Cisco Systems

REVIEW DRAFT—CISCO CONFIDENTIAL

Cisco Unified Application Environment Administration Guide

Release 2.3

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-xxxx-xx

Cisco Unified Application Environment Administration Guide

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain additional information.

Overview

This document explains how to administer and maintain the Cisco Unified Application Environment using the Cisco Unified Application Environment management console.

Audience

This guide is intended for system administrators who are familiar with the Windows operating system. The reader should have a basic understanding of IP telephony, full knowledge of Cisco Unified CallManager, and familiarity with the reader's own IP telephone environment.

Organization

This guide is organized as follows:

Chapter 1, "An Overview of the Cisco Unified Application Environment"	Introduces the Cisco Unified Application Environment and describes example deployment topologies.
Chapter 2, "Getting Started"	Describes how to set up the Cisco Unified Application Environment by accessing the management console, performing basic configuration tasks, and installing applications.
Chapter 3, "Configuring the Cisco Unified Application Server"	Describes how to use the management console to configure and manage application servers.
Chapter 4, "Configuring the Cisco Unified Media Engine"	Describes how to use the management console to configure and manage media engines.
Chapter 5, "Maintaining the Cisco Unified Application Environment"	Describes how to view log files, use log files for troubleshooting, and back up and restore the Cisco Unified Application Server software.

Related Documentation

Documentation on Cisco Unified Communications products is located at this URL:
http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Document Conventions

This publication uses these conventions to convey instructions and information:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Convention	Description
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **The warning symbol means danger.** You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

CHAPTER 1

An Overview of the Cisco Unified Application Environment

The Cisco Unified Application Environment is a development and runtime platform designed for creating, deploying, and executing converged voice and data applications.

This chapter introduces the Cisco Unified Application Environment and includes these sections:

Understanding the Cisco Unified Application Environment

You can use the Cisco Unified Application Environment to create applications supporting these IP telephony functions:

- Mobility
- Recording
- Paging
- Conferencing
- Speech-Enabled applications
- IP Phone Services
- Other voice and data converged applications

The Cisco Unified Application Environment is comprised of the:

- Cisco Unified Application Server—Runs on the Cisco MCS-7845-H1 server and is pre-loaded for shipment
- Cisco Unified Media Engine—Runs on the Cisco MCS-7845-H1 server and is pre-loaded for shipment
- Cisco Unified Application Designer—PC-based client application

The Cisco Unified Application Environment is integrated with Cisco Unified CallManager and supports these application development and deployment technologies:

- Telephony call control protocols: Session Initiation Protocol (SIP), H.323, Skinny Call Control Protocol (SCCP) and Java Telephony Application Programming Interface (JTAPI)

- Other telephony protocols: Cisco Unified IP Phone Services, DeviceListX, AXL-SOAP, Extension Mobility and other Cisco Unified CallManager APIs
- Data services and protocols: Web Services, HTTP, Lightweight Directory Access Protocol (LDAP), Structured Query Language (SQL), Simple Mail Transfer Protocol (SMTP)
- Media processing capabilities: Integrated voice response (IVR), conferencing, transcoding, text-to-speech, speech recognition, speaker verification
- Extensible plug-in framework that customers and partners can use to add support for any standards-based or proprietary protocol or interface

The major components of the Cisco Unified Application Environment are described in these sections:

- Cisco Unified Application Server
- Cisco Unified Media Engine
- Cisco Unified Application Designer

All these are administered by the Cisco Unified Application Environment Management Console

Cisco Unified Application Server

The Cisco Unified Application Server provides the following functions:

- Originates and receives calls over various IP telephony protocols.
- **Ensures the reliability of Cisco Unified CallManager from applications, and provides standard application management.**
- Starts, executes, manages, and terminates application scripts that are operating in their own runtime environment on their own virtual machines.
- Hosts protocol providers that provide an interface to applications for systems outside the application environment.
- Controls one or more Cisco Unified Media Engines to process, mix, analyze, and route digital audio data.

Note Each Cisco Unified Application Environment deployment must contain at least one Cisco Unified Application Server with at least one application installed on the server.

You can configure the Cisco Unified Application Server to host any applications created by the Cisco Unified Application Designer (see the "Cisco Unified Application Designer" section on page 1-3). An application typically includes configuration items that are unique to your deployment and which you must configure after the application is installed.

Cisco Unified Media Engine

The Cisco Unified Media Engine is a software-only media server, which provides media processing capabilities for applications that are built using the Cisco Unified Application Designer.

Note Each Cisco Unified Media Engine is controlled by one or more Cisco Unified Application Servers.

The Cisco Unified Application Environment is designed is designed to allow you to:

- Perform flexible deployment of application servers and media engines, by determining the appropriate number and configuration of servers at the time of deployment.
- Avoid latency and bandwidth issues, by allowing you to distribute media engines closer to the media endpoints used for a particular application, as media engines may generate considerable Real-time Transport Protocol (RTP) traffic.

Note If the application does not have any media components, a Cisco Unified Media Engine is not required.

Cisco Unified Application Designer

The Cisco Unified Application Designer is a visual integrated development environment (IDE). The Cisco Unified Application Designer allows application designers to:

- Develop applications that combine voice and video with enterprise applications and data.
- Install applications directly from PC or build an application package file
- Load installed applications from the Cisco Unified Application Environment management console.

For information on the Cisco Unified Application Designer, go to http://www.cisco.com/en/US/products/ps7056/index.html.

Cisco Unified Application Environment Management Console

The Cisco Unified Application Environment management console is a web-based interface that you must use to administer the Cisco Unified Application Server and Cisco Unified Media Engine.

The Main Control Panel is divided into sections that correspond to the specific management functions that are required to set up the Cisco Unified Application Environment:

- Environment—Configuring Environment Parameters
- System—Configuring System Parameters
- Components—Configuring Components
- Logs—Viewing Log Information

See these chapters for more information about how to configure and maintaining the Cisco Unified Application Environment:

- Chapter 2, “Getting Started”
- Chapter 3, “Configuring the Cisco Unified Application Server”
- Chapter 4, “Configuring the Cisco Unified Media Engine”
- Chapter 5, “Maintaining the Cisco Unified Application Environment”

Understanding the Deployment of the Cisco Unified Application Environment

The Cisco Unified Application Environment supports a variety of deployment topologies incorporating varying numbers of Cisco Unified Application Servers and Cisco Unified Media Engines and integrating with one or more Cisco Unified CallManager clusters.

The choice of deployment topology should be based on requirements for scalability, redundancy, and networking. This section describes these common topologies:

- Single Application Server with a Single Cisco Unified CallManager Cluster
- Single Application Server with Multiple Cisco Unified CallManager Clusters
- A Single Application Server Controlling Multiple Media Engines with Multiple Cisco Unified CallManager Clusters
- Multiple Application Servers Controlling Multiple Media Engines with Multiple Cisco Unified CallManager Clusters

Single Application Server with a Single Cisco Unified CallManager Cluster

In this topology, a single physical server operates as an application server or combined application server and media engine and is integrated with a single Cisco Unified CallManager cluster. This configuration is appropriate when these conditions apply:

- The Cisco Unified Application Environment must support a single Cisco Unified CallManager cluster.
- Fewer than 240[1] simultaneous media streams are required. and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, music on hold (MOH) servers, and hardware and software conference bridges) and the media engine is not expected to add excessive network load.

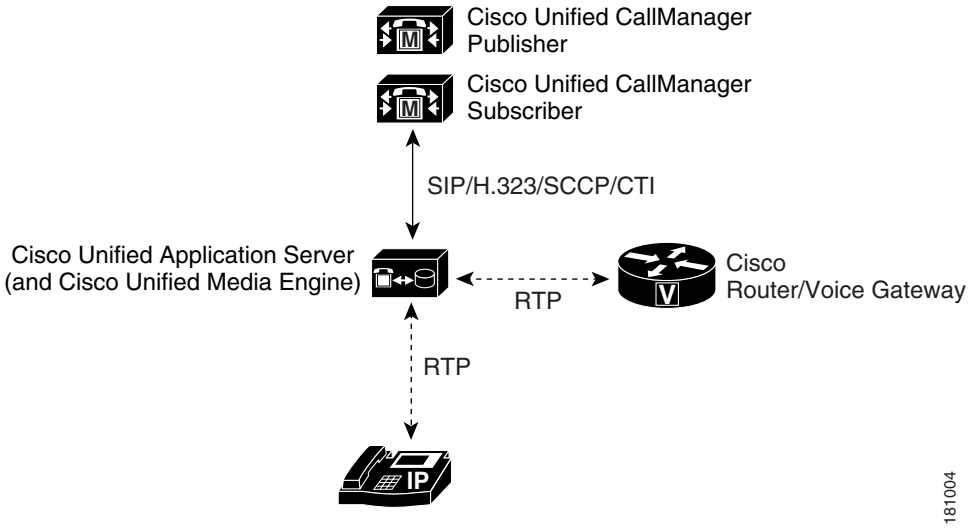
  Note Network traffic concerns are an issue only for applications that require media.

- Redundancy is not required for the application server or media engine.

Figure 1-1 shows the IP telephony integration for this topology.

1. The maximum of 240 media streams is an approximation. If multiple applications involve heavy conferencing, recording and playing, low bit-rate codecs, or CPU-intensive activity, fewer simultaneous media streams will be supported.

Figure 1-1 Single Application Server, Single Cisco Unified CallManager Cluster



Single Application Server with Multiple Cisco Unified CallManager Clusters

In this topology, a single physical server operates as an application server or combined application server and media engine and is integrated with multiple Cisco Unified CallManager clusters. This configuration is appropriate when these conditions apply:

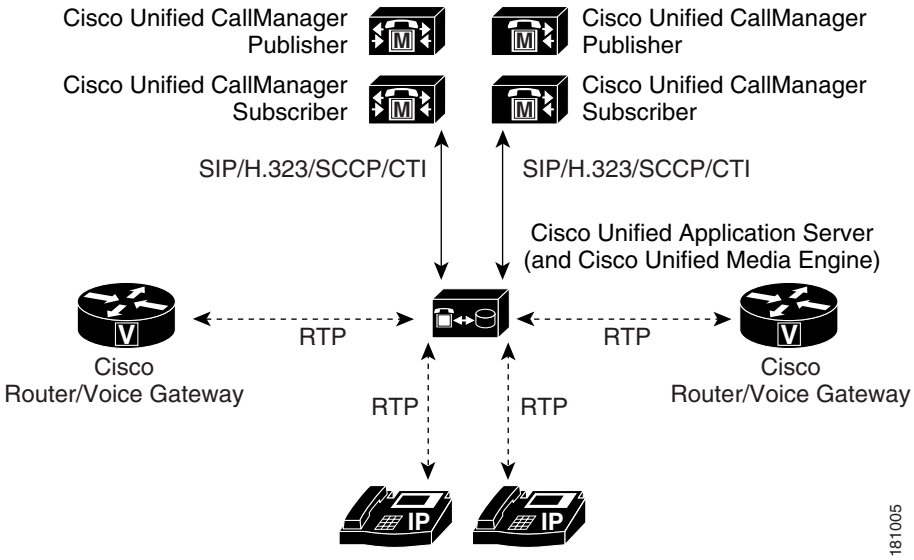
- The Cisco Unified Application Environment must support multiple Cisco Unified CallManager clusters.
- Fewer than 240 simultaneous media streams are required. and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, music on hold (MOH) servers, and hardware and software conference bridges) and the media engine is not expected to add excessive network load.

Note Network traffic concerns are an issue only for applications that require media.

- Redundancy is not required for the application server or media engine.

Figure 1-2 shows the IP telephony integration for this topology.

Figure 1-2 Single Application Server, Multiple Cisco Unified CallManager Clusters



A Single Application Server Controlling Multiple Media Engines with Multiple Cisco Unified CallManager Clusters

In this topology, a single application server controls multiple media engines and is integrated with multiple Cisco Unified CallManager clusters.

Note To avoid latency and bandwidth issues, it is recommended that you distribute media engines closer to the media endpoints used for a particular application.

This configuration is appropriate when these conditions apply:

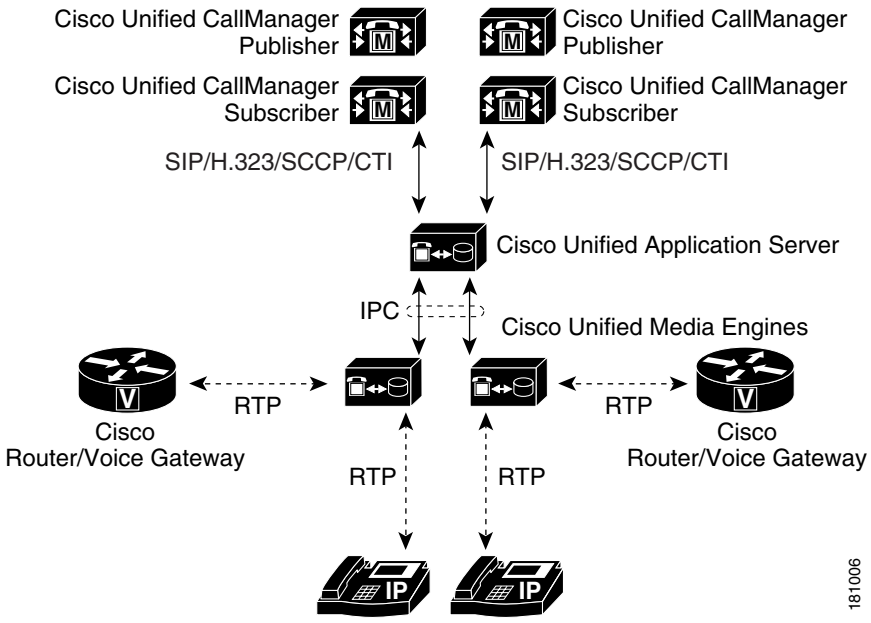
- The Cisco Unified Application Environment must support multiple Cisco Unified CallManager clusters.
- Fewer than 240 simultaneous media streams are required. and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, music on hold (MOH) servers, and hardware and software conference bridges) and the media engine is not expected to add excessive network load.

  Note Network traffic concerns are an issue only for applications that require media.

- Redundancy is not required for the application server.
- Redundancy is required for the media engine.

Figure 1-3 shows the IP telephony integration for this topology.

Figure 1-3 Single Application Server, Multiple Media Engines, Multiple Cisco Unified CallManager Clusters



Multiple Application Servers Controlling Multiple Media Engines with Multiple Cisco Unified CallManager Clusters

In this topology, multiple application servers control multiple media engines and are integrated with multiple Cisco Unified CallManager clusters. This configuration is appropriate when these conditions apply:

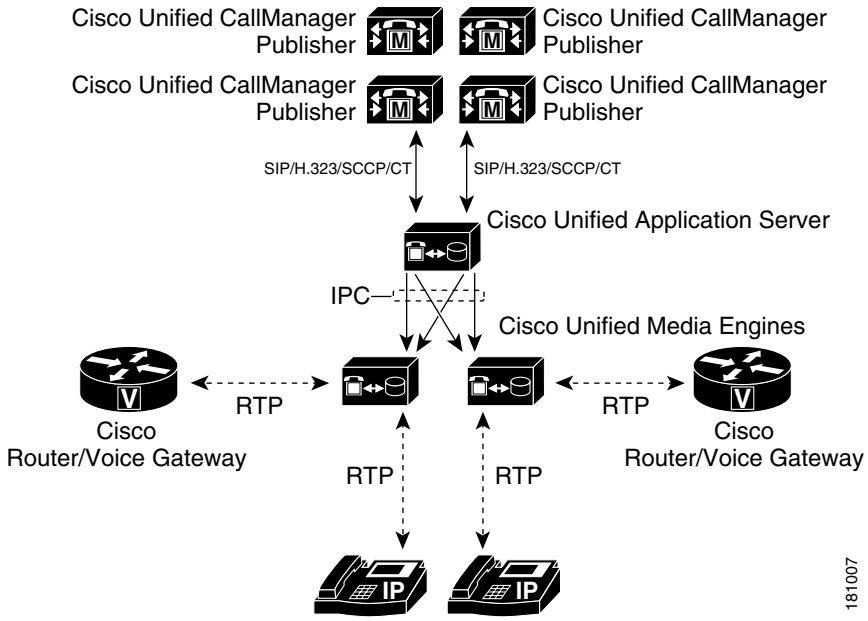
- The Cisco Unified Application Environment must support multiple Cisco Unified CallManager clusters.
- More than 240 simultaneous media streams are required, or the projected amount of media stream traffic between IP endpoints is expected to add significant network load.

Note Network traffic concerns are an issue only for applications that require media.

- Redundancy is required for the application server and media engine.

Figure 1-4 shows the IP telephony integration for this topology.

Figure 1-4 Multiple Application Servers, Multiple Media Engines, Multiple Cisco Unified CallManager Clusters



CHAPTER 2

Getting Started

This chapter describes how to set up the Cisco Unified Application Environment by accessing the management console, performing basic configuration tasks, and installing applications. It also provides an example deployment scenario that describes how to configure an example environment.

This chapter includes these topics:

Before You Begin

Before you begin setting up the Cisco Unified Application Environment, you must do the following:

1. Install the Cisco MCS-7845-H1 server hardware.
2. Download the license key files for any media firmware or text-to-speech licenses that have been purchased by your company or organization by going to cume-license-support@cisco.com. These licenses are required for applications that have media or text-to-speech capabilities. For more information, see Chapter 4, "Configuring the Cisco Unified Media Engine."

Note This guide is intended for system administrators who are familiar with the Windows operating system, have a basic understanding of IP telephony, and have full knowledge of Cisco Unified CallManager and the installed IP telephone environment.

