The device parameter example configurations are shown in the following sections:

- Device: Gateway Parameters, page 102
- Device: Phone Parameters, page 109
- Device: Trunk Parameters, page 114

Device: Gateway Parameters

To configure the device gateway parameters for the Cisco Unified CM, click **Device** > **Gateway** menu in the Cisco Unified CM Administration window.

Figure 78 Device Gateway Cisco Unified CM Administration Window

Figure 79 Device Gateway Enterprise 1 Branch 1 Enterprise 1.com Cisco Unified CM Administration Window

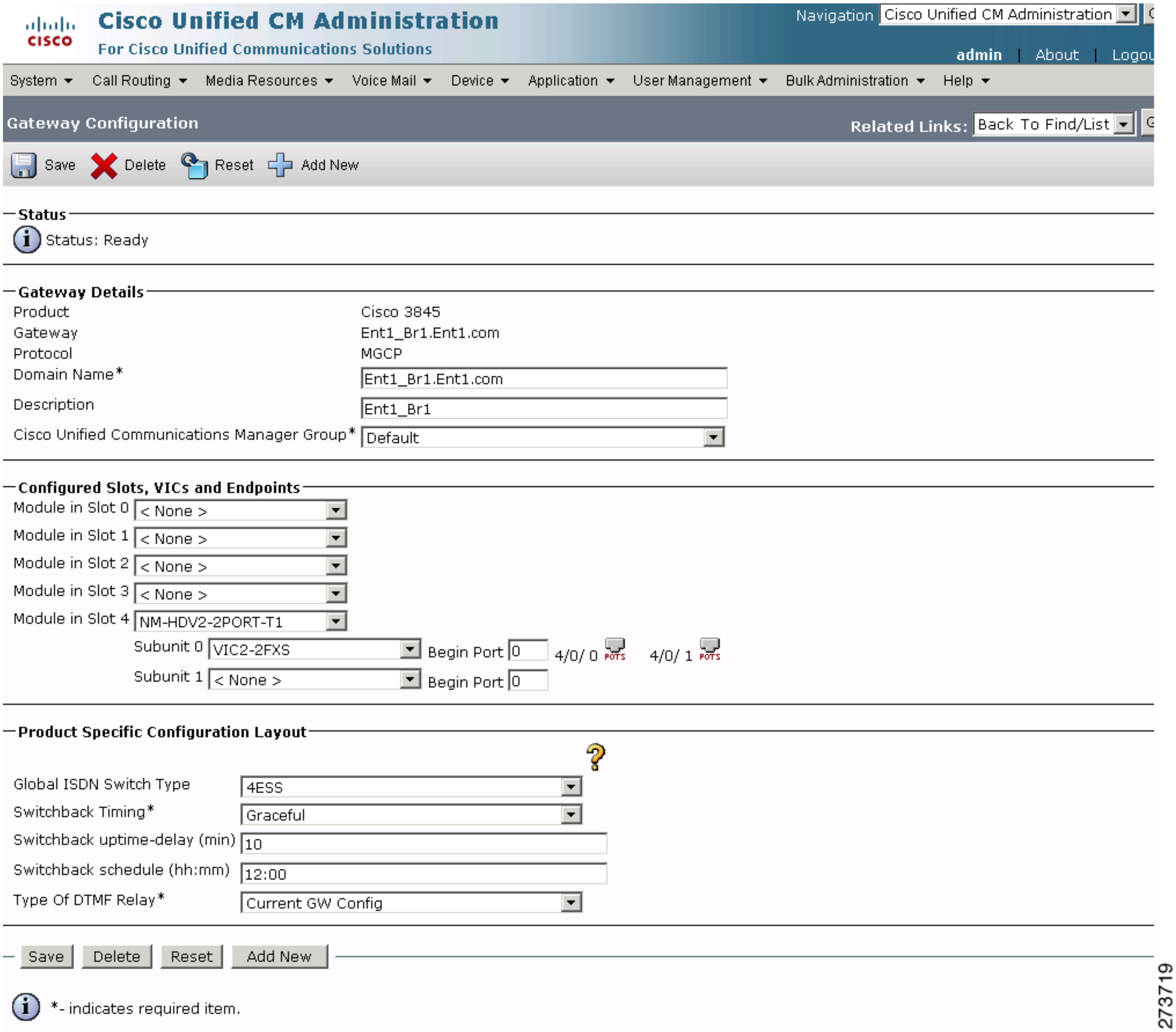


Figure 80 Device Gateway Enterprise 1 Branch 1 Enterprise 1.com pots 1110 Cisco Unified CM Administration Window

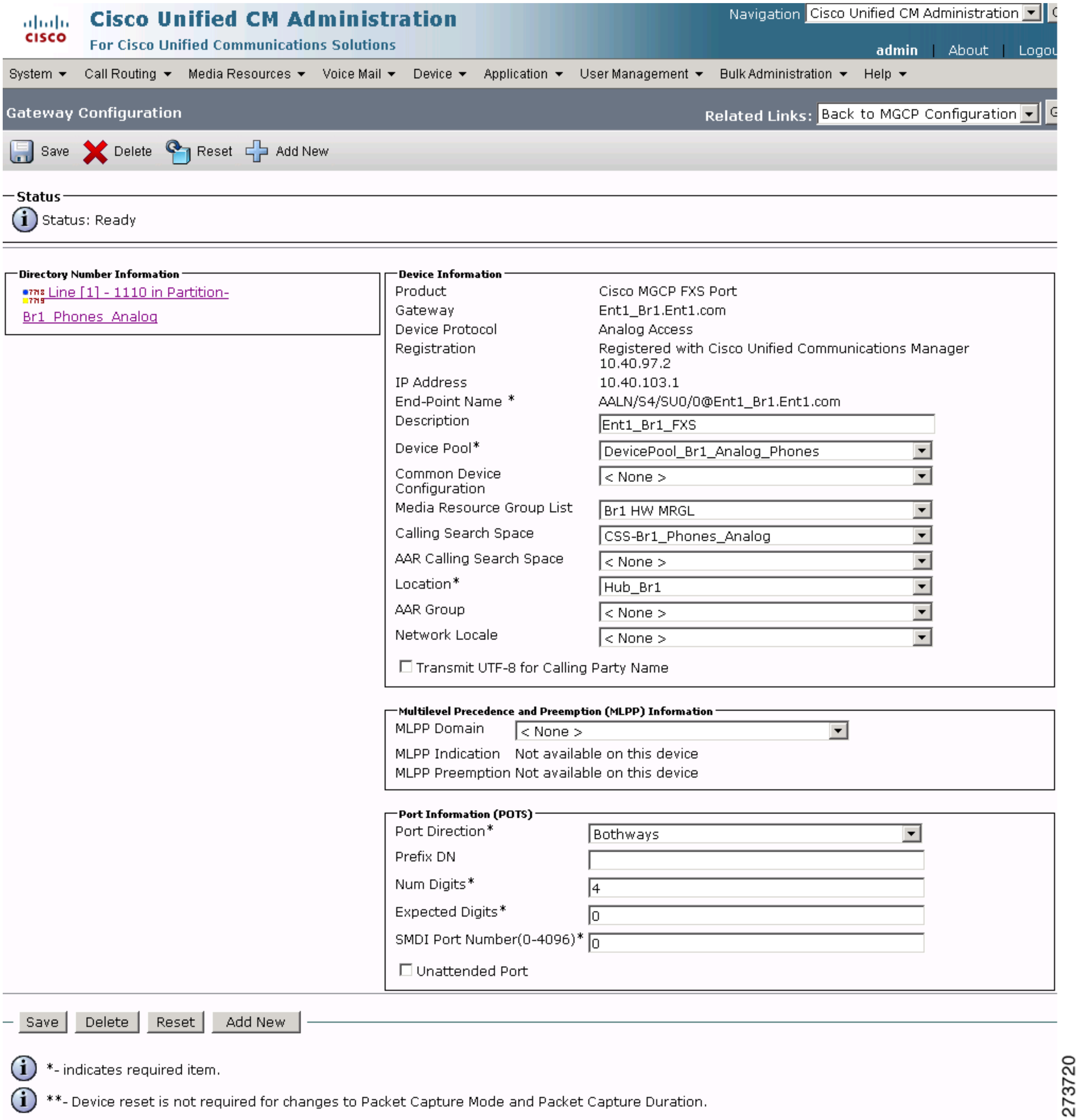


Figure 81 Device Gateway Enterprise 1 Branch 1 Enterprise 1.com pots 1110 Line Administration Window