Setting Up the Cisco Unified Application Environment

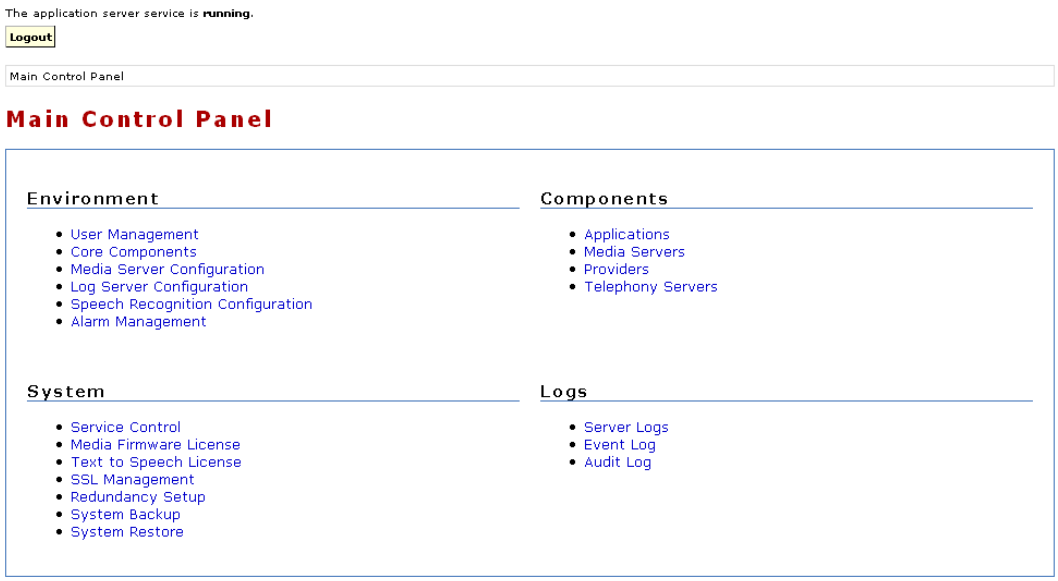
To set up the Cisco Unified Application Environment, you must first perform these installation and configuration tasks:

Task 1: Log into the Management Console

In this task, you must log into the management console to access the Main Control Panel, which you will use to perform various tasks related to the environment, system, components, and logs.

Figure 2-1 shows the Main Control Panel.

Figure 2-1 Main Control Panel



To log into the management console, follow these steps:

Procedure

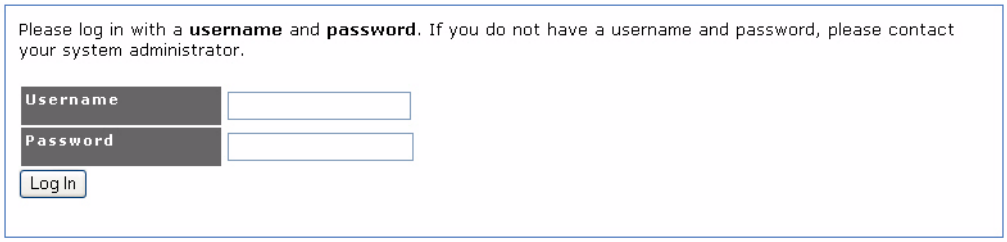
Step 1 Open the management console URL: http://<serverIPaddress>/mceadmin

Step 2 The system response depends upon whether this is a new or existing Cisco Unified Application Environment installation.

- If it is a new installation and the first time a user has accessed the management console, the password wizard opens. Enter and verify a password for the administrator account, and click **Log In**.
- If the management console has been accessed previously, the Management Console Login Screen opens (Figure 2-2). Enter the username and password. Click **Log In**.

The Main Control Panel opens (Figure 2-1).

Figure 2-2 Management Console Login Screen



Note You can reach the Main Control Panel at any time by clicking the Main Control Panel link near the top of the screen.

Now that you are logged into the management console, you can perform the required set-up tasks from the console.

Related Topics

- Task 2: Enter License Keys, page 2-3
- Configuring Components, page 3-1
- Configuring System Parameters, page 3-30
- Configuring Environment Parameters, page 3-35
- Viewing Log Information, page 5-1

Task 2: Enter License Keys

In this task, you use the management console to upload license files for media firmware and text-to-speech applications. Each license file contains a key that is required to activate a feature. Applications that use media capabilities require a media firmware license, and applications that use text-to-speech capabilities require a text-to-speech license.

To upload and activate a media firmware license, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Firmware License**.

Step 2 Click **Browse...** and highlight the file.

Step 3 Click **Open** to make the file available for uploading.

Step 4 Click **Upload and Activate**.

The media server is shut down and restarted.

To upload and activate a text-to-speech license, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Text to Speech License**.

Step 2 Click **Browse...** and highlight the file.

Step 3 Click **Open** to make the file available for uploading.

Step 4 Click **Upload**.

Related Topics

- Task 3: Assign Media Engines to the Application Server, page 2-4
- Uploading and Activating a Media Firmware License, page 4-1
- Uploading and Activating a Text-to-Speech License, page 4-3

Task 3: Assign Media Engines to the Application Server

In this task, it is assumed that the Cisco Unified Application Server will be hosting applications that use media capabilities. Therefore, you must identify the Cisco Unified Application Environment servers that have media engine software activated. When this is completed, you can add the media engines to collections of media engines (media resource groups) and configure an application and associate each partition of the application with a media resource group. This enables the application server to automatically use the available media engines and apply load balancing as needed.

Note It is necessary to add a media server to support media applications even if the application server and media server are on the same hardware platform.

To assign media engines to an application server, follow these steps:

Procedure

Step 1 From the Main Control Panel, click on **Media Servers**.

Step 2 Click **Add a Media Server**.

Step 3 Enter a user-friendly name to identify the media server.

Step 4 Enter the media server IP address.

Step 5 Enter the password required for access to the media server, and re-enter the password to verify.

Step 6 Accept the value Default for the Add to Group field.

Note The Add to Group field lists the available media resource groups For information on adding and assigning additional media resource groups, see the "Applications" section on page 3-1.

Step 7 Keep the Connection Type field as IPC.

Step 8 Click **Add**.

Related Topics

- Task 4: Configure Cisco Unified CallManager Clusters to Integrate with the Cisco Unified Application Server, page 2-5
- Applications, page 3-1

Task 4: Configure Cisco Unified CallManager Clusters to Integrate with the Cisco Unified Application Server

In this task, it is assumed that you plan to use applications that perform telephony operations. Therefore, you must configure one or more telephony servers to serve as endpoints for making and receiving calls to and from the application server.

However, the specific configuration steps are dependent upon the specific telephony protocol that the application uses. The Cisco Unified Application Environment supports the following telephony protocols:

- H.323
- SIP
- CTI
- SCCP

See the "Telephony Servers" section on page 3-24 for instructions on configuring IP telephony servers for each protocol.

Related Topics

- Task 5: Install Applications, page 2-5
- Telephony Servers, page 3-24

Task 5: Install Applications

In this task, you must install the sample MakeCall and AnswerCall applications that were developed using the Cisco Unified Application Designer.

Note The steps required to configure a standard or custom application are specific to the application and are beyond the scope of this guide. See the "Task 4: Install, Configure, and Test Sample Applications" section on page 2-9 for instructions on installing and configuring sample applications.

To install the sample MakeCall or AnswerCall application, follow these steps:

Procedure

Step 1 Download the MakeCall or AnswerCall application to your computer by going to http://www.cisco.com/en/US/products/ps7056/tsd_products_support_series_home.html.

Step 2 From the Main Control Panel, click **Applications**.

Step 3 Click **Browse...** and highlight the application file.

Step 4 Click **Open** to make the file available for uploading.

Step 5 Click **Upload File**.

The file is uploaded and added to the list on the Applications page.

After completing tasks 1-5, you are now ready to use the Cisco Unified Application Environment to create, deploy, and execute converged voice and data applications. The specific procedures for these tasks differ according to your network infrastructure and application type. The next section, Configuring an Example Environment, page 2-6, describes how to configure Cisco Unified Application Environment to support two sample applications, load the applications, and then execute them.

Related Topics

- Configuring an Example Environment, page 2-6

Configuring an Example Environment

This section provides an example deployment scenario for setting up and configuring a Cisco Unified Application Environment.The specific tasks required for setting up the Cisco Unified Application Environment will vary depending on the integration requirements of each application.

Assumptions About the Example Environment

The specific tasks required for setting up the Cisco Unified Application Environment will vary according to specific protocols and applications such as these:

- Number of application servers and media engines
- Number of Cisco Unified CallManager clusters
- Type of telephony protocol
- Types of applications to used

To show how the set-up process is typically performed, this section describes how to set up and configure an example environment having these properties:

- One Cisco Unified Application Server and one Cisco Unified Media Engine co-located on the same physical server, called the UAE Server
- H.323 used for telephony integration
- IP addresses for the UAE server: 10.1.1.50 and 10.1.1.51
- One CallManager cluster consisting of a publisher and a subscriber
  - Publisher IP address: 10.1.1.100
  - Subscriber IP address: 10.1.1.101
- Sample applications used for integration
  - MakeCall
  - AnswerCall

- Route pattern of the form 5000X to route to the application server

Setting Up an Example Deployment and Performing Configuration Tasks

To get started setting up your example deployment, you must perform these configuration tasks:

Note Typically, the required tasks will vary according to the specific protocols and applications.

- Task 1: Create an H.323 Gateway Telephony Server
- Task 2: Identify the H.323 Gateway In Cisco Unified CallManager
- Task 3: Set Up a Route Pattern
- Task 4: Install, Configure, and Test Sample Applications

Task 1: Create an H.323 Gateway Telephony Server

In this task, you will use H.323 as the IP telephony protocol, by first creating a single H.323 gateway telephony server corresponding to the subscriber IP address of the Cisco Unified CallManager cluster, and then placing the gateway into a H,323 call route group (a collection of H.323 gateways). When you later configure an application, you can associate a call route group with each application partition.

To create the H.323 gateway telephony server, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Select **H.323 Gateway** from the Add a Telephony Server pull-down list.

Step 3 Click **Add Server**.

Step 4 Enter a unique name and description for the gateway.

Step 5 Enter the IP address for the gateway, which will be a Cisco Unified CallManager subscriber.

Step 6 Keep the default call route group setting of Default H.323 in the Add to Group field.

Step 7 Click **Add H.323 Gateway** to create the gateway.

Related Topics

- Task 2: Identify the H.323 Gateway In Cisco Unified CallManager

Task 2: Identify the H.323 Gateway In Cisco Unified CallManager

In this task, you must first associate the H.323 gateway you created with the Cisco Unified CallManager and define an H.323 Gateway using the Cisco Unified CallManager administrative interface. You must also verify that the H.323 gateway device name corresponds to the IP address (or DNS name) of the

primary IP address of the Cisco Unified Application Server and then correctly identify the calling search space, which will determine the calling privileges of the application that is configured using the default call route group.

To associate the H.323 gateway and identify the correct parameters, follow these steps:

Procedure

Step 1 Open the Cisco Unified CallManager administrative web interface.

Step 2 Choose **Device > Add a New Device**.

Step 3 Select **Gateway**, and click **Next**.

Step 4 Select **H.323** as the gateway type, and click **Next**.

Step 5 Enter the gateway configuration information. Table 2-1 lists key fields and suggested settings.

Step 6 Uncheck **Wait for Far End H.245 Terminal Capability Set**.

Step 7 Click **Insert**.

Table 2-1 Gateway Configuration Information

Field	Description/Recommendation
Device Pool	Choose a device pool with the understanding that the RTP streams for this H.323 gateway terminate at the media engines in the media resource group used by partitions with this H.323 gateway in their configured call route group.
Location	Choose a location for your deployment with the understanding that the RTP streams for this H.323 gateway terminate at the media engines in the media resource group used by partitions with this H.323 gateway in their configured call route group.
Calling Search Space	Choose the calling search space for your deployment with the understanding that the RTP streams for this H.323 gateway terminate at the media engines in the media resource group used by partitions with this H.323 gateway in their configured call route group.
Media Resource Group List	Choose a media resource group for your deployment with the understanding that the RTP streams for this H.323 gateway terminate at the media engines in the media resource group used by partitions with this H.323 gateway in their configured call route group.
Tunneled Protocol	Recommended setting: None
Signaling Port	Recommended setting: 1720
Media Termination Point	Recommended setting: Uncheck
Retry Video Call	Recommended setting: Audio
Wait for Far End H.245 Terminal Capability Set	Recommended setting: Uncheck
Outbound Calls section	Recommended setting: Use defaults

Related Topics

Task 3: Set Up a Route Pattern

Task 3: Set Up a Route Pattern

In this task, you must set up a route pattern in Cisco Unified CallManager to provide a route to the H.323 gateway just defined.

To set up a route pattern in Cisco Unified CallManager, follow these steps:

Procedure

Step 1 Open the Cisco Unified CallManager administrative web interface.

Step 2 Choose **Route Plan > Route/Hunt > Route Pattern**.

Step 3 Click **Add a New Route Pattern**.

Step 4 Enter the route pattern name 5000X in the Name field. All other fields can be kept at their default values.

Step 5 Click **Insert**.

You are now ready to install, configure, and test some sample applications.

Related Topics

Task 4: Install, Configure, and Test Sample Applications

Task 4: Install, Configure, and Test Sample Applications

After completing tasks 1-3, you can install, configure, and test these sample applications:

- MakeCall—Sample application, which generates a call to a configured directory number (DN).
- AnswerCall—Sample application, which answers an incoming call to the Cisco Unified Application Server.

In this task, you will:

- Install the MakeCall application.
- Test outbound dialing from the application server to Cisco Unified CallManager.
- Verify the trigger parameters for the HandleMakeCall script.
- Install the AnswerCall application.
- Define the trigger parameter for the HandleInboundCall.
- Answer a call routed to the Application Server to verify that you have successfully integrated outbound calling using H.323 and the Application Environment.

MakeCall Application

The MakeCall application tests outbound dialing from the application server to Cisco Unified CallManager. The MakeCall application:

1. Uses a configured number to place an outbound call to a specified DN.
2. Plays ‘goodbye’ three times.
3. Hangs up on the called party.

A successful call indicates that the Cisco Unified CallManager cluster interprets the call as originating from the H.323 gateway that represents the Cisco Unified Application Server.

Figure 2-3 shows the call flow in which the MakeCall application makes a call to an internal IP phone.

1. The application server makes an H.323 call to Cisco Unified CallManager.
2. Cisco Unified CallManager makes a call using SCCP to the IP phone as a result of the call from the application server.
3. When the call is answered by the Application Server, RTP streams are established between the IP phone and the media engine.

Figure 2-3 MakeCall Application Call Flow

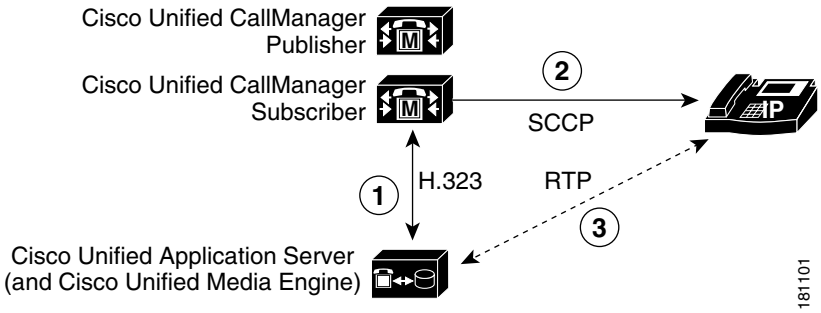
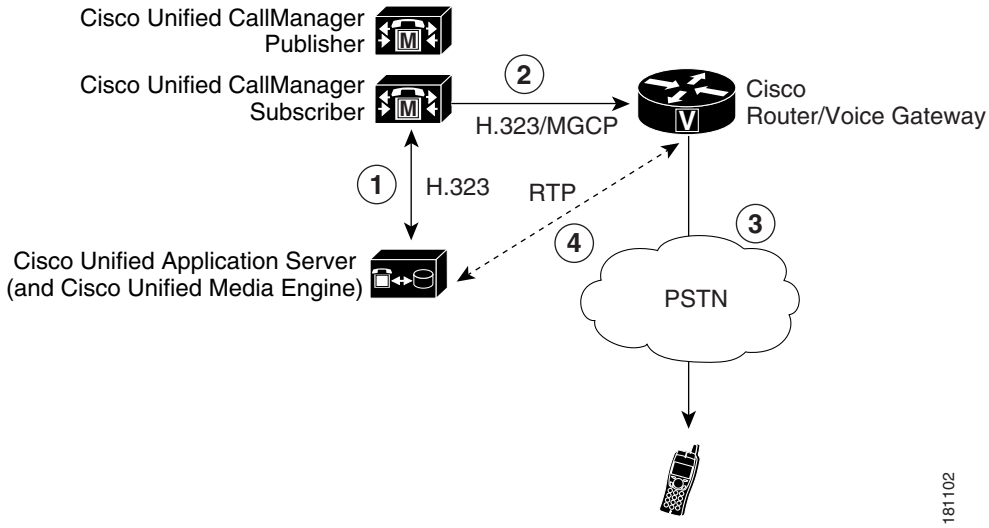


Figure 2-4 shows the call flow in which the MakeCall application makes a call to a phone on the Public Switched Telephone Network (PSTN).

1. The application server makes an H.323 call to Cisco Unified CallManager.
2. Cisco Unified CallManager makes a call using H.323 or MGCP to the gateway as a result of the call from the application server.
3. The gateway makes a call to the PSTN as a result of the call from Cisco Unified CallManager.
4. When the call is answered by the phone on the PSTN, RTP streams are established between the gateway and the media engine.

Figure 2-4 MakeCall Application Call Flow



To install the MakeCall application, follow these steps:

Procedure

Step 1 Download the MakeCall application to your computer by going to http://www.cisco.com/en/US/products/ps7056/index.html.

Step 2 From the Main Control Panel, click **Applications**.

Step 3 Click **Browse...** and highlight the application file.

Step 4 Click **Open** to make the file available for uploading.

Step 5 Click **Upload File**.

The file is uploaded and added to the list on the Applications page.

Step 6 Click the underlined MakeCall link to configure the application.

Step 7 Click **Apply**.

Note Each application must execute as a partition. For the MakeCall example, the application is running in the default partition. If you click the Edit button for the Default partition on the MakeCall page, you will see that the default call route group and media resource group are automatically selected and that the dialed number you configured is included. See the "Partitions" section on page 3-3 for information on configuring partitions.

The MakeCall application incorporates the HandleMakeCall script, which triggers, or initiates, when an HTTP request is received over port 8000 on the application server. Because multiple HTTP-triggered scripts can be installed on the application server, you must verify that the HandleMakeCall script uses a unique trigger parameter.

To verify the trigger parameters for the HandleMakeCall script, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the MakeCall link to open the MakeCall page.

Step 3 Scroll down to the Partition section, and click the Edit button for the Default partition.

Step 4 Scroll down and click **Edit Trigger Parameters.**

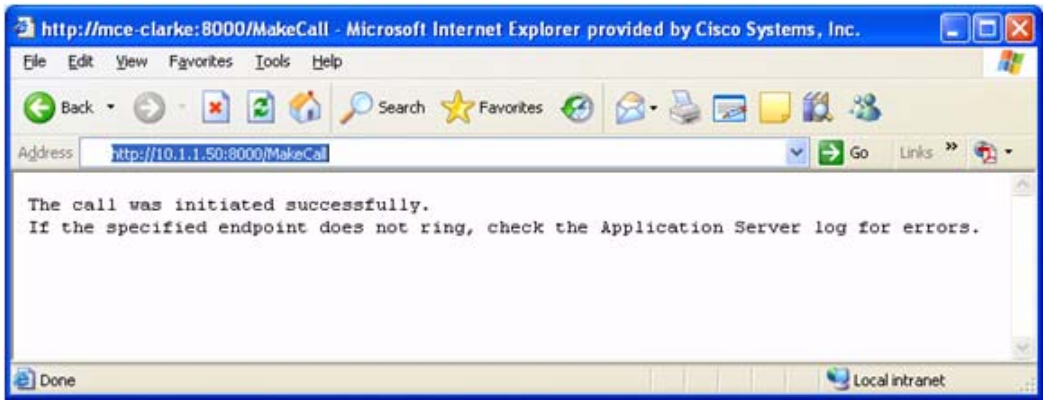
Step 5 Verify that the url trigger parameter value has the value /MakeCall. This means that the HandleMakeCall script will initiate when an HTTP request comes in with the URL http://<Application Server IP>:8000/MakeCall.

Step 6 Click **Apply Parameter Values**.

After installing the MakeCall application and verifying the trigger setting you can test the application by opening a web browser and entering http://<Application Server IP>:8000/MakeCall.

If the outbound call succeeds as message is presented, as shown in Figure 2-5, and you hear 'goodbye' three times, then you have successfully integrated outbound calling using H.323 and the Application Environment.

Figure 2-5 Testing the MakeCall Application



Note If the test does not work, check the server logs for any errors. See XXX.

AnswerCall Application

The AnswerCall application tests inbound calling to the application server. The AnswerCall application:

1. Answers a call routed to the application server.
2. Plays 'goodbye' three times.
3. Hangs up on the caller.

A successful call indicates that the Cisco Unified Application Server is able to receive incoming calls.

Figure 2-6 shows the call flow in which the AnswerCall application answers a call from an internal IP phone.

1. A call is made from an IP phone to Cisco Unified CallManager.
2. Cisco Unified CallManager makes an H.323 call as a result of the call from the IP phone.
3. When the call is answered by the application server, RTP streams are established between the IP phone and the media engine.

Figure 2-6 AnswerCall Application Call Flow

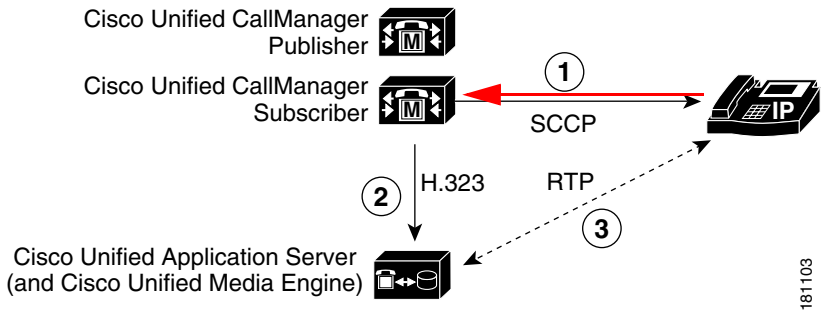
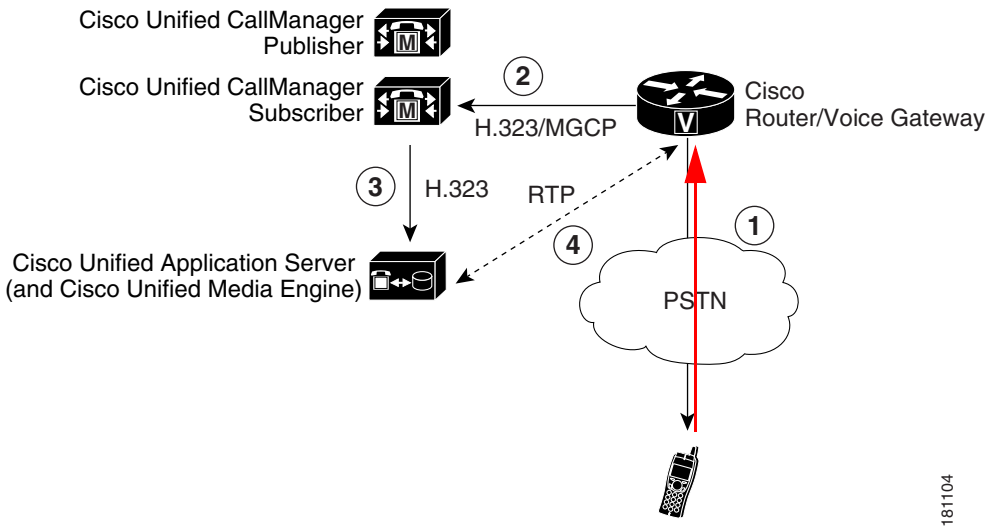


Figure 2-7 shows the call flow in which the AnswerCall application answers a call from the PSTN.

1. A phone on the PSTN makes a call to an H.323 or MGCP gateway.
2. The gateway makes a call to Cisco Unified CallManager as a result of the call from the PSTN phone.
3. Cisco Unified CallManager makes an H.323 call as a result of the call from the gateway.
4. When the call is answered by the application server, RTP streams are established between the gateway and the media engine.

Figure 2-7 AnswerCall Application Call Flow



To install the AnswerCall application, follow these steps:

Procedure

Step 1 Download the AnswerCall application to your computer by going to http://www.cisco.com/en/US/products/ps7056/index.html.

Step 2 From the Main Control Panel, click **Applications**.

Step 3 Click **Browse...** and highlight the application file.

Step 4 Click **Open** to make the file available for uploading.

Step 5 Click **Upload File**.

The file is uploaded and added to the list on the Applications page.

Step 6 Click the underlined AnswerCall link to configure the application.

Step 7 Click **Apply**.

Note Each application must execute as a partition. For the AnswerCall example, the application is running in the default partition. If you click the Edit button for the Default partition on the AnswerCall page, you will see that the default call route group and media resource group are automatically selected. See the "Partitions" section on page 3-3 for information on configuring partitions.

The HandleInboundCall script which handles calls routed to the application server, does not contain any pre-defined trigger parameters. However, because it is a dial-in application (you dial a number to test it), it is a good idea to define a trigger parameter for the script.

For consistency with the route pattern 5000X, which was previously defined (Task 3: Set Up a Route Pattern, page 2-9), you should define a trigger parameter with the name 'to' and value '50000.'

To define the trigger parameter for the HandleInboundCall script, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the AnswerCall link to open the AnswerCall page.

Step 3 Scroll down to the Partition section, and click the Edit button for the Default partition.

Step 4 Scroll down and click **Edit Trigger Parameters.**

Step 5 Enter 50000 for the parameter value.

Step 6 Click **Apply Parameter Values**.

To test the application, call 50000 from an IP phone that is configured to dial to the route pattern that was previously defined (Figure 2-8). The call should answer immediately, and you should hear three 'goodbye's followed by a hang up.

Note If the test does not work, check the server logs for any errors. See XXX.

Figure 2-8 Testing the AnswerCall Application

You have now completed the installation, configuration, and testing of two sample applications. See these chapters for additional configuration and maintenance information and instructions:

- Chapter 3, "Configuring the Cisco Unified Application Server"
- Chapter 4, "Configuring the Cisco Unified Media Engine"
- Chapter 5, "Maintaining the Cisco Unified Application Environment"

Planning for Redundancy and Load Balancing

The Cisco Unified Application Environment includes limited support for redundancy (with clustering) and load balancing.

Clustering

The Cisco Unified Application Environment is intended to be used in a ring configuration. For example, if you have three application servers, they can each act as a hot standby for the others. Each server can act as both a redundancy master and standby.

When the master/standby relationship is established, the standby machines create an active replication link with the respective master servers. If a master server becomes unreachable, its standby uses the replicated configuration information to register the devices held by the master server in addition to its own.

When the master server recovers, the standby relinquishes the devices that were originally owned by the master and then signals the master to begin registration. The master registers its original devices and the configuration is restored.

The clustering mechanism is subject to these limitations:

- Active calls that involve the failing server may or may not be terminated depending on the signalling protocol used and whether or not the call used media resources that were located on the failing appliance.
- All active application instances and related state information are be lost during failover.

Load Balancing and Scalability

The mechanism used to scale the Cisco Unified Application Environment depends upon the interfaces that are used by applications running on the server.

Application instances are isolated to the server on which they run; servers in a cluster do not share application runtime information. Therefore, it is imperative that the load-balancing mechanism enables application instances to receive the signals that they require and that those signals are not routed to other servers in the cluster.

For example, if an application triggers on an HTTP request and then expects to receive a call into an H.323 gateway, you must ensure that the call will be routed to the same server as the HTTP request.

<<The rest of this description seemed rather incomplete, so I did not add it.>>

CHAPTER 3

Configuring the Cisco Unified Application Server

This chapter describes how to use the Cisco Unified Application Environment management console to manage application servers and includes these sections:

Configuring Components

The management console provides access to the system components used to manage IP telephony applications. The Components group contains links to these configuration pages.

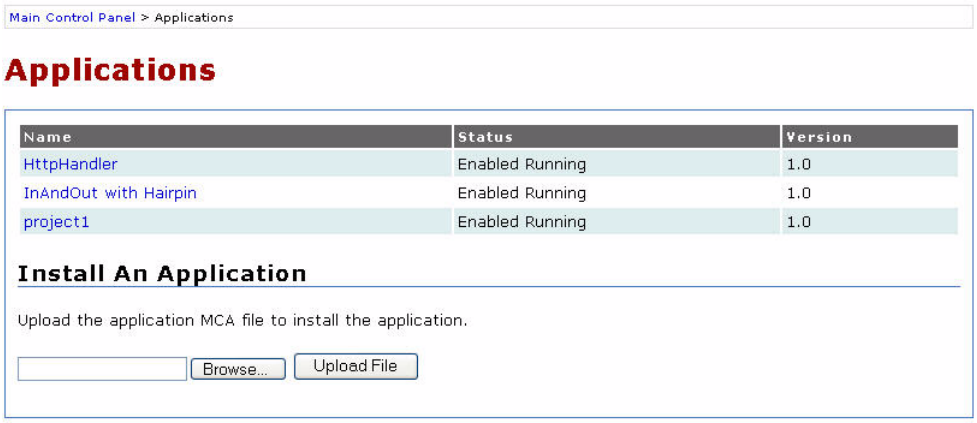
- Applications—Install and uninstall applications
- Partitions—Control configuration profiles for an application
- Media Servers—Enable the Cisco Unified Application Environment to act as a media endpoint
- Providers—Display the list of providers, which open network ports and allow the runtime environment to communicate with devices
- Telephony Servers—Configure interactions with IP telephony devices

Applications

You must open the Applications page (Figure 3-1) to install and uninstall applications. When you open the Applications page, the page displays the application name (displayed as a link), status, and version number. An application typically includes configuration items that are unique to your deployment and which you must configure after the application is installed.

Note All application configuration occurs at the partition level. See the "Partitions" section on page 3-3 for information about partitions.

Figure 3-1 Applications Page



To install an application, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click **Browse** and highlight the file.

Step 3 Click **Open**.

Step 4 Click **Upload File**.

The Application Manager processes the file, installs the application, and updates the Applications page to list the application.

To enable an application, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the underlined application link.

Step 3 Click **Enable Application**.

The application begins running. If you return to the Applications page, the Status column shows that the application is enabled.

To disable an application, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the underlined application link.

Step 3 Click **Disable Application**.

The application stops running. If you return to the Applications page, the Status column shows that the application is Disabled.

To modify application settings, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the underlined application link.

Step 3 Make changes as needed.

Step 4 Click **Apply**.

To uninstall an application setting, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the underlined application link.

Step 3 Click **Uninstall Application**.

Step 4 Click **OK** to confirm. <<Is this correct?>>

The application is removed.

Partitions

All application configuration occurs at the partition level. A partition is a configuration profile for an application. Applications can support multiple partitions, enabling you to create and execute multiple versions of the same application on a single Cisco Unified Application server.

Partitions are flexible and can be useful in a variety of situations. For example, if an application is intended to serve end-users located on distinct Cisco Unified CallManager clusters, it is desirable for all call control and media streams to terminate to the cluster and the corresponding network and telephony resources. At the same time, it may be desirable to have another configurable protocol on the application, such as LDAP, which makes reference to the same central location, regardless of the partition.

Each partition is associated with a call route group and media resource group. By defining unique call route groups and media resource groups, you can identify the partitions that use individual media servers. For each partition, you can also determine which Cisco Unified CallManager cluster is used for making calls by specifying a call route group that corresponds to the particular telephony protocol and group.

Each application is also associated with scripts, which are partitioned along with the application. Because multiple scripts can execute actions through the same protocol, you must specify the conditions under which a partitioned script should initiate action.

For example, assume that an application has one script and three partitions and activates on an IncomingCall trigger. The default partition has no triggering parameters and can act as a catch-all for events which do not match other partitions.

The application server determines the best match handler for a given event. Other partitions take effect if their trigger parameters are activated. For example, if Partition 2 specifies to=2000, then when a call comes in for extension 2000, partition 2 will activate. If no trigger matches, the default partition will be active.

A partition is similar to a configuration template for a script and follows these rules:

- The application developer sets the event that triggers a script. The event applies to all partitions and cannot be changed.
- All installed script partitions across all applications are treated as equal.
- If any two partitions have identical triggering criteria, either one may trigger; therefore, it is important that all partitions have unique triggering criteria.
- The router will match the handler that best fits the events. For example, if partition A specifies to=2000 and partition B specifies to=2000 and from=1000, then a call from 1000 to 2000 triggers B.

To create a new partition, follow these steps:

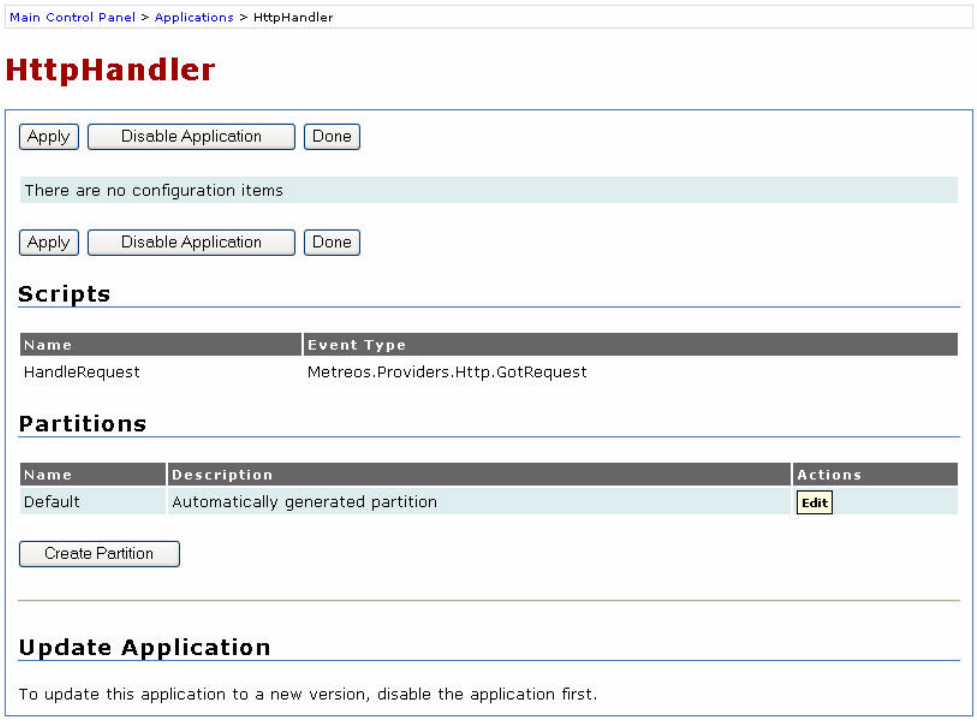
Procedure

Step 1 From the Main Control Panel, click **Applications**.

Step 2 Click the underlined application name.

A page opens to display available settings (Figure 3-2).

Figure 3-2 Application Manager Example Page



Step 3 Click **Create Partition**.

Step 4 Configure settings as described in Table 3-1.

Step 5 Click **Create Partition**.

Note Parameter values are inherited from the default partition, and all unchanged parameters in the new partition remain linked to parameters in the default partition. These parameter values will be updated in the new partition to match any changes made to them in the default partition.

Step 6 Under Scripts, click **Edit Trigger Parameters**.

Step 7 Enter at least one trigger parameter name and value. Trigger requirements are dictated by the needs of the application and are beyond the scope of this document.

Step 8 Click **Done** to return to the application page.