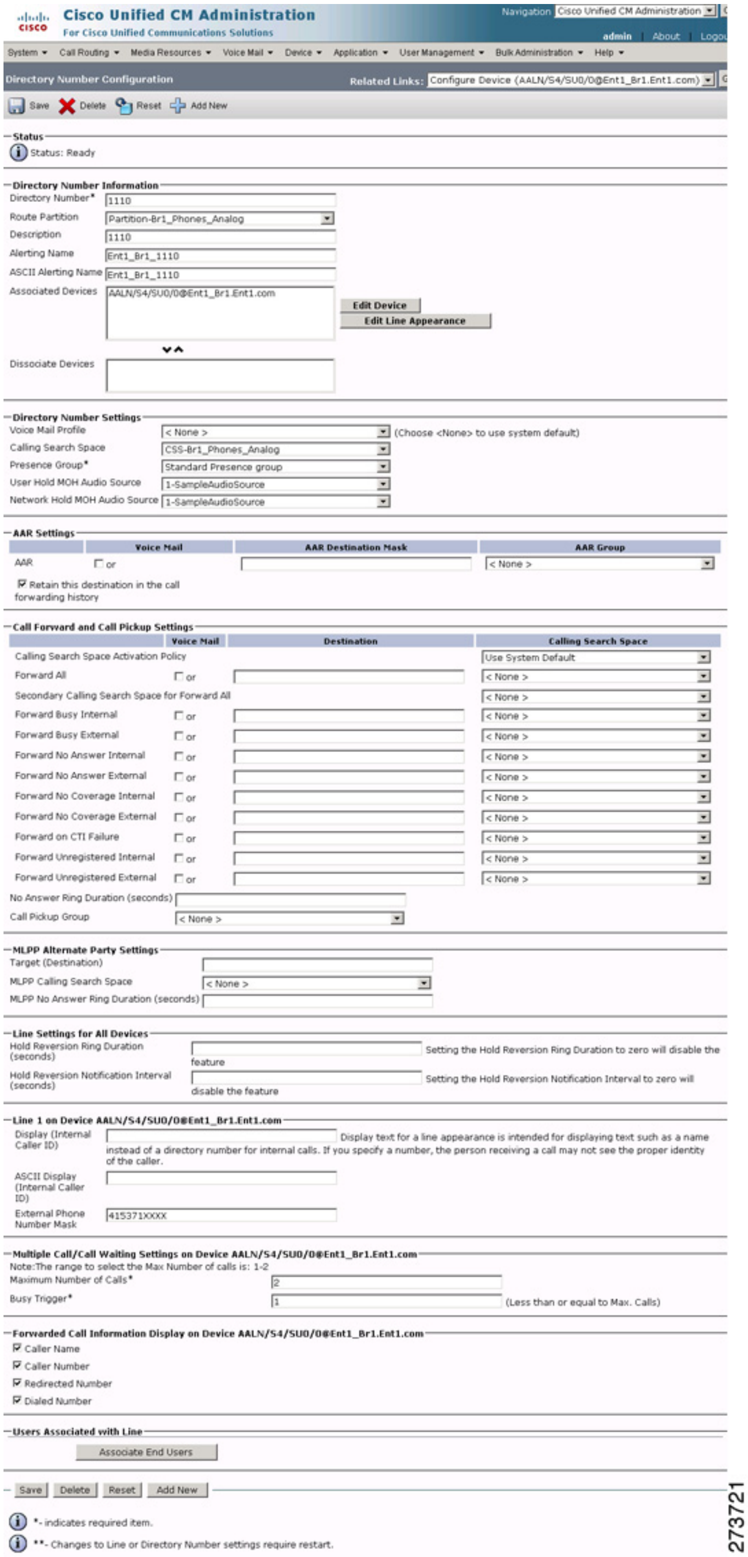


Figure 82 Device Gateway Enterprise 1 HQ VG224 Cisco Unified CM Administration Window

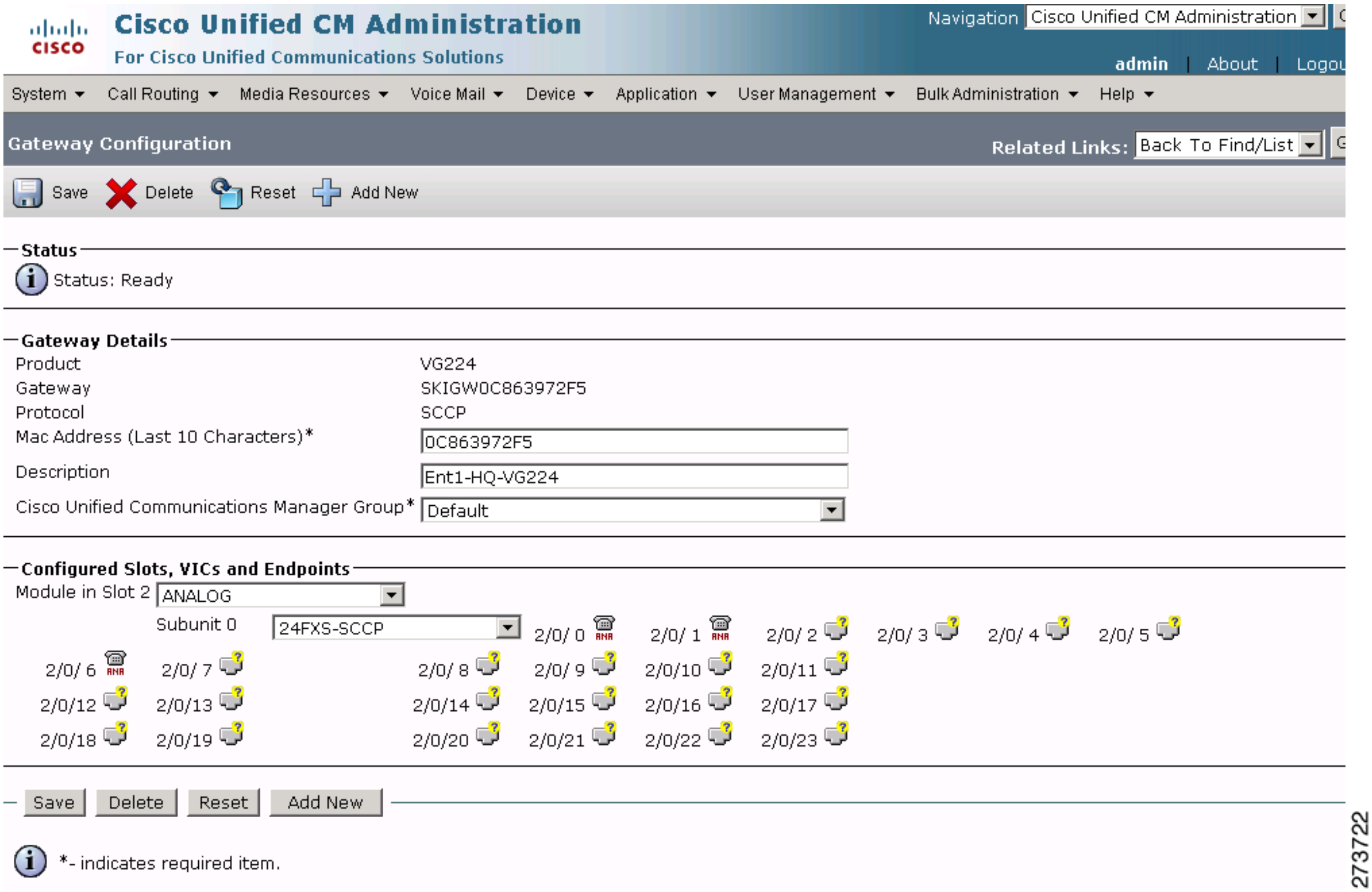


Figure 83 Device Gateway Enterprise 1 HQ VG224 ANA 1050 Cisco Unified CM Administration Window