Table 3-1 Partition Parameters

Field	Description
Name	Name of partition.
Description	Information to identify the partition.
Enable	Indication of whether or not the partition is active.
Reserve Media Early	Field in which to reserve media ports early to reduce setup time.
Call Route Group	Used by an application only when making outbound calls. The protocol of the inbound call is determined by a combination of Cisco Unified CallManager configuration and triggering parameters on the partitioned script.
Media Resource Group	Media server group that is closest in proximity to IP endpoints that will be using this application.
Preferred Codec	Preferred media resource codec.

Defining Trigger Parameters

You can define triggers in any of the following ways:

- Single value—Figure 3-3 shows an example trigger that activates when extension 2000 receives a call.
- List of values—Figure 3-4 shows an example trigger that activates when a call is received from extension 2000, 2001, or 2003.
- Single regular expression—Figure 3-5 shows an example trigger that activates when a call is received on any of the extensions 2000-2999 (regex:2[0-9][0-9][0-9]).
- Combination of methods—Figure 3-6 shows an example trigger that includes a single value trigger that activates when the extension 2000 is called and a regular expression trigger that activates when a call is received on any of the extensions 2000-2999 (regex:2[0-9][0-9][0-9]).

Note A regular expression is indicated by adding regex: before the expression. You cannot mix literal values and regular expressions in a list. Only a single regular expression can be used as a trigger parameter for a given partition. The syntax [0-9] in a regular expression is equivalent to the CallManager X notation used in route patterns and CTI Route point line numbers.

Figure 3-3 Example Single Value Trigger Parameter Configuration

Figure 3-4 Example Value List Trigger Parameter Configuration

Figure 3-5 Example Regular Expression Trigger Parameter Configuration

Figure 3-6 Example Combined Trigger Parameter Configuration

Event Types and Trigger Parameters

This section lists trigger parameters for the following event types:

- Metreos.CallControl.IncomingCall—Table 3-2
- Metreos.Providers.Http.GotRequest—Table 3-3
- Metreos.Providers.JTapi.JTapiIncomingCall—Table 3-4
- Metreos.Providers.JTapi.JTapiCallInitiated—Table 3-5
- Metreos.Providers.TimerFacility.TimerFire—Table 3-6

Table 3-2 Metreos.CallControl.IncomingCall

Trigger Parameter	Description
To	The called party, or last redirected number, if redirected.
From	The number of the calling party.
OriginalTo	The original called party, even if redirected.
DisplayName	The textual display name associated with the calling party.

Table 3-3 Metreos.Providers.Http.GotRequest

Trigger Parameter	Description
Url	Path portion of the requested URI. This must always begin with a /.
Hostname	Host portion of the requested URI. This will not contain port info
Host	Host portion of the requested URI, and may contain port info.
Port	Port portion of the requested URI.
Body	The content of the request
Method	Request method. This will be either GET or POST.
Query	Query string portion of the requested URI.
RemoteHost	The IP address and port of the remote client
RemoteIPAddress	The IP address of the remote client.

Table 3-4 Metreos.Providers.JTapi.JTapiIncomingCall

Trigger Parameter	Description
To	The called party, or last redirected number, if redirected.
From	The number of the calling party.
OriginalTo	The original called party, even if redirected.
DeviceName	The name of the device that the call came in on.

Table 3-5 Metreos.Providers.JTapi.JTapiCallInitiated

Trigger Parameter	Description
To	The called party.
From	The number of the calling party.
DeviceName	The name of the device that the call was initiated from.

Table 3-6 Metreos.Providers.TimerFacility.TimerFire

Trigger Parameter	Description
TimerUserData	An opaque token used to allow distinguishable events to be raised. In practice, an administrator would need to informed of what this value should be.

Media Servers

In order for the Cisco Unified Application Environment to act as a media endpoint, a media server must be present and the Cisco Unified Application Environment must be configured to use the server. The decision to use a media server ultimately rests with the needs of the application. All applications that place or answer calls require a media server.

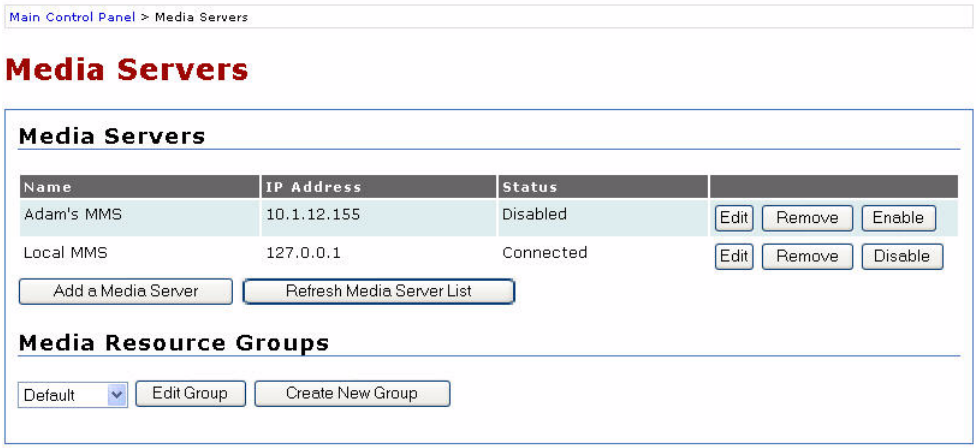
Note Some applications do not require media engines; for example, telephony applications that use peer-to-peer media negotiation.

To be available for use by applications, each media server must be placed in a media resource group, which is assigned within the application partition. All media servers are placed automatically into the Default media resource group, and all application partitions can use the default group. Creating custom media resource groups is recommended in the following cases:

- Diverse geography—If a single Cisco Unified Application Environment provides call control for calls that originate and terminate in different countries, it is desirable to use media servers that are physically located in each country to service the calls directed to that country. For example, a click-to-talk application may reside on the Cisco Unified Application Server in New York but be triggered by a user in India to call another phone number in India. If all media servers in India are assigned to a custom media resource group, the application can be instructed to use the servers in the Indian media resource group to process calls that originate and terminate in India.
- Resource guarantees—Some applications, such as scheduled conferencing, are sensitive to resource utilization and may not recover well from unexpected loss of media resources due to the demands of other applications. To reserve the needed resources, you can assign specific media servers to a custom media resource group. The application then reserve the resources of the custom media resource group.

Use the Media Servers page (Figure 3-7) to create and configure media servers and media server groups. A media server group is a container for a collection of media servers. Each media server must be associated with one or more groups. It is also possible, but not necessary, to create media server groups. The system provides a default media server group for use if multiple groups are not needed.

Figure 3-7 Media Servers Page



To create and configure media servers, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Servers**.

Step 2 Choose from these actions:

- Add a media server:

  Click **Add a Media Server**, enter values as described in Table 3-7, and click **Add**.

- Edit parameters for an existing media server:

  Click the Edit button to the right of the server entry, enter values as described in Table 3-7, and click **Apply**.

- Enable a media server:

  Click the Enable button to the right of the server entry.

- Remove a media server.

  Click the Enable button to the right of the server entry.

Table 3-7 Media Server Parameters

Field	Description
Name	Name of media server
IP Address	IP address of media server
Password	Password for access to media server
Connection Type	Method of connecting to media server (use IPC)
Add to Group	Group to which media server is assigned

To add a media resource group, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Servers**.

Step 2 Click **Create New Group**.

Step 3 Enter values as described in Table 3-7, and click **Add**.

Step 4 Add or remove members:

- To add a member, select the member name, and click **Add Member**. Add additional members as needed.
- To remove a member, select the member name, and click **Remove**.

Step 5 Click **Create Group**.

To edit an existing media resource group, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Servers**.

Step 2 In the Media Resource Groups area, click **Edit New Group**.

Step 3 Enter values as described in Table 3-7.

Step 4 Add or remove members:

- To add a member, select the member name, and click **Add Member**. Add additional members as needed.
- To remove a member, select the member name, and click **Remove**.

Step 5 Click **Apply**.

The system adds the server and displays it in the Media Servers list.

To confirm that the Media Server was added to the correct group, select the group from the drop-down list at the bottom of the page and click the Edit Group button.

To remove the media server from the group without removing it from the system, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Servers**.

Step 2 In the Media Resource Groups area, select the group from the pull-down list, and click **Edit Group**.

Step 3 Click **Delete Group**.

Step 4 Click **OK** to confirm.

The group is deleted and removed from the pull-down list on the Media Servers page.

Caution A media server cannot be used unless it is associated with a group. If removed from a group, it must be reassigned before an application can access it; if not explicitly added to a group, it will be inaccessible.

To remove a media server from the system, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Servers**.

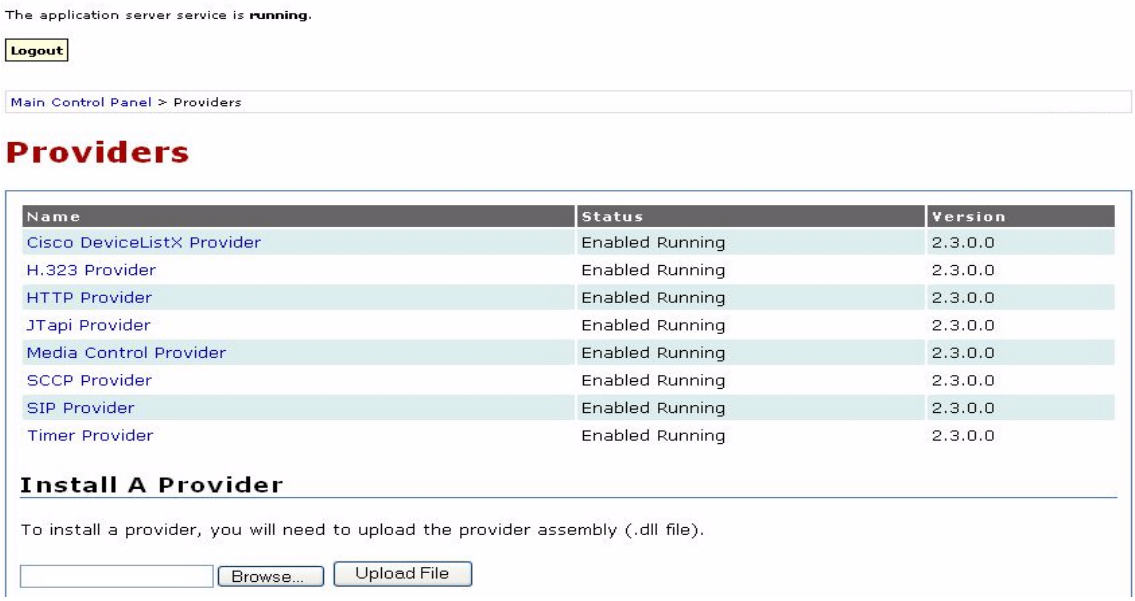
Step 2 Click **Remove** to the right of the Media Server you want to delete.

The media server is deleted and removed from the list on Media Servers page.

Providers

Providers are application server plug-in modules that open network ports and allow the runtime environment to communicate with devices on the network. Use the Providers page (Figure 3-8) to display the list of providers shipped with the Cisco Unified Application Server, the status of each provider (Enabled, Running or Disabled), and the version number. Clicking on the provider name launches the configuration page for that provider.

Figure 3-8 Providers Page



From the Main Control Panel, click **Providers** to display the list of providers.

Each provider configuration page includes following sections:

- Configuration—Configurable parameters for the provider.
- Extensions—Special actions exposed by the provider and invoked only through the management console rather than by a script (not all providers have extensions)

To invoke the extension, click **Invoke Extension**.

Note Disabling the provider allows for its subsequent uninstallation, which resets it back to its default configuration settings and makes it unavailable. Restarting the application server will automatically restart the provider.

Click an underlined link to select one of the following providers:

- CiscoDeviceListX Provider
- H.323 Provider
- HTTP Provider
- JTAPI Provider
- Media Control Provider
- SCCP Provider
- SIP Provider
- Timer Provider

To modify provider settings, make changes as needed, and click **Update**. Click **Done** to return to the Providers page.

CiscoDeviceListX Provider

The CiscoDeviceListX provider communicates with Cisco Unified CallManager to retrieve and cache real-time device information for application use. The CiscoDeviceListX (3.X, 4.X) and SNMP (5.X) protocols are used to gather this information. The Cisco Unified CallManagers are specified in the Telephony Servers pages.

The CiscoDeviceListX provider supports the following extensions, which you can invoke on the CiscoDeviceListX Provider page:

- Metreos.Providers.CiscoDeviceListX.Refresh—Forces the application server to reinitialize the real-time cache. This is recommended if phone device IP addresses have been changed.

Figure 3-9 shows the Cisco DeviceListX page, and Table 3-8 lists parameters.

Figure 3-9 Cisco DeviceListX Provider Page

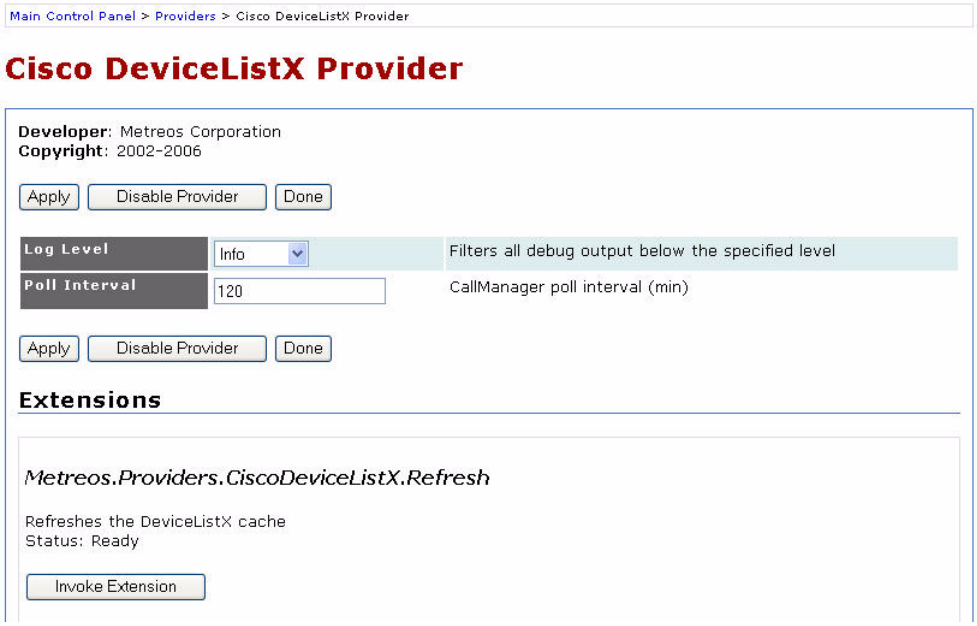


Table 3-8 Cisco DeviceListX Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Poll Interval	Interval in minutes between requests sent to Cisco Unified CallManager to refresh device information (cache refresh)

H.323 Provider

The H.323 provider uses the H.323 protocol to create, receive, and control IP telephony calls between Cisco Unified CallManager nodes. The H.323 provider operates as an H.323 gateway relative to Cisco Unified CallManager.

Figure 3-10 shows the H.323 Provider page, and Table 3-9 lists parameters.

Figure 3-10 H.323 Provider Page

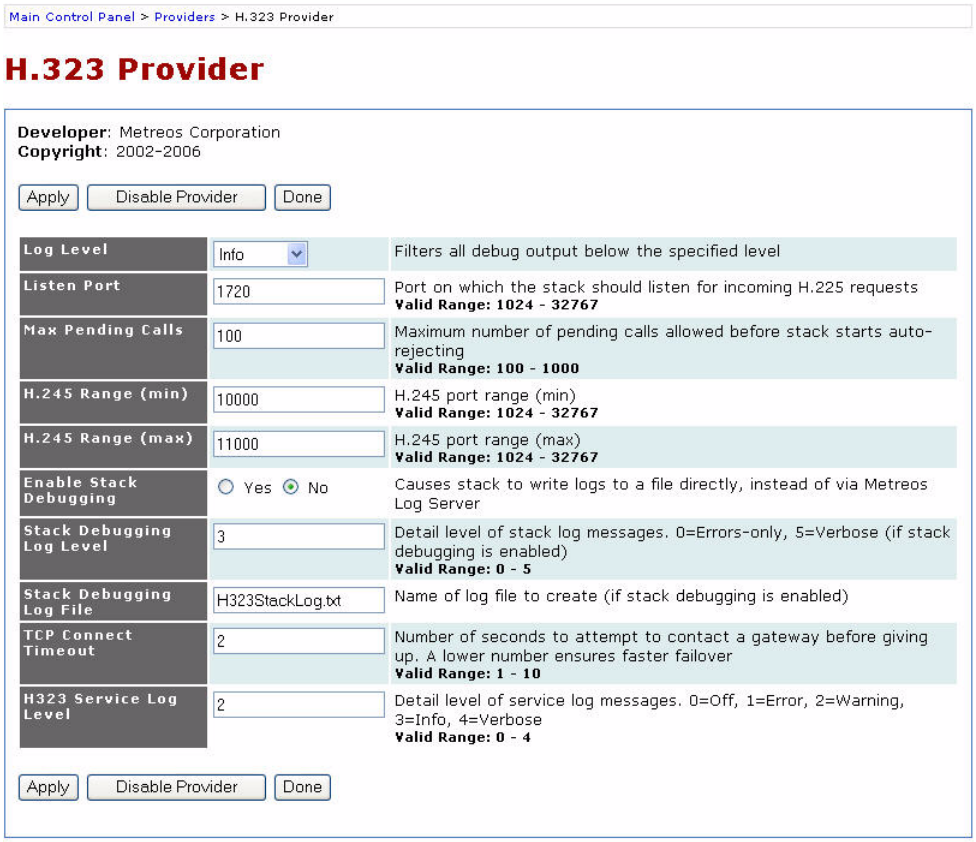


Table 3-9 H.323 Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Port	Number of the port on which H.323 listens
EnableStackDebugging	Field in which to enable StackDebugger, a tool that writes logs to a file for H.323 diagnostics
StackDebuggingLogLevel	Log level specifying detail of logs written by the StackDebugger (valid values are 0 – 5, where 0 disables debugging, and 5 maximizes debugging)
StackDebuggingLogFile	Name of log file for the StackDebuggingLog function
EnableProcessWindow	Field in which to configure H.323 to write debug output to a window rather than a log file

HTTP Provider

The HTTP provider receives HTTP requests from applications over port 8000.