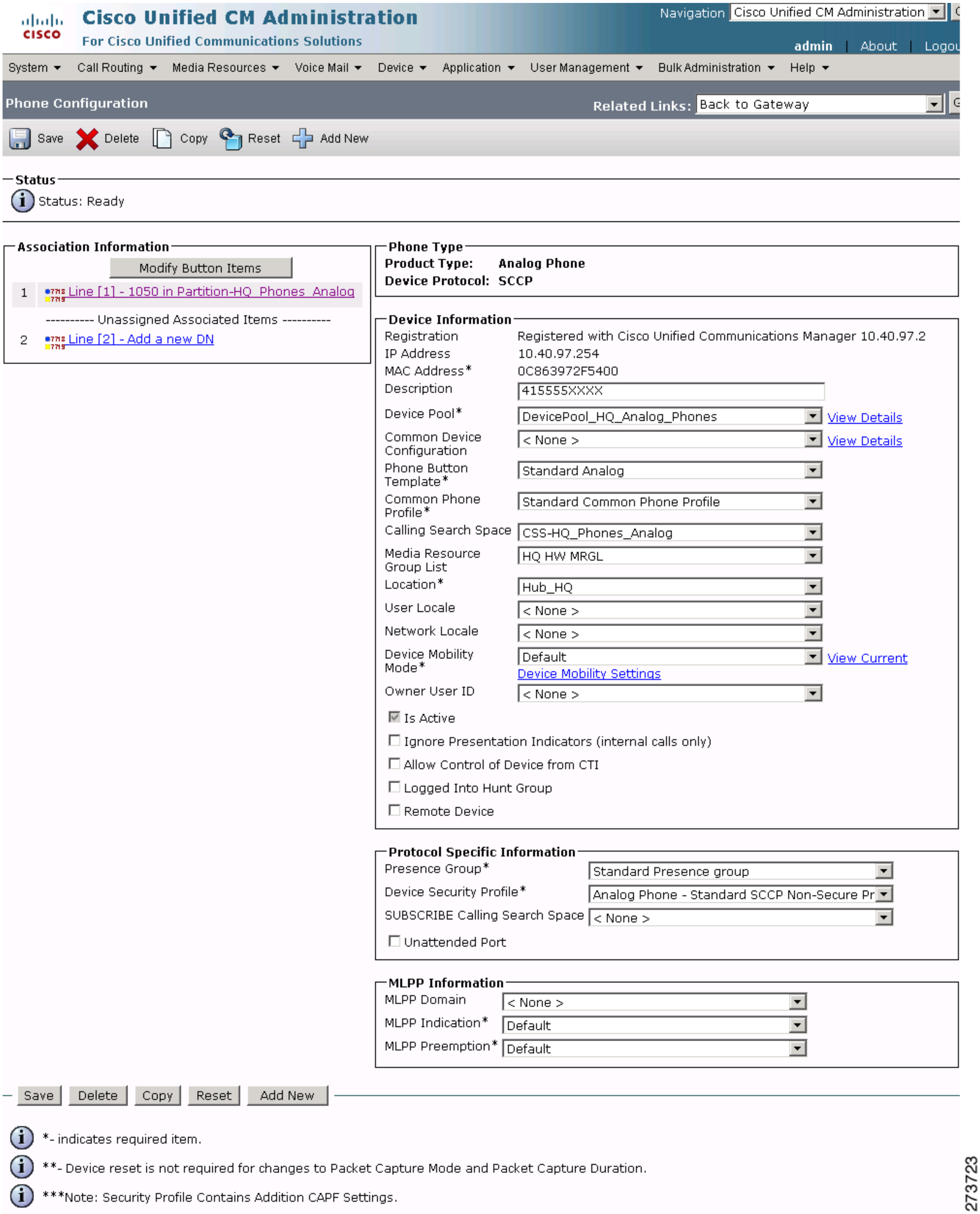
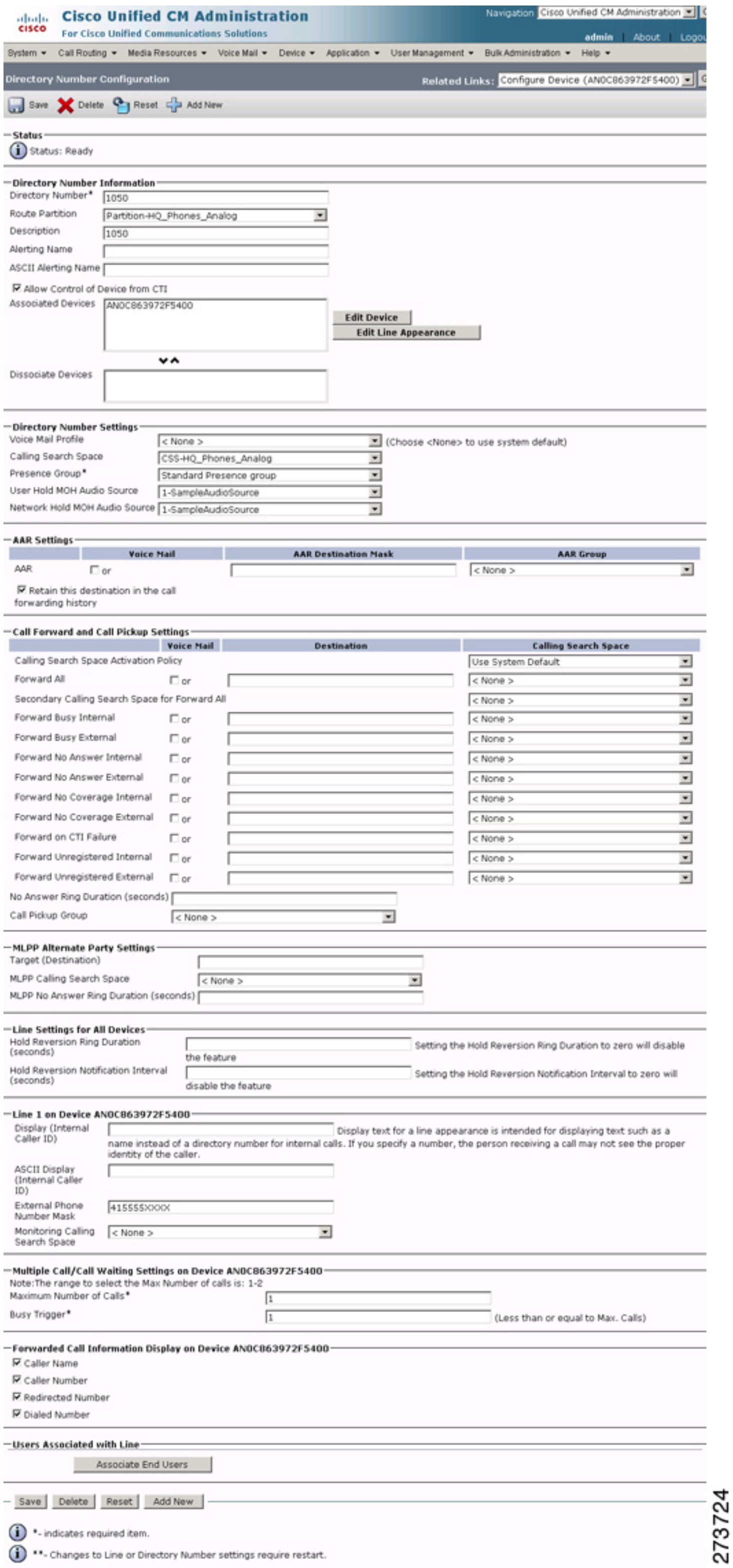


Figure 84 Device-Gateway Enterprise 1 HQ VG224 ANA 1050 Line Cisco Unified CM Administration Window



Device: Phone Parameters

To configure the device phone parameters for the Cisco Unified CM, click **Device** > **Phone** menu in the Cisco Unified CM Administration window.

Figure 85 Device Phone 4155551000 Cisco Unified CM Administration Window

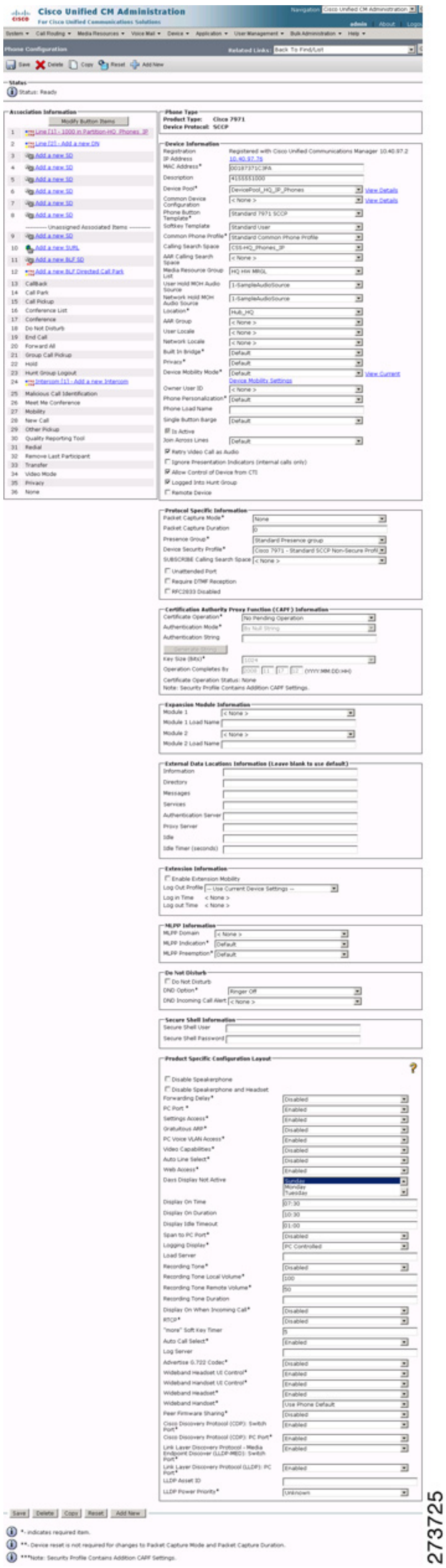
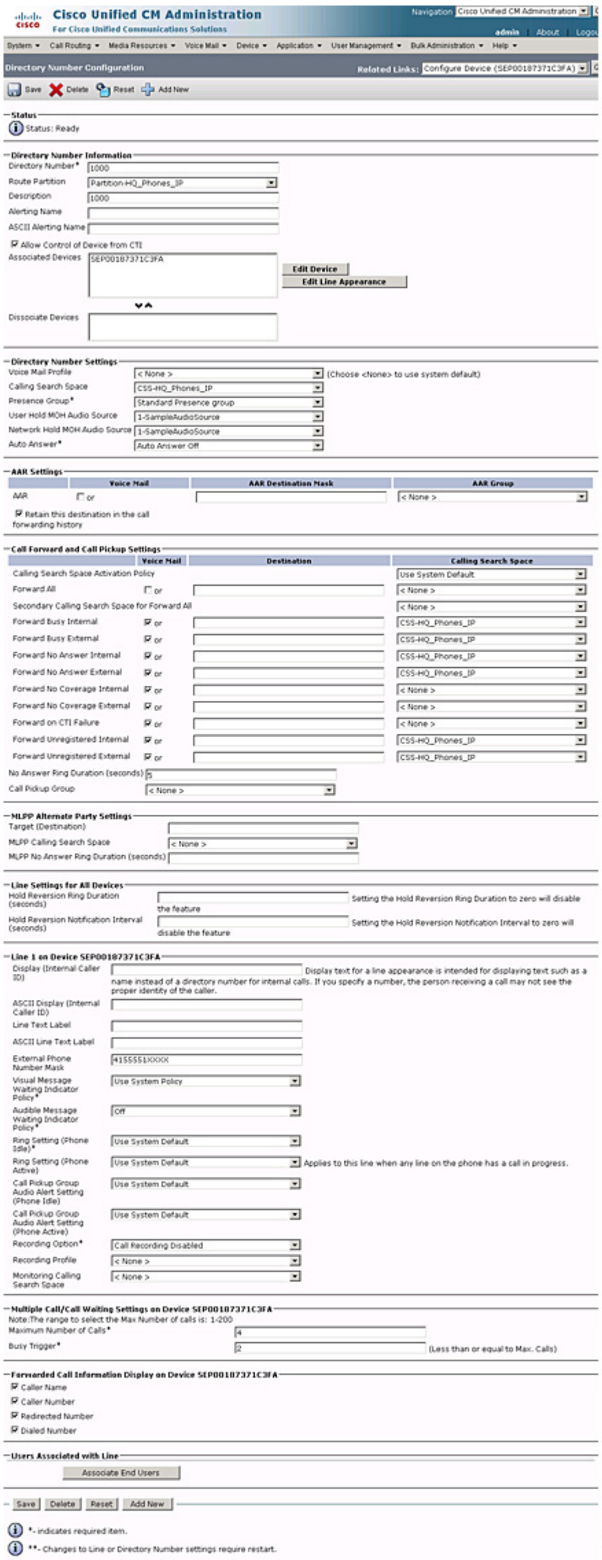