Figure 3-11 shows the HTTP Provider page, and Table 3-10 lists the parameters.

Figure 3-11 HTTP Provider Page

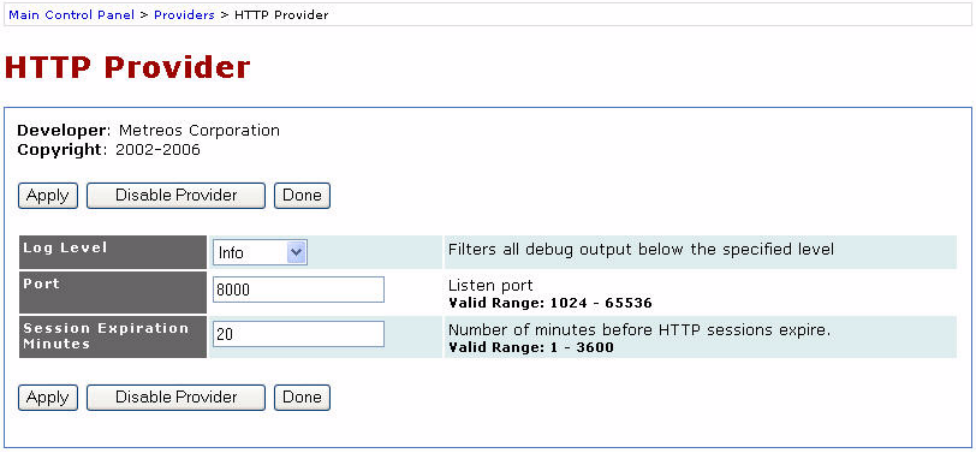


Table 3-10 HTTP Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Name	Name of HTTP provider
Port	Number of the port on which the provider listens
Session Expiration Minutes	Number of inactive minutes before the session is automatically terminated
Session Cleanup Minutes	Interval between clean-up of resources for terminated sessions in minutes

JTAPI Provider

The JTAPI provider uses the CTI protocol to create, receive, and control IP telephony calls. The JTAPI provider registers as CTI router point and CTI port in Cisco Unified CallManager.

Figure 3-12 shows the JTapi Provider page, and Table 3-11 lists the parameters.

Figure 3-12 JTAPI Provider Page

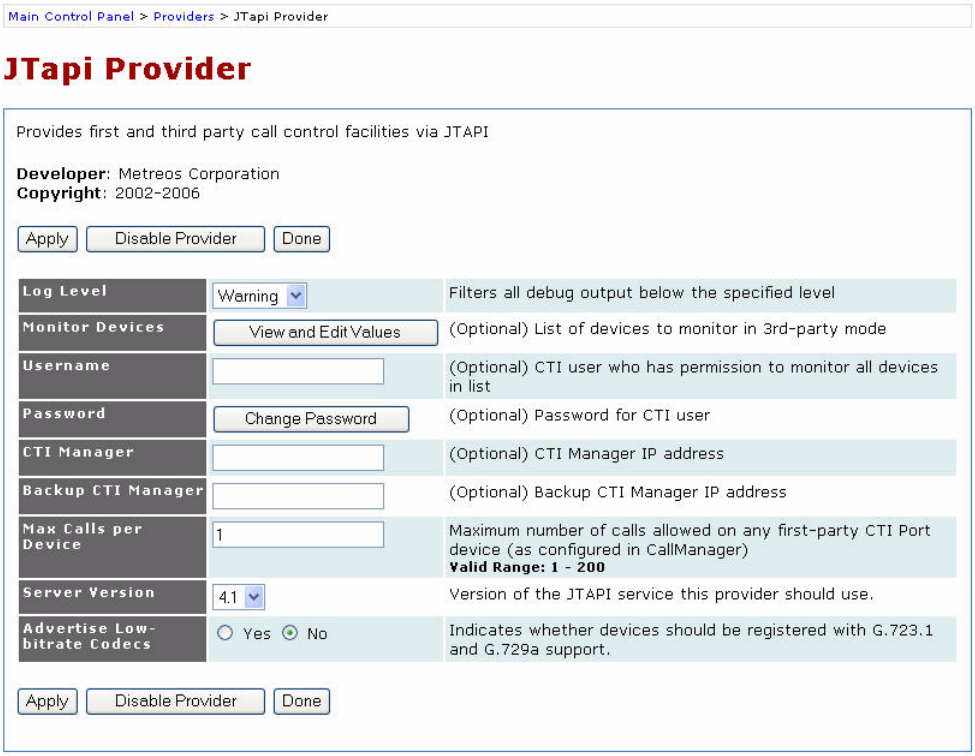


Table 3-11 JTAPI Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Monitor Devices	Devices to monitor
User name	User with permission to monitor specified devices
Password	Password for user with permission to monitor the specified devices
CTI Manager	IP address of CTI manager
Backup CTI Manager	IP address of backup CTI manager
Max Calls per Device	Maximum number of calls allowed on any first-party CTI Port device (this value must match the equivalent value in Cisco Unified CallManager)
Server version	Cisco Unified CallManager release
Advertise Low-bitrate Codecs	Indication of whether devices should be registered with G.723.1 and G.729a support

Perform these actions on the JTAPI provider page:

- Click **View and Edit Values** to create a list of devices to monitor in third party mode. Enter the device name, and click **Add**.

- Click **Change Password** to assign a new password. Enter the new password, reenter it in the Verify Password field, and click **Apply**.
- Click **Done** to return to the Providers page.

Media Control Provider

The Media Control provider manages media engines to provide media capabilities to applications. The Media Control provider supports the following extensions, which you should invoke only under the direction of a Cisco technical support engineer:

- Metreos.MediaControl.RefreshMediaServers—Forces the application server to reinitialize control of the media engines.
- Metreos.MediaControl.ClearMRGCache—Forces the application server to reinitialize the media engine internal storage.
- Metreos.MediaControl.PrintServerTable—Forces the application server to write a summary of all configured media engines to the application server log.
- Metreos.MediaControl.PrintDiags—Forces the application server to write diagnostic information about currently connected media engines to the application server log.

Figure 3-13 shows an excerpt of the Media Control Provider page, and Table 3-12 lists parameters.

Figure 3-13 Media Control Provider Page

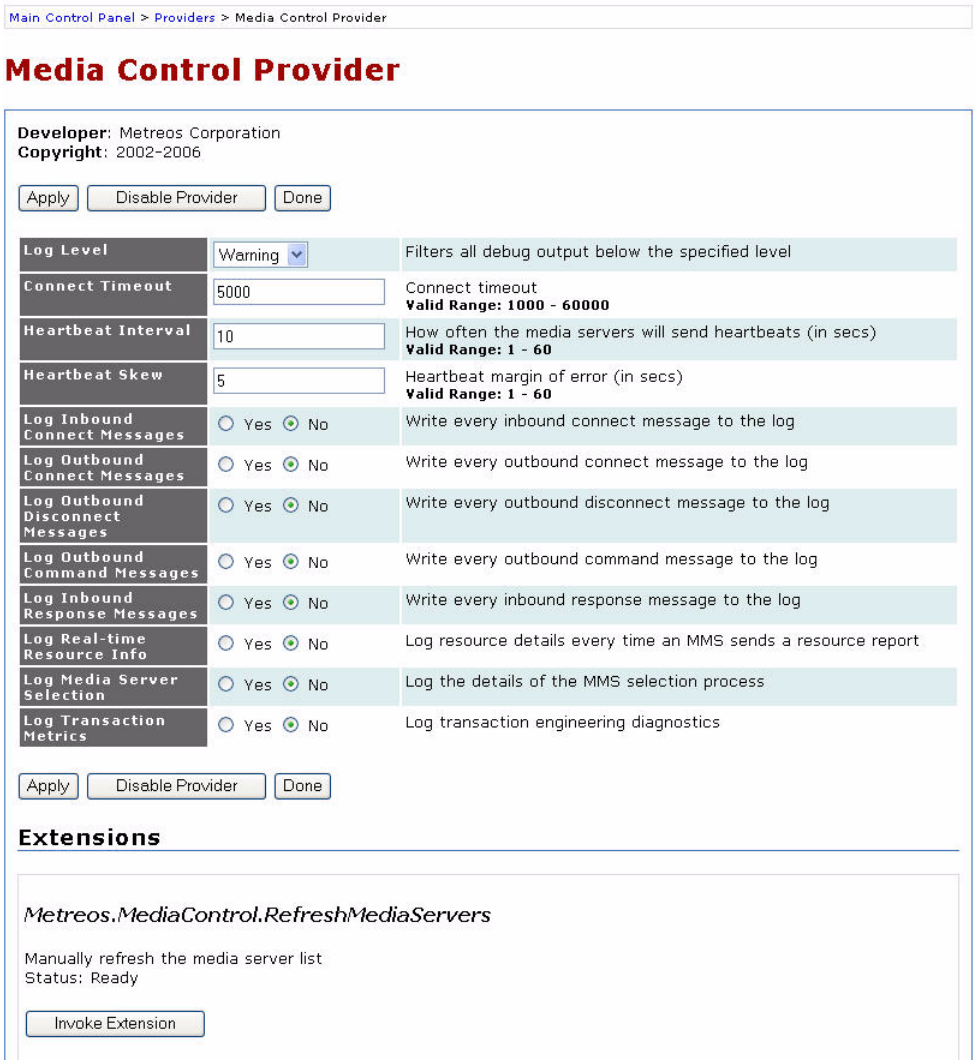


Table 3-12 Media Control Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Connect Timeout	Interval in milliseconds before a connection is deemed unsuccessful and the system attempts to retry
Heartbeat Interval	Interval, in seconds, between heartbeat signals to a media server
Heartbeat Skew	Interval, in seconds, MediaControlProvider waits for a response to the heartbeat signal
DiagInboundConnectMessages	Inbound connect messages written to the Log Server
DiagOutboundConnectMessages	Outbound connect messages written to the Log Server

Table 3-12 Media Control Provider Parameters (continued)

Field	Description
DiagOutboundDisconnectMessages	Outbound disconnect messages written to the Log Server
DiagOutboundCommandMessages	Outbound command messages written to the Log Server
DiagInboundResponseMessages	Responses written to the Log Server
DiagHeartbeatResourceInfo	Heartbeat signal information written to the Log Server

SCCP Provider

The SCCP Provider uses the SCCP protocol to create, receive, and control IP telephony calls. The SCCP provider registers as SCCP 7960 devices in Cisco Unified CallManager.

Figure 3-13 shows an excerpt of the SCCP Provider page. Table 3-13 lists the basic SCCP parameters; the screen also includes an extensive set of advanced parameters, which should not require modification.

Figure 3-14 SCCP Provider Page

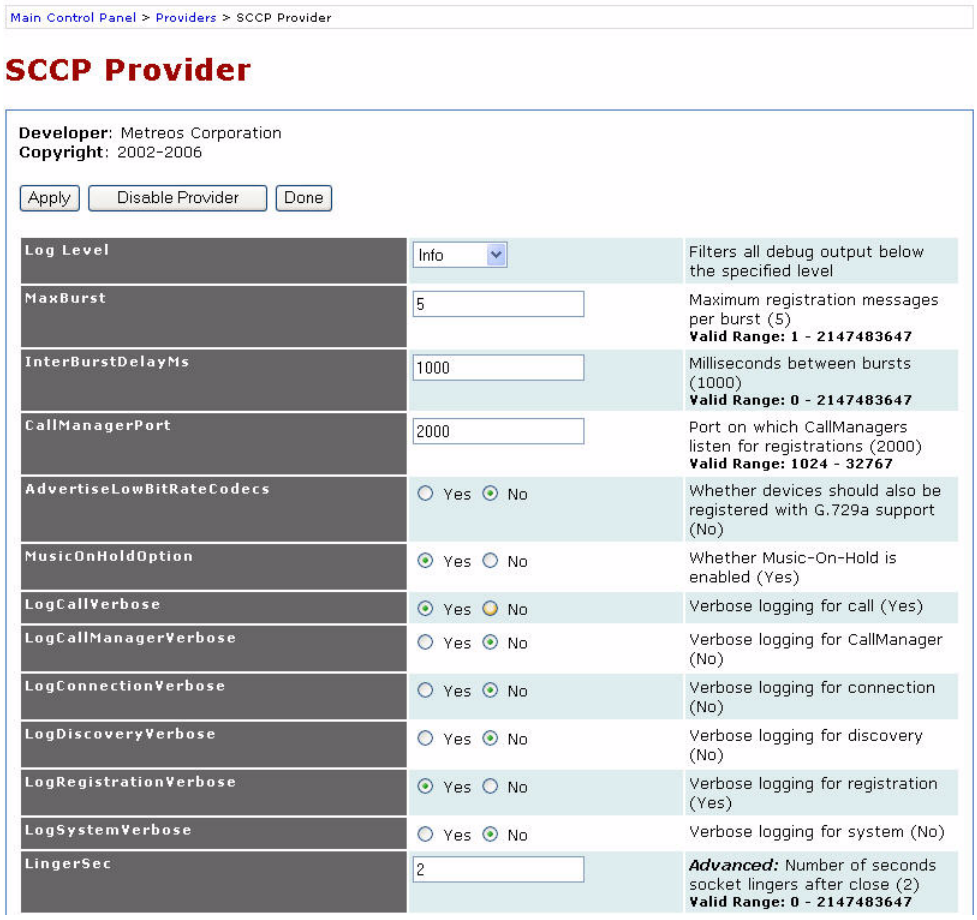


Table 3-13 SCCP Provider Parameters

Field	Description
Log Level	Filter for all debug output (below the specified level)
MaxBurst	Maximum registration messages per burst (5) (valid range: 1 - 2147483647)
InterBurstDelayMs	Milliseconds between bursts (1000) (valid range: 0 - 2147483647)
CallManagerPort	Port on which Cisco Unified CallManagers listen for registrations (2000) (valid range: 1024 - 32767)
AdvertiseLowBitRateCodecs	Indication of whether devices should also be registered with G.729a support (No)
MusicOnHoldOption	Indication of whether Music-On-Hold is enabled
LogCallVerbose	Verbose logging for call (Yes)
LogCallManagerVerbose	Verbose logging for CallManager (No)
LogConnectionVerbose	Verbose logging for connection (No)
LogDiscoveryVerbose	Verbose logging for discovery (No)

Table 3-13 SCCP Provider Parameters (continued)

Field	Description
LogRegistrationVerbose	Verbose logging for registration (Yes)
LogSystemVerbose	Verbose logging for system (No)

SIP Provider

The SIP provider uses the SIP protocol to create, receive, and control IP telephony calls between Cisco Unified CallManager nodes. The SIP provider either behaves as a SIP trunk or registers as SIP 7961G-GE devices in Cisco Unified CallManager.

Figure 3-15 shows the SIP Provider page, and Table 3-14 lists parameters.

Figure 3-15 SIP Provider Page

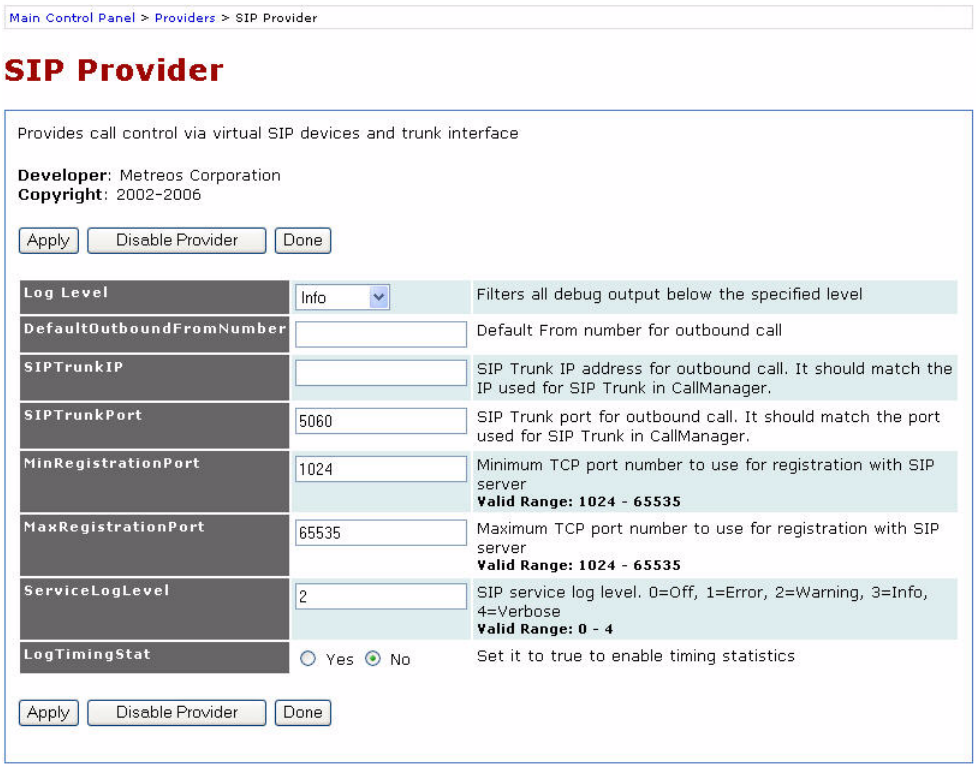


Table 3-14 SIP Provider Parameters

Field	Description
Log Level	Filter for all debug output (below the specified level)
DefaultOutboundFromNumber	Default From number for outbound call
SIPTrunkIP	SIP Trunk IP address for outbound call (should match the IP used for SIP Trunk in CallManager)

Table 3-14 SIP Provider Parameters (continued)

Field	Description
SIPTrunkPort	SIP Trunk port for outbound call (should match the port used for SIP Trunk in CallManager)
MinRegistrationPort	Minimum TCP port number to use for registration with SIP server (valid range: 1024 - 65535)
MaxRegistrationPort	Maximum TCP port number to use for registration with SIP server (valid range: 1024 - 65535)
ServiceLogLevel	SIP service log level (0=Off, 1=Error, 2=Warning, 3=Info, 4=Verbose, valid range: 0 - 4)
LogTimingStat	Timing statistics (enabled when set to true)

Timer Provider

The Timer provider makes timers available for use by applications. It does not communicate with any other system.

Click the Timer provider link to configure the Timer Provider. Figure 3-16 shows the Timer Provider page, and Table 3-15 lists parameters.

Figure 3-16 Timer Provider Page

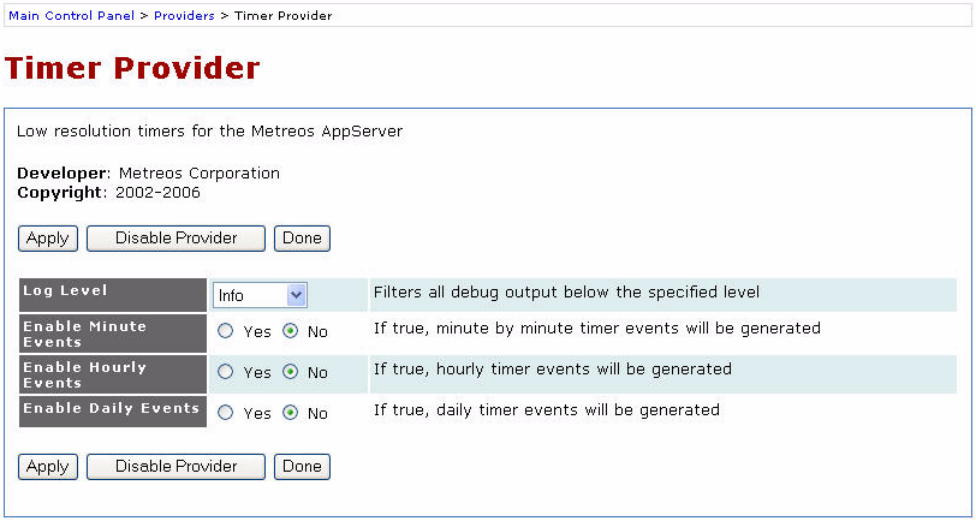


Table 3-15 Timer Provider Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Enable Minute Events	Field in which to enable minute by minute timer events (enabled when set to true)

Table 3-15 Timer Provider Parameters (continued)

Field	Description
Enable Hour Events	Field in which to enable hourly timer events (enabled when set to true)
Enable Daily Events	Field in which to enable daily timer events will be generated (enabled when set to true)

Telephony Servers

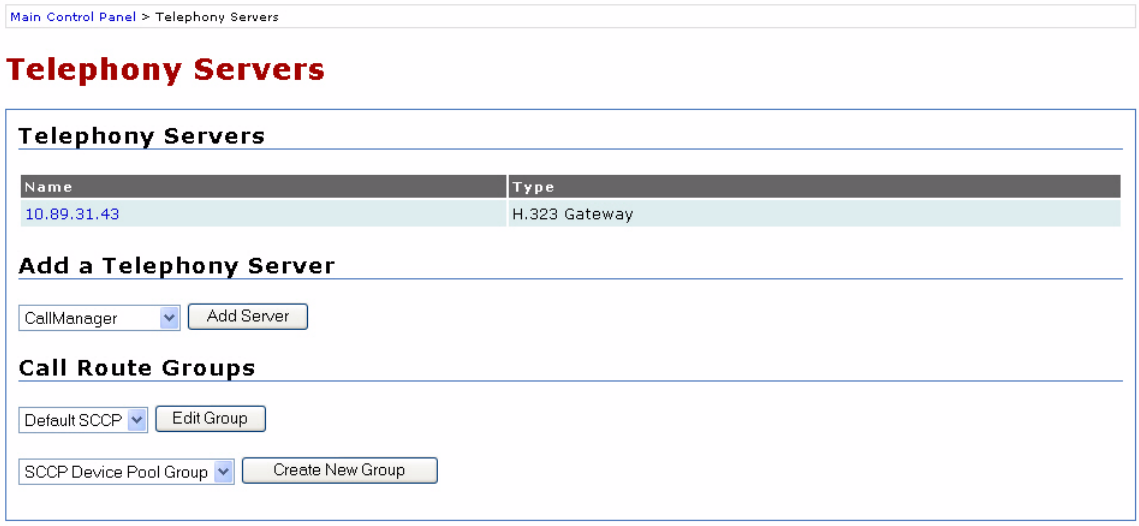
Every IP telephony system must contain at least one telephony server. The management console provides a telephony server configuration page for adding and configuring telephony servers and devices on those servers. When adding a telephony server, however, all of its devices must be associated with one or more call route groups.

Just as a media server group functions as a container for media servers, a call route group functions as a container for telephony devices. Each telephony device must belong to one or more groups.

Note Creating a call route group is optional; the system provides a default call route group to be used if multiple groups are not needed.

From the main Main Control Panel, click Telephony Servers to open the Telephony Servers page (Figure 3-17).

Figure 3-17 Telephony Servers Page



The application server currently supports these call control protocols:

- H.323
- CTI
- SCCP
- SIP

It also supports these types of telephony servers:

- H.323 gateways—Telephony servers, which are used exclusively with H.323.
- CallManager—Multipurpose telephony server devices supporting SCCP and CTI in the Cisco Unified system.
- Cisco SIP domain—Defines a SIP interface into Cisco Unified CallManager. By creating a Cisco SIP domain, you can use SIP trunks and SIP devices that the Cisco Unified Application Server creates in Cisco Unified CallManager.
- IETF SIP domain—Defines a telephony server that supports IETF-specific SIP.

Creating H.323 Call Route Groups and Gateways

This section describes how to create and configure H.323 call route groups and gateways. If a call route group other than the default is required, you can create a new H.323 call route group using this procedure.

To add a new call route group, follow these steps:

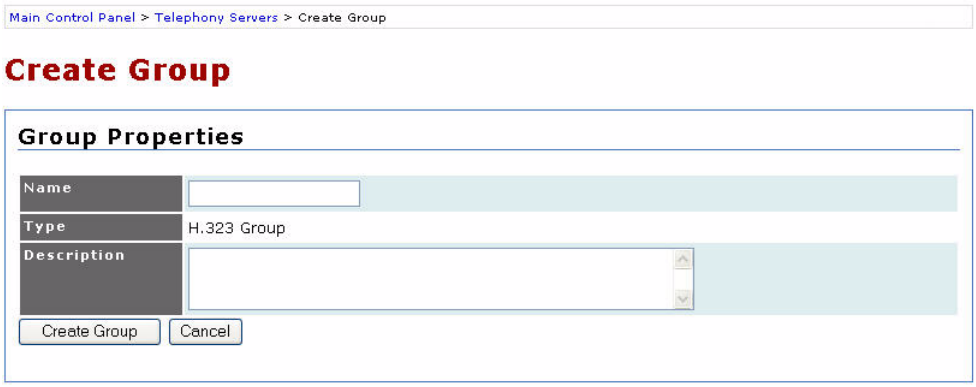
Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Select **H.323 Group** from the Create New Group pull-down list.

Step 3 Click **Create New Group**.

Figure 3-18 Configuring a New H.323 Telephony Group



Step 4 Enter the name of the group in the Name field.

Step 5 Enter a description in the Description field.

Step 6 To specify a previously created failover group, select the group from the Failover Group drop-down list.

Step 7 Select **Create Group**.

Before you can add H.323 telephony server to a group, you must create an H.323 gateway. Because H.323 does not require static configuration of devices, the gateway is added to a call route group. All logical devices created during runtime will automatically be part of that same group.

To create a H.323 Gateway, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Select **H.323 Gateway** from the Add a Telephony Server pull-down list.

Step 3 Click **Add Server**.

Step 4 Configure settings as described in Table 3-16.

Step 5 Click **Add H.323 Gateway** to create the gateway.

Table 3-16 H.323 Gateway Parameters

Field	Description
Name	Name of gateway
Description	Information to identify the gateway
IP address	IP address of gateway
Add to Group	Group to which gateway is assigned

Creating CTI Telephony Devices

Computer Telephony Integration (CTI), unlike H.323, is an IP telephony protocol based on line-oriented telephony devices. This section describes how to set up and administer CTI ports and route points that are configured on a CTI Manager. These properties apply to CTI devices:

- A CTI route point is a group unto itself.
- CTI ports are grouped into device pools.
- CTI ports and route points must each have at least one CTI manager associated with them.
- Call route groups should contain exactly one route point or one device pool. The application server does not allow a call route group containing a combination of route points and device pools.
- CTI route points and device pools are contained within a CTI Manager and are associated with CTI Groups.

These procedures describe how to create:

- CTI Groups
- CTI Managers
  - CTI route points
  - CTI device pools

To create a CTI route group, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Select **CTI Server Group** from the Create New Group drop-down list.

Step 3 Click **Create New Group**.

Step 4 Enter the name of the group in the Name field.

Step 5 Enter a description in the Description field.

Step 6 To specify a previously created failover group, select the group from the Failover Group drop-down list.

Step 7 Click **Create Group**.

Cisco Unified CTI clusters are known as Cisco Unified CallManager clusters. You can create a Cisco Unified CallManager cluster and associate it with the new group.

To add a Cisco Unified CallManager cluster, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Select **CallManager** from the Add Server drop-down list.

Step 3 Click **Add Server**.

Step 4 Configure settings as described in Table 3-17.

Step 5 Click **Create CallManager Cluster**.

Table 3-17 Cisco Unified CallManager Parameters

Field	Description
Name	Name to identify the server
Version	Cisco Unified CallManager version **Note** The Application Environment supports 3.3, 4.0, and 4.1. Enter only the first two digits of the version number (example: 4.0, not 4.0.1). If the gateway is not part of a CallManager installation, enter 1.0.
Publisher IP	IP address of the publisher of the Cisco Unified CallManager cluster
Publisher Admin Username	Administrator user name for the publisher
Publisher Admin Password	Password for the publisher
Retype Publisher Admin Password	Password verification for the publisher
SNMP Community	SNMP community string for the publisher
Description	Text to describe the publisher

To create a CTI manager, follow these steps:

Procedure

Step 1 On the Telephony Servers page, click the underlined name of the server to open the server configuration page.

Step 2 Scroll down and click **Add CTI Manager**.

Step 3 Enter the manager name in the Name field.

Step 4 Enter the IP address in the IP Address field.

Step 5 Click **Add CTI Manager**.

You can now create devices.

To create a CTI device pool, follow these steps:

Procedure

Step 1 On the Telephony Servers page, click the underlined name of the server to open the server configuration page.

Step 2 Scroll down and click **Create CTI Device Pool**.

Step 3 Configure values as described in Table 3-18.

Step 4 Click **Create CTI Device Pool**.

Table 3-18 Device Pool Parameters

Field	Description
Name	Name of the pool (enter in Name field)
How many devices to register?	Valid range: 1 - 9,999
Device Name Prefix	String used to construct the device names in conjunction with the number of devices registered. Format is Device Name Prefix + Device Count
Primary CTI Manager	Primary CTI Manager for CTI device pool
Secondary CTI Manager	Secondary CTI Manager for CTI device pool
Username	Username to allow monitoring of CTI device pool
Password	Password for monitoring the CTI device pool (must reenter to verify)
Add To Group	Call route group selected for this device pool

To create a CTI route point, follow these steps:

Procedure

Step 1 On the Telephony Servers page, click the underlined name of the server to open the server configuration page.

Step 2 Scroll down and **Create CTI Route Point**.

Step 3 Configure values as described in Table 3-19.

Step 4 Click **Create CTI Route Point**.

Table 3-19 CTI Route Point Parameters

Field	Description
Name	Name of the pool (enter in Name field)
Device Name	Device name of the CTI route point as created in Cisco Unified CallManager (name is case-sensitive)
Primary CTI Manager	Primary CTI Manager for CTI device pool
Secondary CTI Manager	Secondary CTI Manager for CTI device pool
Username	Username to allow monitoring of CTI device pool
Password	Password for monitoring CTI device pool (must reenter to verify)
Add To Group	Call route group selected for this device pool

Click any of the View or Edit buttons associated with the devices to view or edit them.

Configuring SCCP Devices

For applications that require the use of SCCP devices, there must be at least one SCCP device pool configured to contain SCCP devices.

To add a subscriber to Cisco Unified CallManager, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Click the underlined name of the telephony server to be added as an SCCP subscriber.

Step 3 Click **Add Subscriber**.

Step 4 Enter the subscriber Name in the Name field.

Step 5 Enter the Subscriber IP address in the IP Address field.

Step 6 Click **Add Subscriber**.

To create a device pool on the subscriber created to contain SCCP devices, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Telephony Servers**.

Step 2 Click the underlined name of the telephony server.

Step 3 Click **Create SCCP Device Pool** in the SCCP Device Pools section.

Step 4 Configure settings as described in Table 3-20.

Step 5 Click **Create Device Pool**.

Table 3-20 Device Pool Parameters

Field	Description
Name	Name of the pool (enter in Name field)
Device Name	Text used to used to construct the device names of SCCP devices in conjunction with the number of devices registered, in the form device name prefix + device count
Primary CTI Manager	Primary CTI Manager for CTI device pool
Secondary CTI Manager	Secondary CTI Manager for CTI device pool
Username	Username to allow monitoring of CTI device pool
Password	Password for monitoring CTI device pool (must reenter to verify)
Add To Group	Call route group selected for this device pool

Configuring System Parameters

The System group contains links to these Cisco Unified Application Environment configuration pages.

- Service Control
- SSL Management
- Redundancy Setup
- Applications

Service Control

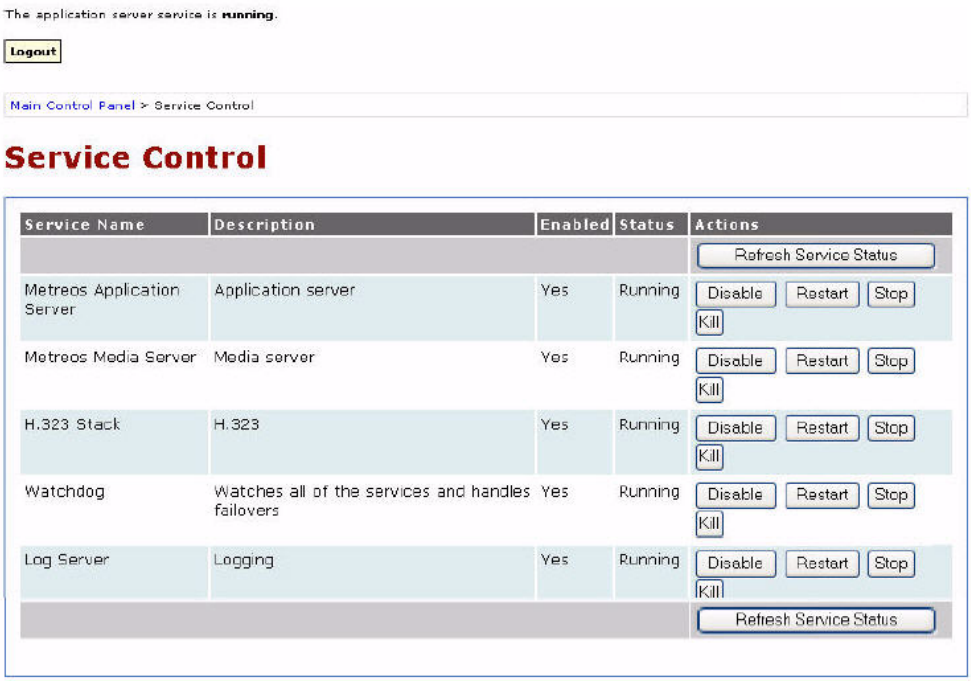
The Service Control page is used to enable, disable, stop, restart, or kill services that run on the application server. Under normal circumstances, it should not be necessary to perform these functions; these functions are required only in these instances:

- You have modified configuration parameters using the management console, and a message has indicated that you must restart a particular service for the configuration change to take effect.
- A service is not functioning properly.
- A Cisco support representative has asked you to restart a service to help debug an issue.

Note Services require differing amounts of time to restart. The media engine and application server can take approximate one minute to start or stop.

From the Main Control Panel, open the Service Control page (Figure 3-19) to show the services that are currently running and to enable, disable, start, restart, or stop the services.

Figure 3-19 Service Control Page



The following information is presented for each service:

- Service Name—Name of service
- Description—Explanation of service
- Enabled—Indication of whether the service is active
- Status:
  - Running—Service is available
  - Stop Pending—Service is shutting down
  - Stopped—Service is unavailable
  - Start Pending—Service is starting up
  - Unknown—Status is unknown
- Actions:
  - Disable—Make service unavailable (disallows automatic start at reboot)
  - Restart—Stop and restart the service
  - Stop—Make service unavailable
  - Kill—Stop the service
  - Enable—Allow automatic start at reboot
  - Start — Make service available

An enabled service automatically starts when the system is rebooted; a disabled service does not. When a service is disabled, the system automatically stops it.