Figure 86 Device Phone 1000 Cisco Unified CM Administration Window



273726

Figure 87 Device Phone 4155551170 Cisco Unified CM Administration Window

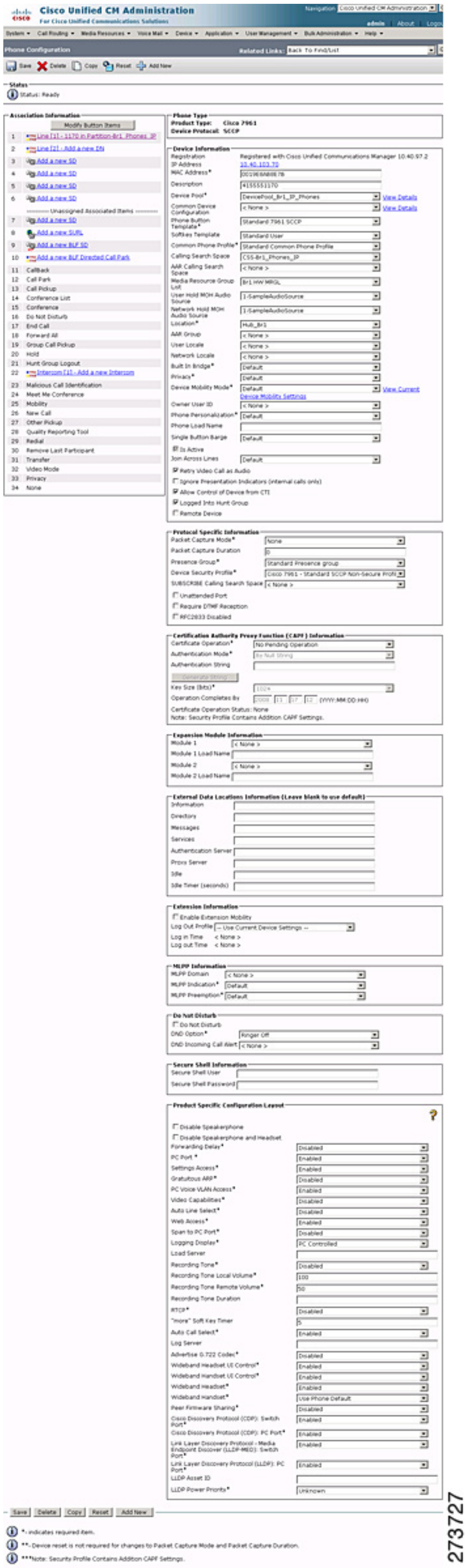
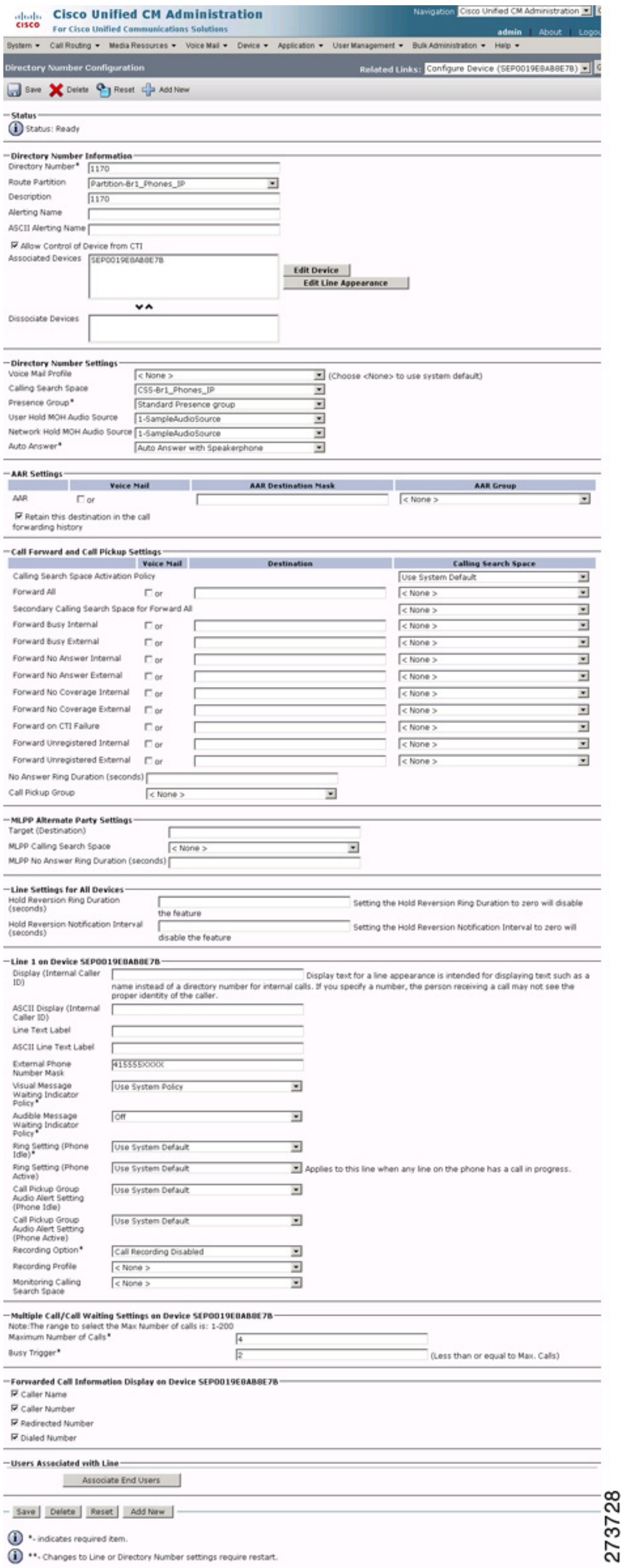


Figure 88 Device Phone 1170 Cisco Unified CM Administration Window



Device: Trunk Parameters

To configure the device trunk parameters for the Cisco Unified CM, click **Device** > **Trunk** menu in the Cisco Unified CM Administration window.

Figure 89 Device Trunk Cisco Unified CM Administration Window

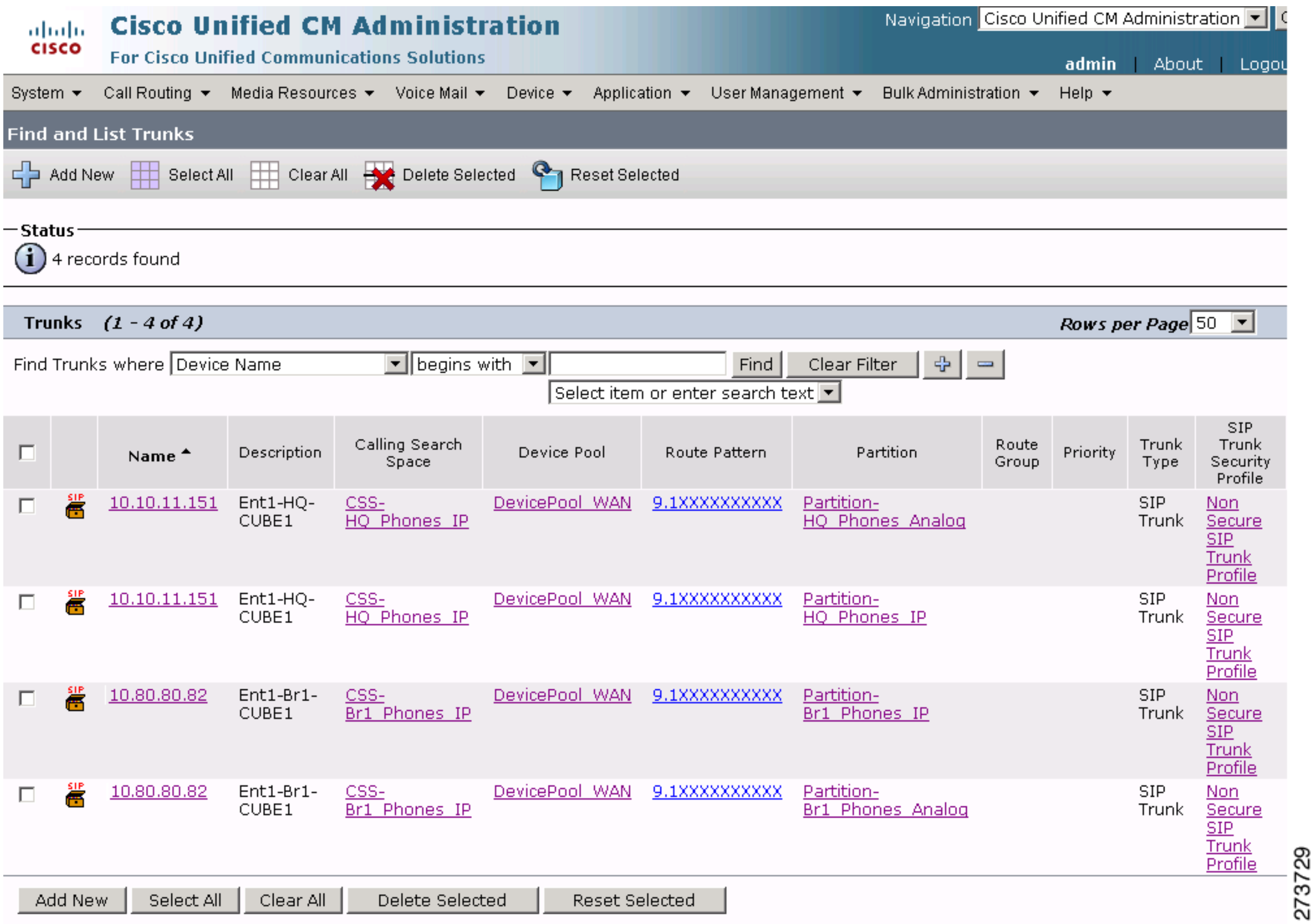


Figure 90 Device Trunk Enterprise 1 HQ CUBE1 Phones Analog Cisco Unified CM Administration Window

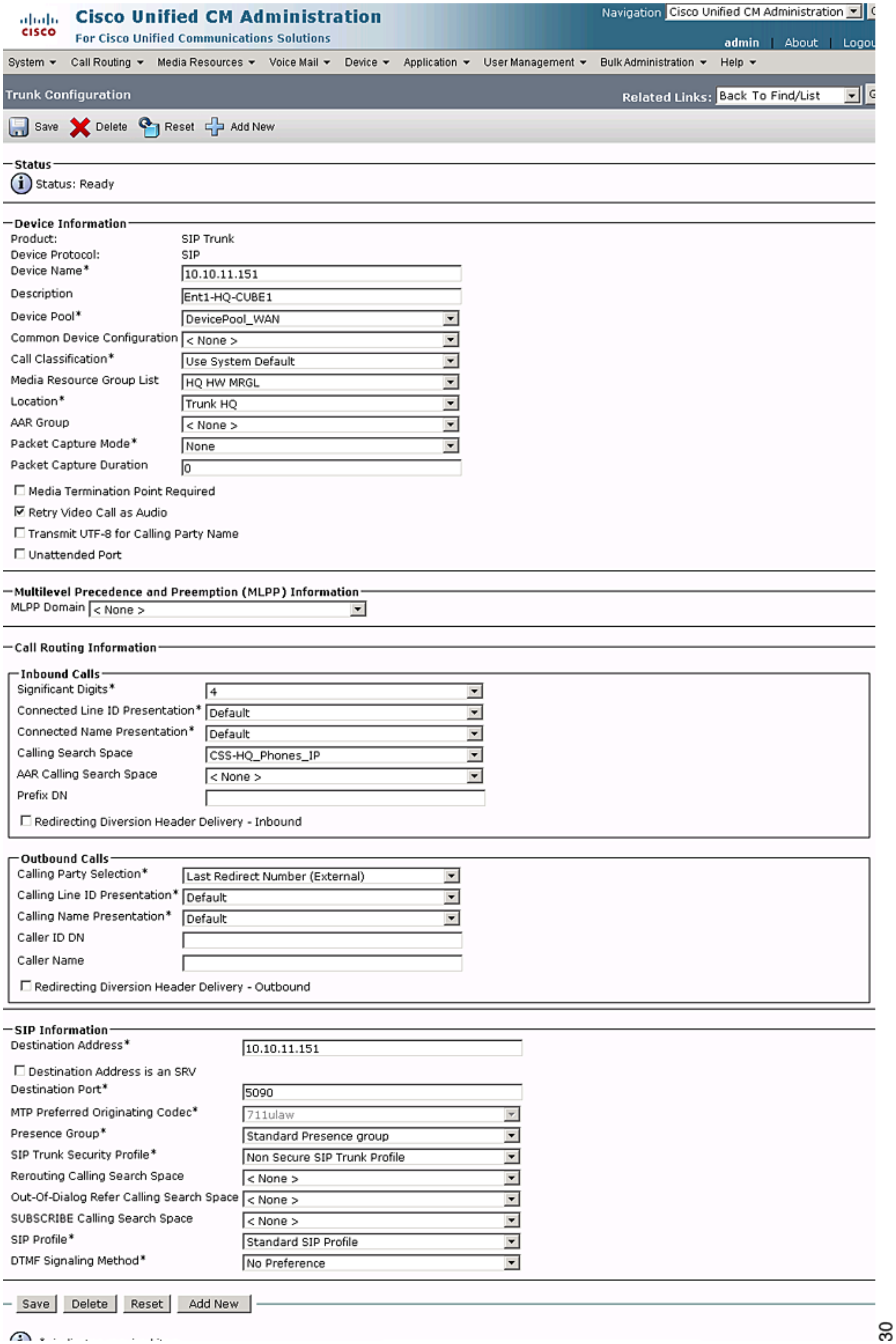
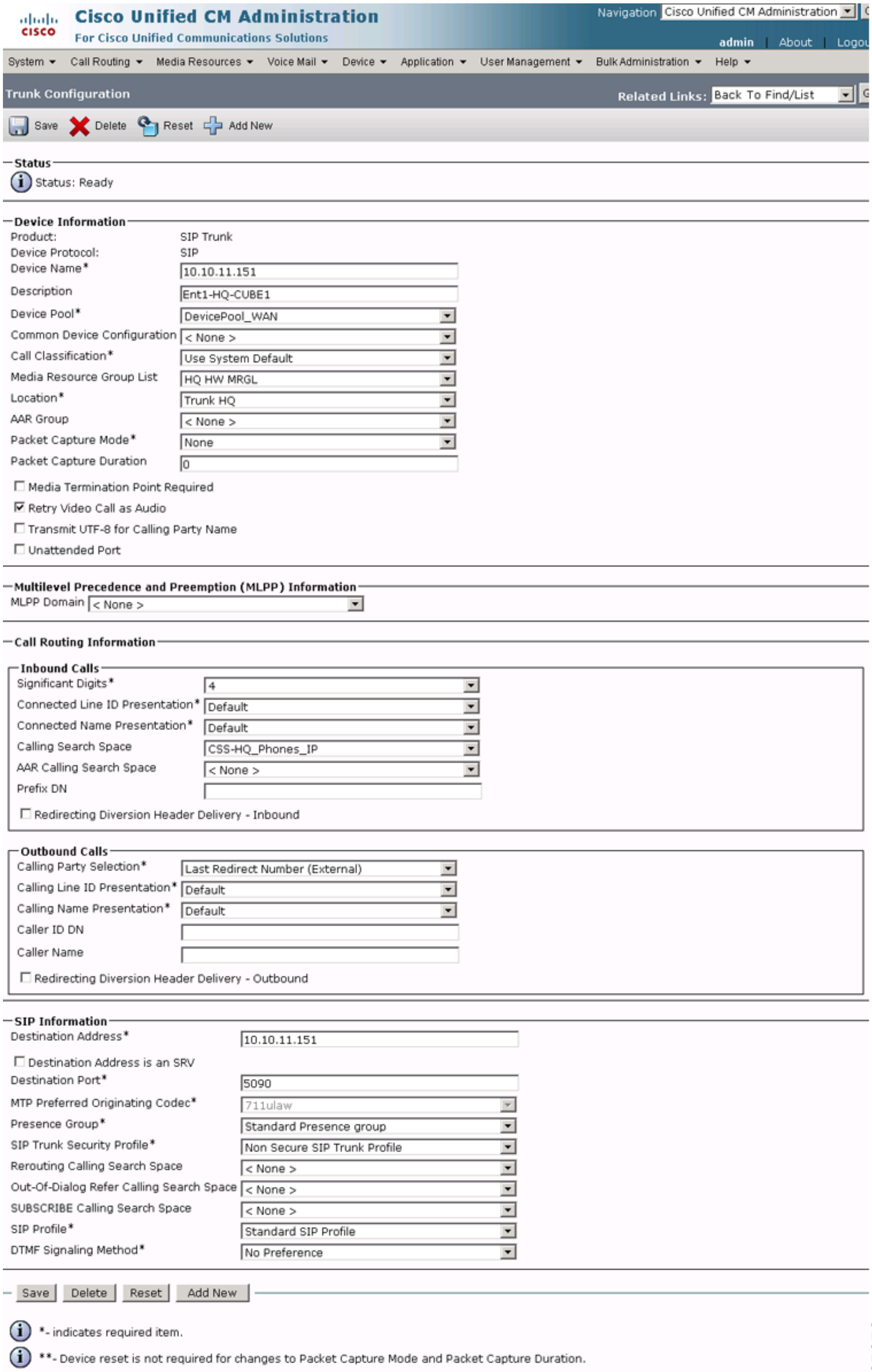


Figure 91 Device Trunk Enterprise 1 HQ CUBE1 Phones IP Cisco Unified CM Administration Window



273731

Figure 92 Device Trunk Enterprise 1 Branch 1 CUBE1 Phones Analog Cisco Unified CM Administration Window