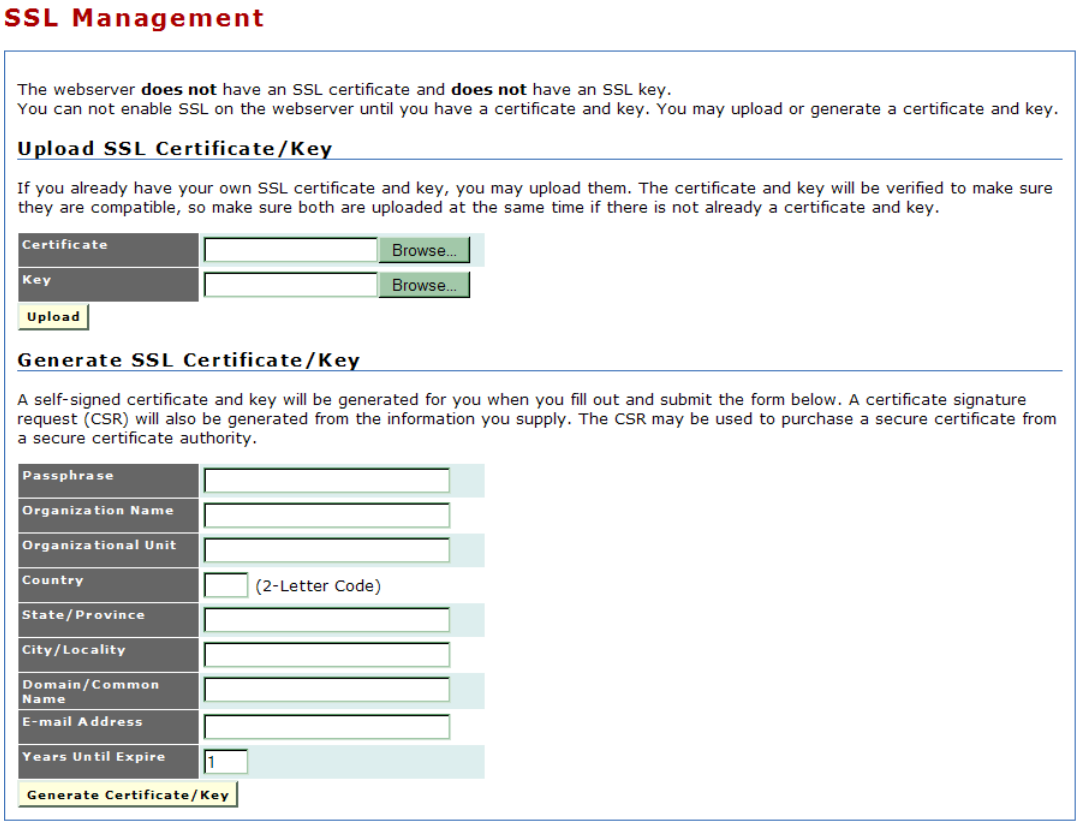
To perform an action on a service, click the desired button to the right of the action.

SSL Management

The management console web server does not have an SSL certificate or SSL key. If you need to use HTTPS (HTTP-over-SSL) instead of HTTP for management console access, then you must supply a security certificate and key. Open the SSL Management page (Figure 3-20) to manage SSL certificates and keys.

If you already have your own SSL certificate and key, they are verified upon upload to make sure that they are compatible. Make sure you upload them at the same time.

Figure 3-20 SSL Management Page



To upload an SSL certificate and key, follow these steps:

Procedure

Step 1 Open the SSL Management page.

Step 2 Click **Browse** and highlight the certificate file, then click **Open** to make the file available for uploading.

Step 3 Click **Browse** and highlight the key file, then click **Open** to make the file available for uploading.

Step 4 Click **Upload** to copy the certificate and key to the server.

To generate a new SSL certificate and key, follow these steps:

Procedure

Step 1 Open the SSL Management page.

Step 2 Enter the values as described in Table 3-21.

Step 3 Click **Generate Certificate/Key**.

Table 3-21 SSL Certificate Parameters

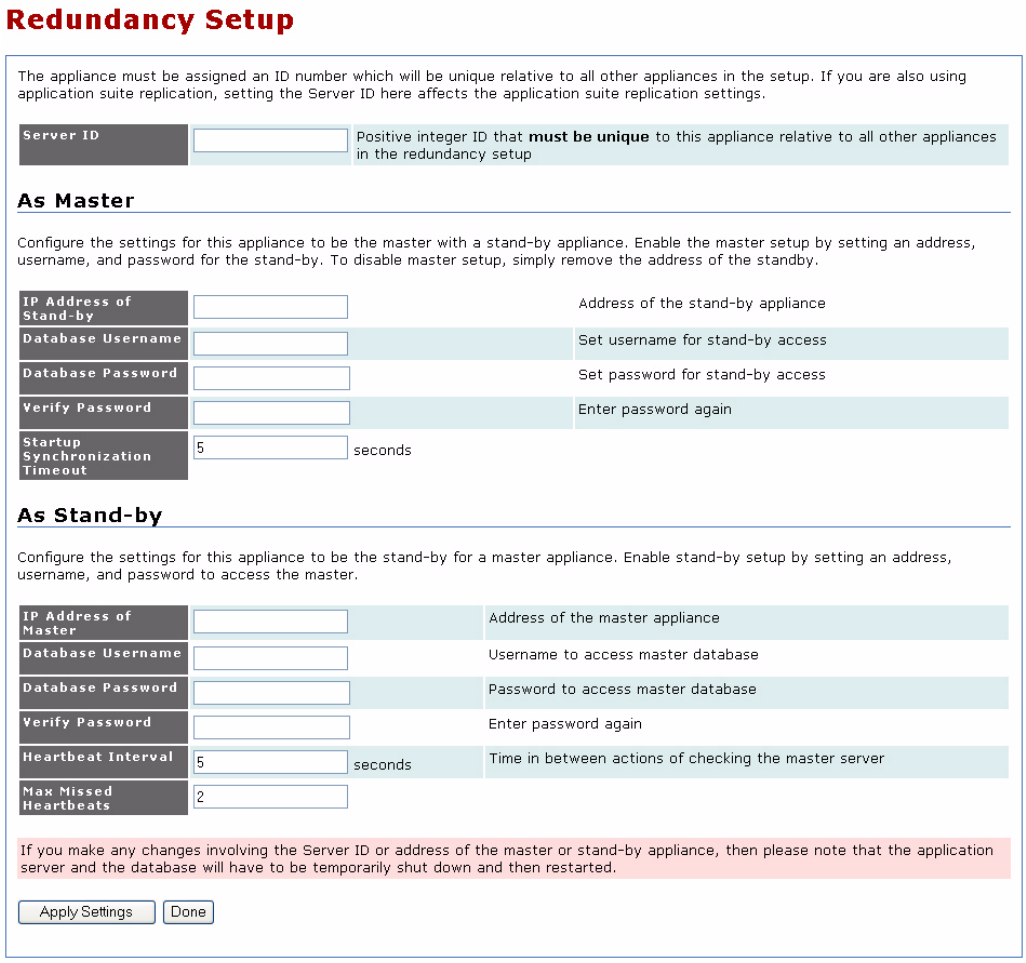
Field	Description
Passphrase	Code that is used to encrypt the private key
Organization Name	Name of the organization submitting the certificate request
Organizational Unit	Type of organization submitting the certificate request
Country	Standard two-letter country code
State/Province	Full name of the state or province where the server is located
City/Locality	City or other local jurisdiction where the server is located
Domain/Common Name	Host and domain name (for example, cisco.com)
Email Address	Contact email address
Years Till Expire	Number of years SSL certificate should be valid

Redundancy Setup

The Cisco Unified Application Environment supports redundant configurations for certain protocols, including Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and computer telephony integration (CTI). You can configure a master and stand-by application server. The stand-by server attempts to contact the master server every few seconds. If the specified number of attempts fails, the stand-by server takes over.

Use the Redundancy Setup page (Figure 3-21) to assign a unique ID number for each of the application servers and to configure the master and stand-by servers.

Figure 3-21 Redundancy Setup Page



To set up redundant operations, follow these steps:

Procedure

Step 1 From the Main Control Panel page, click **Redundancy Setup.**

Step 2 Enter a unique server ID to identify this server.

Step 3 Enter settings in the As Master fields as described in Table 3-22.

Step 4 Enter settings in the As Stand-by fields as described in Table 3-23.

Step 5 Click **Apply Settings**.

Step 6 Click **Done** to return to the Main Control Panel.

Table 3-22 Master Server Parameters

Field	Description
IP Address of Standby	IP address of stand-by server
Database Username	User name for access to stand-by server
Database Password	Password or access to stand-by server
Verify Password	Field in which to verify password
Startup Synchronization Timeout	Number of seconds after which the master server is considered unavailable

Table 3-23 Stand-by Server Parameters

Field	Description
IP Address of Master	IP address of stand-by server
Database Username	User name for access to stand-by server
Database Password	Password for access to the stand-by server
Verify Password	Field in which to verify password
Heartbeat Interval	Number of seconds stand-by server waits between attempts to contact the master server
Max Missed Heartbeats	Number of attempts after which the master server is considered unavailable

Note When you make changes that involve the Server ID or address of the master or stand-by appliance, you must shut down and restart the application server and database.

Configuring Environment Parameters

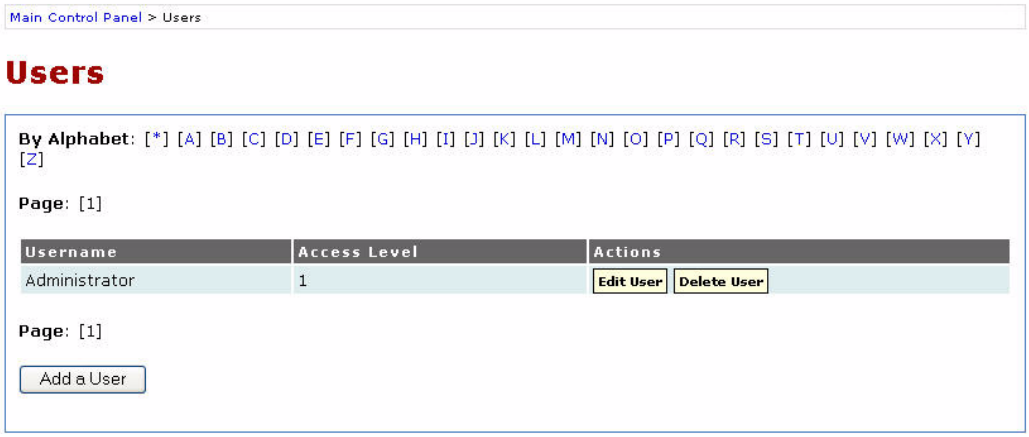
The Environment group contains links to the following Application Environment configuration pages:

- User Management
- Configuring Core Components
- Log Server
- Alarm Management

User Management

A user account is required for each user who will access the system. By creating a different account for each user, you can ensure that audit logs will accurately record each user's interactions with the system. From the Main Control Panel, open the Users page (Figure 3-22) to add users and to list existing users and their access levels.

Figure 3-22 Users Page



To add a user, follow these steps:

Procedure

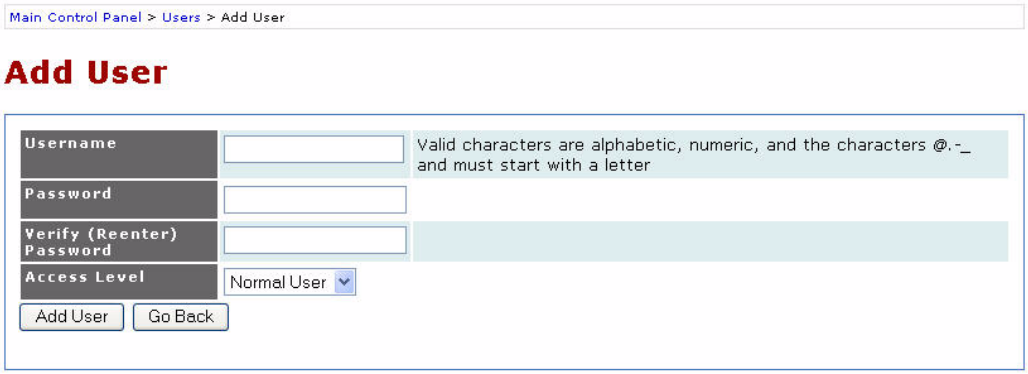
Step 1 From the Main Control Panel, click **User Management**.

Step 2 Click **Add a User**.

The Add User page opens.

Note From the Users page, you can list all users or click a letter to select the users whose names begin with that letter. Click the asterisk (*) next to the A in the alphabet string to return to the default view (all users).

Figure 3-23 Add User Page



Step 3 Enter the user name in the Username field.

Step 4 Enter a password in the Password field, then reenter it in the Verify (Reenter) Password field.

Step 5 Select Normal User or Administrator from the Access Level pull-down menu. Users assigned the Administrator role are allowed full access to the management console. Users assigned the Normal User role may manage only the following system components:

- Core Components
- Applications
- Media servers
- Providers
- Telephony Servers

Step 6 Click **Add User**.

Step 7 Click **Go Back** to return to the Users page.

To change a user password, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **User Management**.

Step 2 Click * to list all users, or click the first letter of the user name.

Step 3 Scroll to find the user name, and click the associated Edit User button.

The Edit User page opens.

Step 4 Enter and verify the new password.

Step 5 Click **Apply**.

Step 6 Click **Go Back** to return to the Users page.

To remove a user, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **User Management**.

Step 2 Click * to list all users, or click the first letter of the user name.

Step 3 Scroll to find the user name, and click the associated Delete User button.

Step 4 Click **Yes** to confirm.

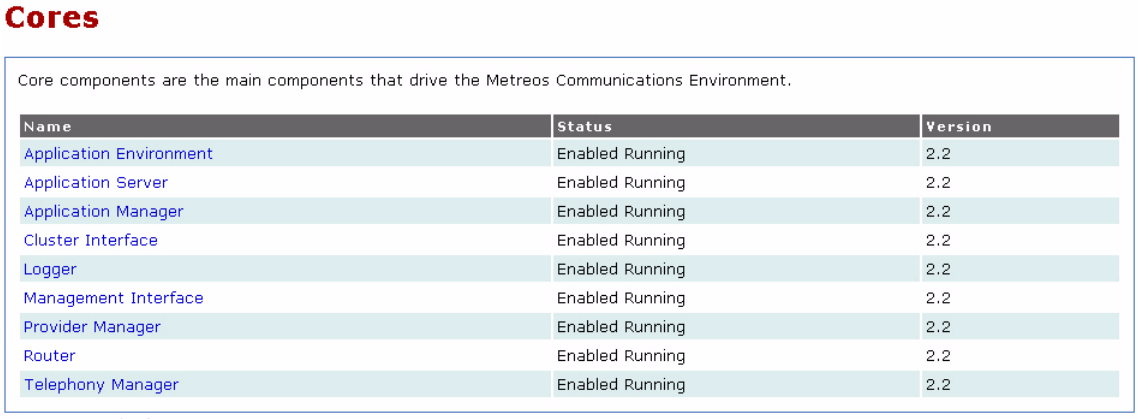
The user record is deleted.

Step 5 Click **Go Back** to return to the Users page.

Configuring Core Components

From the Main Control Panel, open the Cores page (Figure 3-24) to configure Cisco Unified Application Environment core components.

Figure 3-24 Cores Page



To configure core components, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Core Components**.

Step 2 Click the link for the desired application.

Step 3 Enter or select values as described in the following tables:

- Application Environment, Table 3-24
- Application Server, Table 3-25
- Application Manager, Table 3-26
- Cluster Interface, Table 3-27
- Logger, Table 3-28

- Management Interface, Table 3-29
- Provider Manager, Table 3-30
- Router, Table 3-31
- Telephony Manager, Table 3-32

Step 4 Click **Apply**.

Step 5 Click **Done** to return to the Cores page.

You can also invoke extensions from some of the core components pages that provide additional services.

Table 3-24 Application Environment Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
GC Interval	Time interval in seconds between garbage collection events (periodically, the system searches the runtime environment for objects that are no longer being used by the application, but have not released memory, then removes those objects and any associated resources)
Max Threads	Size of thread pool used for concurrent execution of actions

Table 3-25 Application Server Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Server Name	Identifier for application server

Table 3-26 Application Manager Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Debug Listen Port	Number of port on which debugger listens for debug commands

Table 3-27 Cluster Interface Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component

Table 3-28 Logger Parameters

Field	Description
DebugView Logger Level	Filter for Windows debug output (below specified level)
Console Logger Level	Filter for console debug output (below specified level)
Event Log Level	Filter for Windows debug output (below specified level)
File Logger Level	Filter for file debug output (below specified level)
Max File Log Lines	Maximum number of lines written to the log file before starting a new file (valid range: 100 - 1000000)
TCP Logger Level	Filter for remote console debug output (below specified level)
TCP Logger Port	Number of port on which TCP remote console logger remote server listens for connections
Log Server Sink Logger Level	Filter for log server debug output (below specified level)
Enable Logger	Queue diagnostics

Table 3-29 Management Interface Parameters

Field	Description
Log Level	Filter for all debug output (below specified level)
Management Port	Port on which the application server listens for commands from the management console and the Cisco Unified Application Designer.

Table 3-30 Provider Manager Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Shutdown Timeout	Length of time in milliseconds the system waits before forcing a shutdown
Startup Timeout	Length of time in milliseconds the system waits before considering a provider unloadable

Table 3-31 Router Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Default Action Timeout	Maximum length of time in milliseconds the system waits for a provider to respond to an action

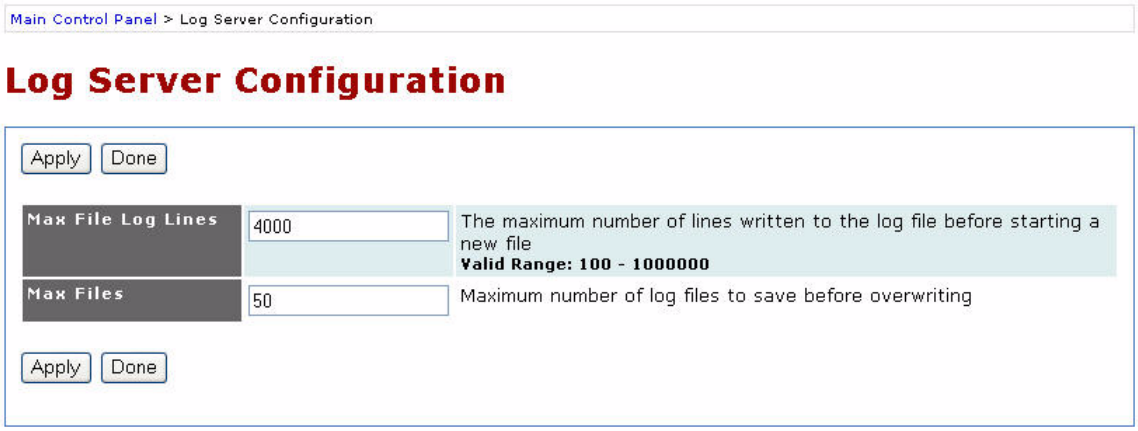
Table 3-32 Telephony Manager Parameters

Field	Description
Log Level	Type and amount of information the system writes to the log for each component
Enable Call/Connection Sandboxing	Indication of whether or not sandboxing is enabled (when enabled, the system clears any remaining calls and media connections while the controlling script exits.
Missing Enable Periodic Diagnostics	Indication of whether the Telephony Manager will occasionally output diagnostics about calls and performance.