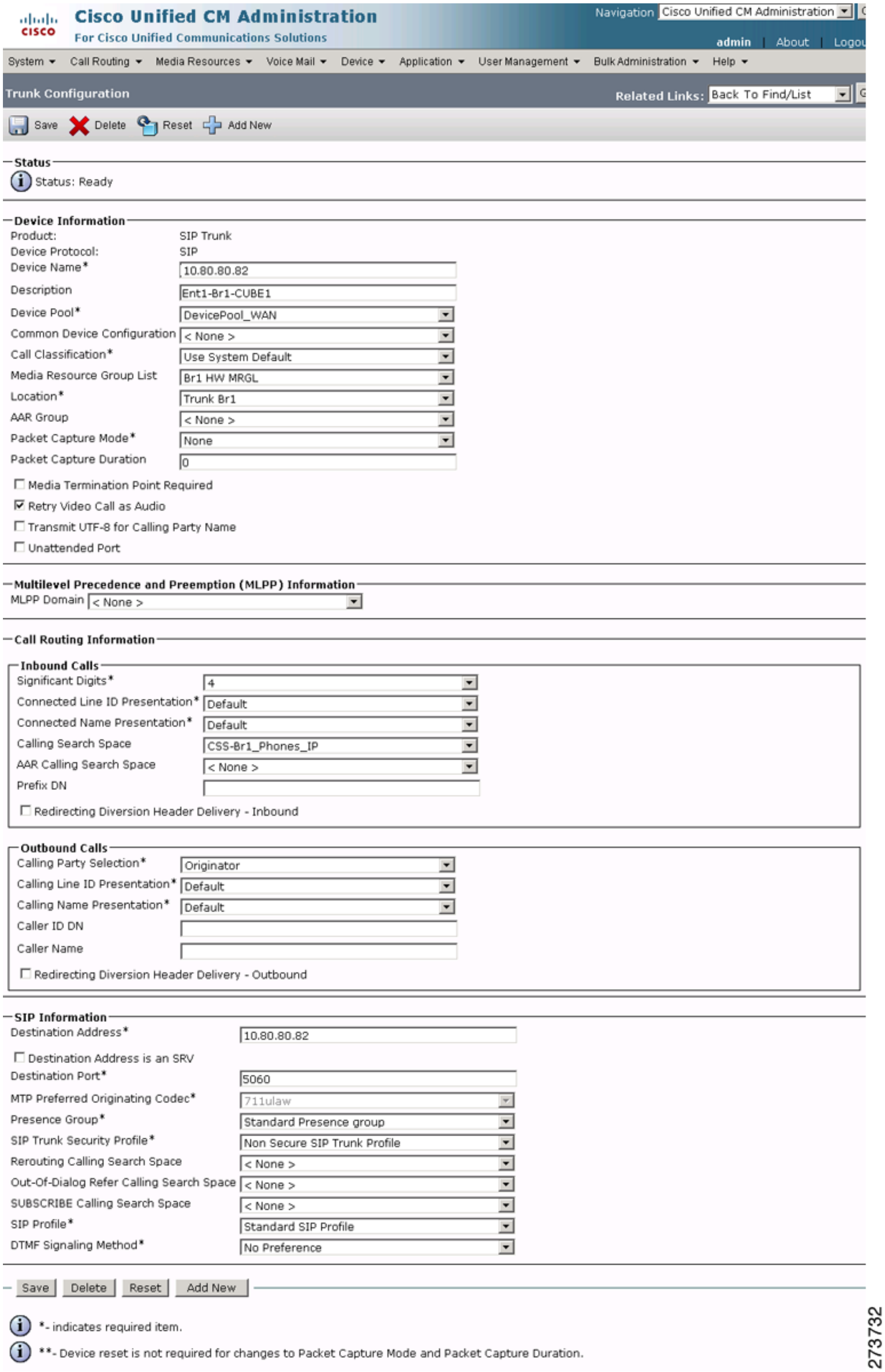
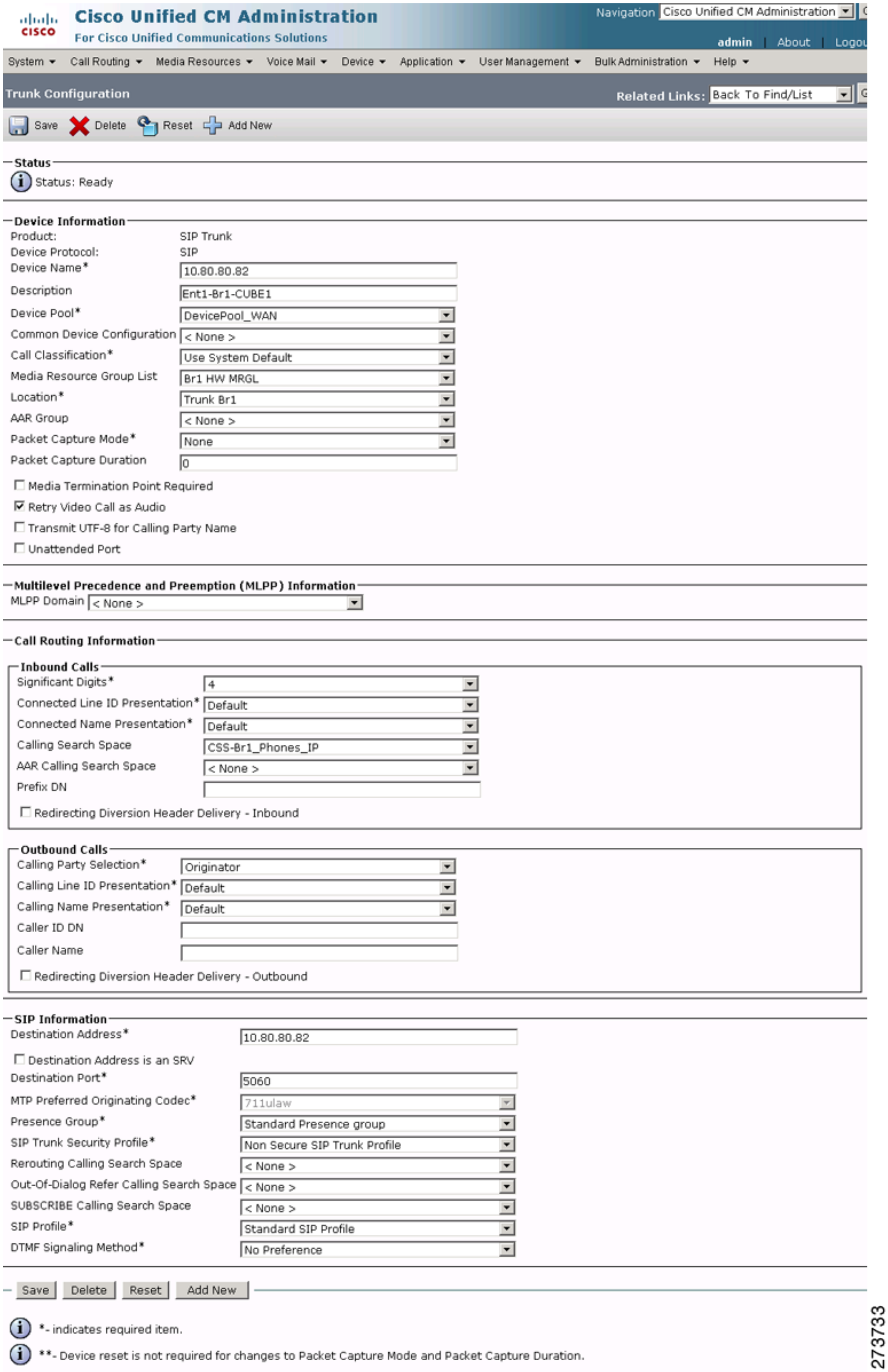


Figure 93 Device Trunk Enterprise 1 Branch 1 CUBE1 Phones IP Cisco Unified CM Administration Window



Enterprise 1 HQ Cisco Unity and Cisco Unity Express Example Configuration

To integrate the Cisco Unity version 5.0 with Cisco Unified CM configuration, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Release 5.0.*

Enterprise 1 HQ and Cisco VG224 Analog Phone Gateway Example Configuration

The following is a command-line interface (CLI) configuration example for the enterprise 1 HQ the Cisco VG224 Analog Phone Gateway for the test topology described in Figure 8.

```
Ent1_HQ_VG224#
!
stcapp ccm-group 1
stcapp
!
voice service voip
 fax protocol pass-through g711ulaw
 modem passthrough nse codec g711ulaw
!
interface FastEthernet0/0
 ip address 10.40.97.254 255.255.0.0
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
voice-port 2/0
 timeouts ringing infinity
 caller-id enable
!
voice-port 2/1
 timeouts ringing infinity
 caller-id enable
!
sccp local FastEthernet0/0
sccp ccm 10.40.97.2 identifier 10
sccp
!
sccp ccm group 1
 associate ccm 10 priority 1
!
dial-peer voice 1 pots
 service stcapp
 port 2/0
!
dial-peer voice 2 pots
 service stcapp
```

```
 port 2/1
!
Ent1_HQ_VG224#
```

Enterprise 1 HQ Cisco ASA Firewall Example Configuration

The following is a command-line interface (CLI) configuration example for the enterprise 1 HQ the Cisco ASA 8.0(4) 5500 Series Adaptive Security Appliances firewall for the test topology described in Figure 8.

```
Ent1-HQ-ASA#
!
interface Vlan65
 nameif inside
 security-level 100
 ip address 10.40.99.1 255.255.255.0
!
interface Vlan70
 nameif outside
 security-level 0
 ip address 10.40.98.2 255.255.255.0
!
interface Ethernet0/0
 description *** To WAN ***
 switchport access vlan 70
!
interface Ethernet0/1
 description *** To LAN ***
 switchport access vlan 65
!
ftp mode passive
access-list 100 extended permit icmp any any
access-list 100 extended permit icmp any any echo
access-list 100 extended permit icmp any any echo-reply
access-list 100 extended permit tcp any host 40.40.97.2 eq 2000
access-list 100 extended permit udp any host 40.40.97.2 eq sip
access-list 100 extended permit tcp any host 40.40.97.2 range h323 h323
access-list 100 extended permit tcp any host 10.10.11.151 eq 5090
access-list 100 extended permit udp any host 10.10.11.151 eq 5090
access-list 100 extended permit tcp any host 40.40.97.2 eq 2428
access-list 100 extended permit udp any host 40.40.97.2 eq 2427
pager lines 24
logging enable
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-524.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
http server enable
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map sipoutin
 match port udp eq 5090
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
policy-map outsidein
 class sipoutin
  inspect sip
 class inspection_default
  inspect skinny
!
service-policy global_policy interface inside
service-policy outsidein interface outside
prompt hostname context
Cryptochecksum:xxxxxxxxxxxxxxxxxxxxxxxxxxx
: end
Ent1-HQ-ASA#
```

Branch 1 Cisco UBE, TDM Gateway, and Cisco Unified SRST Example Configuration

The following is a command-line interface (CLI) configuration example for the branch 1 Cisco Unified Border Element, TDM Switching in the Cisco AS5000 Gateway, and Cisco Unified SRST for the test topology described in Figure 8.

```
Ent1_Br1#

!
 voice-card 4
 dspfarm
 dsp services dspfarm
!
voice service voip
 address-hiding
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 supplementary-service media-renegotiate
```

```
 fax protocol pass-through g711ulaw
 modem passthrough nse codec g711ulaw
 sip
  min-se  90
  header-passing error-passthru
  midcall-signaling passthru
!
voice translation-rule 1
 rule 1 /^61/ /1/
 rule 2 /^71/ /1/
!
 voice translation-profile OUTGOING-SIP-TRK-DIGIT-STRIP
 translate called 1
!
interface Loopback0
 ip address 10.10.11.154 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shut
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description *** To Local LAN ***
 no ip address
 ip virtual-reassembly
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.1
 encapsulation dot1Q 103
 ip address 10.40.103.1 255.255.255.0
 ip helper-address 10.40.97.2
 ip virtual-reassembly
!
interface Serial4/0:0
 description *** To WAN ***
 ip address 10.80.80.82 255.255.255.252
 ip virtual-reassembly
 encapsulation frame-relay
 load-interval 30
 cdp enable
 frame-relay map ip 10.80.80.81 202
 frame-relay interface-dlci 202
 no frame-relay inverse-arp NOVELL 202
 no frame-relay inverse-arp APPLETALK 202
 no frame-relay inverse-arp DECNET 202
 frame-relay lmi-type ansi
 frame-relay local-dlci 202
!
interface Serial4/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn incoming-voice voice
 no cdp enable
!
call treatment on
call threshold global cpu-avg low 68 high 75
call threshold global total-mem low 75 high 85
```

```
call threshold global total-calls low 1 high 12
!
!
voice-port 2/1/0
!
voice-port 2/1/1
!
voice-port 4/0/0
!
voice-port 4/0/1
!
voice-port 4/0:23
!
ccm-manager mgcp
!
mgcp
mgcp call-agent 10.40.97.2 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp sdp simple
mgcp fax t38 inhibit
mgcp bind control source-interface GigabitEthernet0/1.1
mgcp bind media source-interface GigabitEthernet0/1.1
!
mgcp profile default
!
sccp local GigabitEthernet0/1.1
sccp ccm 10.40.97.2 identifier 1 priority 1 version 6.0
sccp ip precedence 3
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/1.1
 associate ccm 1 priority 1
 associate profile 3 register XCD001AA29DF631
 associate profile 2 register CON001AA29DF631
 associate profile 1 register MTP001AA29DF631
 keepalive retries 1
 keepalive timeout 10
 switchover method immediate
 switchback method immediate
!
dspfarm profile 3 transcode
 description transcode bridge
 codec g711ulaw
 codec g729r8
 maximum sessions 5
 associate application SCCP
!
dspfarm profile 2 conference
 description conference bridge
 codec g711ulaw
 codec g729r8
 maximum sessions 4
 associate application SCCP
!
dspfarm profile 1 mtp
 codec g729r8
 maximum sessions software 5
 associate application SCCP
!
!
dial-peer voice 2000 voip
 description *** Voice: LAN to WAN - Incoming Dial-Peer ***
 huntstop
```

```
 codec g729r8
 session protocol sipv2
 incoming called-number 6T
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2001 voip
 description *** Voice: LAN to WAN - Outgoing Dial-Peer ***
 translation-profile outgoing OUTGOING-SIP-TRK-DIGIT-STRIP
 huntstop
 destination-pattern 6T
 codec g729r8
 voice-class sip early-offer forced
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.3.33.22
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2100 voip
 description *** Voice: WAN to LAN - Incoming Dial-Peer ***
 huntstop
 codec g729r8
 session protocol sipv2
 incoming called-number 415T
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 2101 voip
 description *** Voice: WAN to LAN - Outgoing Dial-Peer ***
 huntstop
 destination-pattern 415T
 codec g729r8
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.40.97.2
 dtmf-relay rtp-nte digit-drop
 no vad
!
dial-peer voice 3000 voip
 description *** Fax: LAN to WAN - Incoming Dial-Peer ***
 huntstop
 session protocol sipv2
 incoming called-number 7T
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3001 voip
 description *** Fax: LAN to WAN - Outgoing Dial-Peer ***
 translation-profile outgoing OUTGOING-SIP-TRK-DIGIT-STRIP
 huntstop
 destination-pattern 7T
 voice-class sip early-offer forced
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.3.33.22
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3100 voip
 description *** Fax: WAN to LAN - Incoming Dial-Peer ***
 huntstop
```

```
 session protocol sipv2
 incoming called-number 415555111[0,1]
 dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 3101 voip
 description *** Fax: WAN to LAN - Outgoing Dial-Peer ***
 huntstop
 destination-pattern 415555111[0,1]
 max-redirects 5
 session protocol sipv2
 session target ipv4:10.40.97.2
dtmf-relay rtp-nte digit-drop
 codec g711ulaw
 no vad
!
dial-peer voice 1 pots
 service mgcpapp
 port 4/0/0
!
dial-peer voice 2 pots
 service mgcpapp
 port 4/0/1
!
dial-peer hunt 3
sip-ua
 authentication username yyyyy password 7 xxxxxxxxxx
 no remote-party-id
 retry invite 2
 retry response 5
 retry bye 2
 retry cancel 2
 retry register 10
 retry options 1
 g729-annexb override
!
call-manager-fallback
 video
 max-conferences 10 gain -6
 transfer-system full-consult
 log table max-size 1000
 ip source-address 10.40.103.1 port 2000
 max-ephones 50
 max-dn 50
 system message primary Ent1_Br1
 dialplan-pattern 1 415555.... extension-length 4
 transfer-pattern .T
!
Ent1_Br1#
```

Branch 1 Cisco Unity Express 3.2 and Cisco Unified CM Example Configuration

To integrate the Branch 1 Cisco Unity Express with Cisco Unified CM configuration, see the *CallManager for Cisco Unity Express Configuration Example.*