Log Server

From the Main Control Panel, open the Log Server Configuration page (Figure 3-25) to specify the maximum size and number of log files.

Figure 3-25 Log Server Configuration Page



To configure the log server, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Log Server Configuration**.

Step 2 Enter or select values as described Table 3-33.

Step 3 Click **Apply**.

Step 4 Click **Done** to return to the Main Control Panel.

Table 3-33 Log Server Parameters

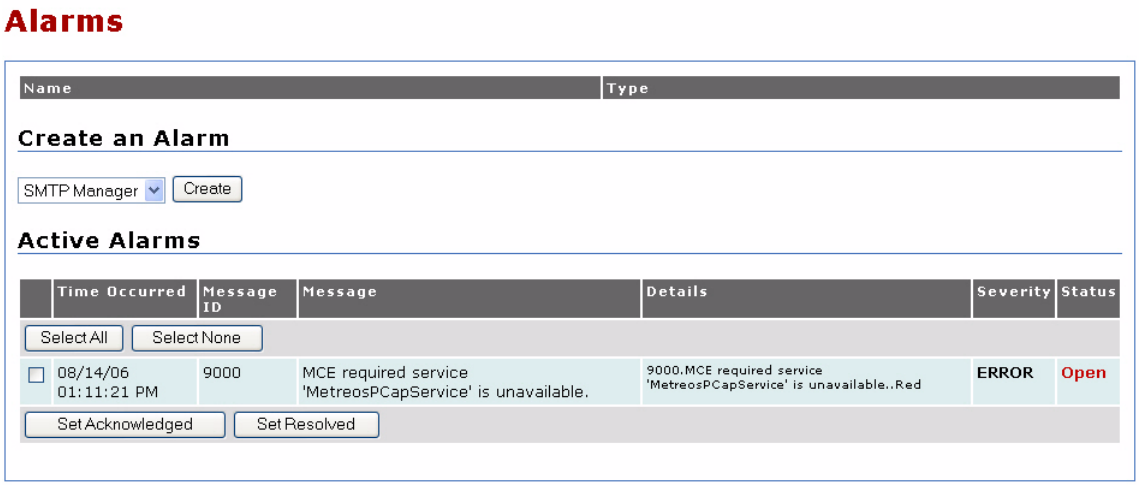
Field	Description
Max File Log Lines	Maximum number of lines written to the log file before starting a new file (valid range: 100 - 1000000)
Max Files	Maximum number of files to store in an individual log folder; when this limit is surpassed, older files are deleted to keep the total within the maximum

Alarm Management

Real-time alarm messages warn of critical system events, such as a server failing to start. Use the Alarms page to define the SMTP or SNMP manager that will receive the alarm messages.

From the Main Control Panel, open the Alarms page (Figure 3-26) to list current alarms and specify the destinations to receive alarm messages.

Figure 3-26 Alarms Page



To add new alarm destinations, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Alarm Management**.

Step 2 Choose **SMTP Manager** or **SNMP Manager**, then click **Create**.

Step 3 Configure settings for the selected option:

- SMTP Manager—Enter values as described in Table 3-34, then click **Add SMTP Manager**.
- SNMP Manager—Enter values as described in Table 3-35, then click **Add SNMP Manager**.

Table 3-34 SMTP Alarm Manager Parameters

Field	Description
Name	Name of alarm manager
Description	Description of alarm manager
Recipient	Email address to which to send alarm message
Sender	Email address from which to send alarm message
Server	IP address of SMTP server
Username	(Optional) User name for outbound SMTP authentication
Password	(Optional) Password for outbound SMTP authentication
Server Port	SMTP server port (default is 25)
Trigger Level	Event level that triggers alarm

Table 3-35 SNMP Alarm Manager Parameters

Field	Description
Name	Name of alarm manager
Description	Description of alarm manager
SNMP Manager	IP address of SNMP manager
Trigger Level	Event level that triggers alarm

CHAPTER 4

Configuring the Cisco Unified Media Engine

This chapter describes how to configure the Cisco Unified Media Engine from the management console and contains the following sections:

Uploading and Activating a Media Firmware License

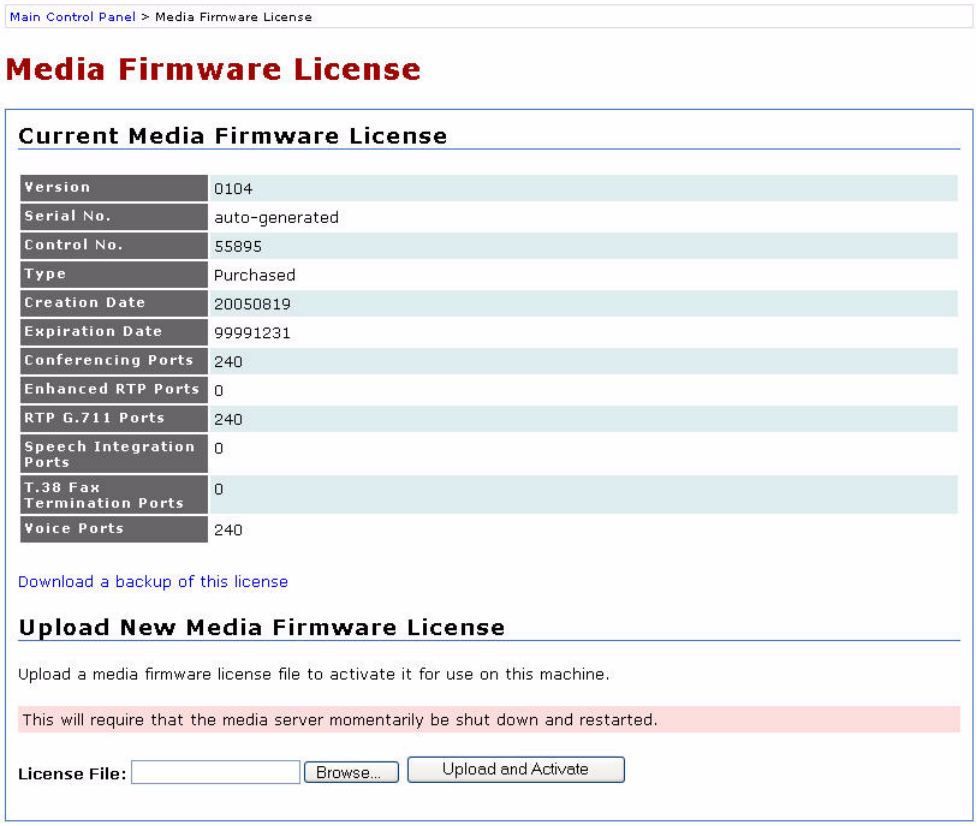
Each media engine requires a valid Host Media Processor (HMP) license. If an application requires media capabilities, then you must upload the appropriate license file when the media engine is first installed and configured.

Note If your organization has purchased a media engine license, go to cume-license-support@cisco.com to access the license file.

HMP Licenses are bound to a valid MAC address on a network adapter on the server. If the MAC address of the server changes (for example, if a network adaptor is replaced), then you must request a replacement license for the new MAC address.

Open the Media Firmware License page (Figure 4-1) to view information about the current license, download a backup of the current license, or upload a new license.

Figure 4-1 Media Firmware License Page



To upload a new license, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Service Control** and verify that the media server is running.

Step 2 From the Main Control Panel, click **Media Firmware License**.

Step 3 Click **Browse...** and highlight the file.

Step 4 Click **Open** to make the file available for uploading.

Step 5 Click **Upload and Activate**.

Step 6 Reboot the server.

To download a backup of the current license, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Firmware License**.

Step 2 Click **Download a backup of this license**.

Step 3 Click **Save** to specify a location for the license file.

Step 4 Click **Save**.

Uploading and Activating a Text-to-Speech License

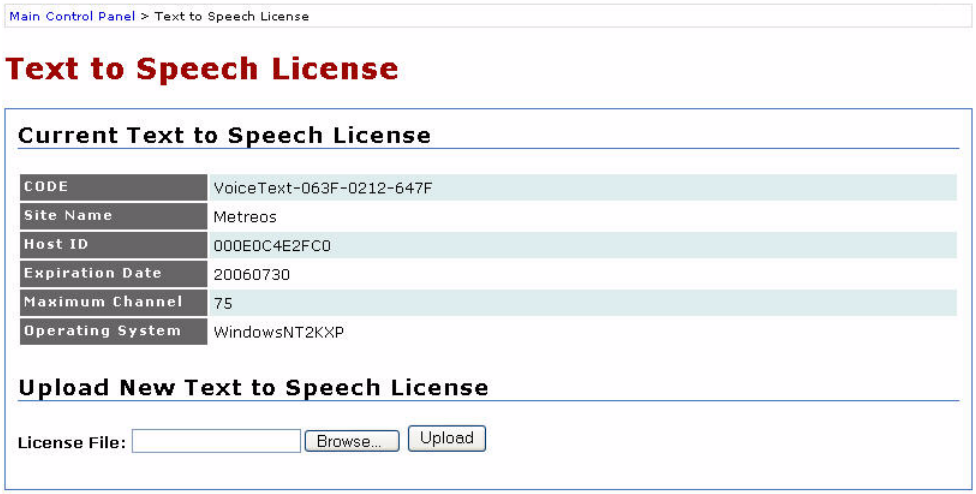
Each media engine requires a valid text-to-speech license if an application uses text-to-speech capabilities. If an application requires media capabilities, then you must upload the appropriate license file when the media engine is first installed and configured.

Note If your organization has purchased a text-to-speech license, go to cume-license-support@cisco.com to access the license file.

Text-to-speech licenses are bound to a valid MAC address on a network adapter on the server. If the MAC address of the server changes (for example, if a network adaptor is replaced), then you must request a replacement license for the new MAC address.

Open the Text to Speech License page (Figure 4-1) to view information about the current text-to-speech license or upload a new text-to-speech license.

Figure 4-2 Text to Speech License Page



To upload a new text-to-speech license, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Text to Speech License**.

Step 2 Click **Browse** and highlight the file.

Step 3 Click **Open** to make the file available for uploading.

Step 4 Click **Upload**.

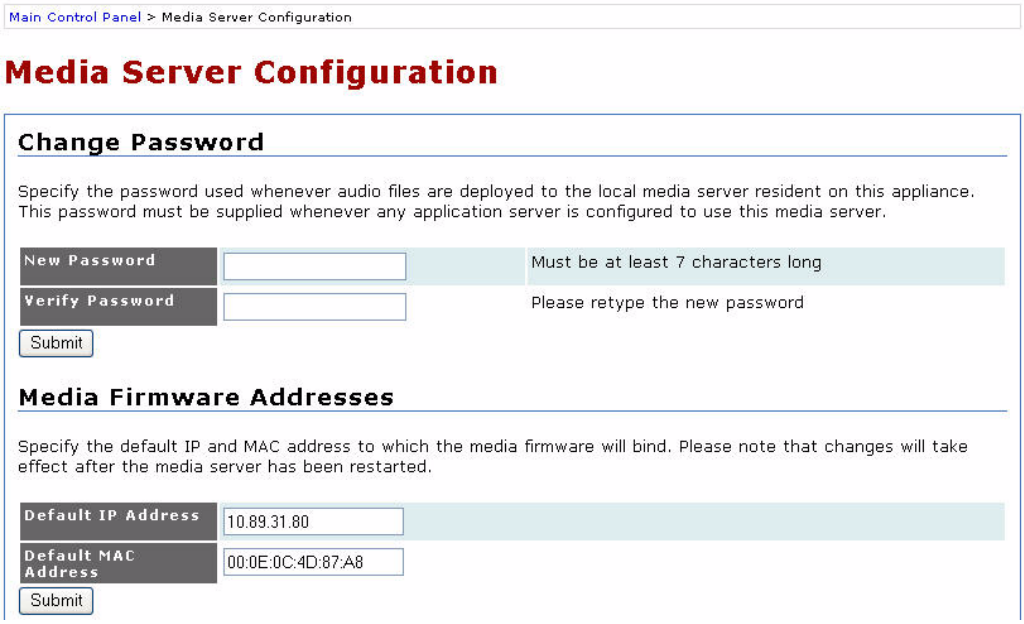
Configuring the Media Server Password and Firmware Address

To configure a media engine to work with the application server, you must assign the media server password that the application server will use to deploy media files to media engines when an application is installed. The password is checked each time you add a media server entry by way of the Media Servers page in the management console. If the media server password is changed while an application server is controlling a media engine, then the password must be updated in the management console; otherwise, the application may fail to execute.

You must also enter the default IP address and MAC address to which the media firmware will bind. Because the hardware running on the media engine can have more than one network adapter, these fields enable you to determine the network adapter to be used. If a different adaptor is needed, you should update both the IP address and MAC address fields. Changing the IP address causes Realtime Transfer Protocol (RTP) streams sent to the media engine to use the new IP address, enabling you to assign different functions to different network adaptors on the media engine.

From the Main Control Panel, open the Media Server Configuration page (Figure 4-3) to specify the media server password and media firmware addresses.

Figure 4-3 Media Server Configuration Page



To configure the media server settings, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Media Server Configuration**.

Step 2 To change the password, enter a new password in the New Password field, then reenter it in the Verify Password field.

Step 3 Click **Submit**.

Step 4 Enter or verify the default IP address and default MAC address to which the media firmware will bind. These changes are implemented when the media server is restarted.

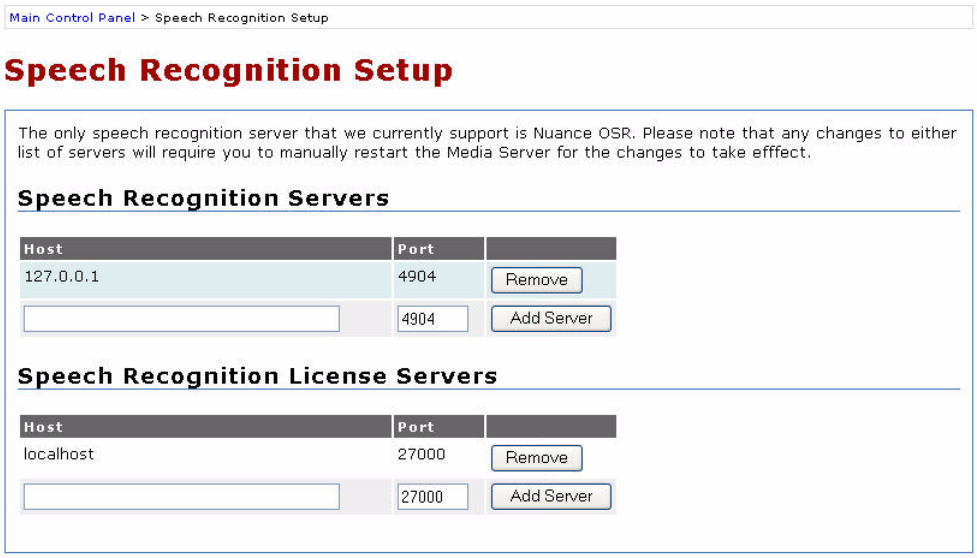
Step 5 Click **Submit**.

Configuring Speech Recognition Parameters

The Cisco Unified Application Environment supports the Nuance Open Speech Recognizer (Nuance OSR) for speech recognition. If an installed application requires speech recognition capabilities, then you must identify the Nuance OSR servers. Whenever the application performs a speech recognition operation, the identified servers will be used to perform the operation.

From the Main Control Panel, open the Speech Recognition Setup page (Figure 4-4) to specify speech recognition servers and licenses for the Nuance OSR.

Figure 4-4 Speech Recognition Setup Page



To configure the speech recognition settings, follow these steps:

Procedure

Step 1 From the Main Control Panel, click **Speech Recognition Setup**.

Step 2 Enter the host or IP address and port for the speech recognition server, then click **Add Server**.

Step 3 Enter the host or IP address and port for the speech recognition license server, then click **Add Server**.

Step 4 From the Main Control Panel, open the Service Control page, and restart the Media Server Service.

Note When you make changes that involve either list of servers, you must manually reset the media server.

To remove a speech recognition server, follow these steps:

Procedure

Step 1 On the Speech Recognition Setup page, click **Remove**.

Step 2 From the Main Control Panel, open the Service Control page, and restart the Media Server Service.

Note When you make changes that involve either list of servers, you must manually reset the media server.

CHAPTER 5

Maintaining the Cisco Unified Application Environment

This chapter describes how to view log files, use log files for troubleshooting, and back up and restore the Cisco Unified Application Server software.

This chapter includes these topics:

Viewing Log Information

The following management console logs provide diagnostic information:

- Server Logs—Information about server activity.
- Event Log—Information about system events (such as H.323 stack is unavailable).
- Audit Log—All Application Environment activity.

The Cisco Unified Application Environment supports log level filtering. The log level determines the amount of recorded detail about logged events (Table 5-1).

Table 5-1 Logging Levels

Log Level	Description
Off	No logging
Error	Only error messages written to log
Warning	Only warning and error messages written to log
Information	Warning, error, and terse event information messages written to the log
Verbose	Warning, error, and detailed event information messages to the log

Each log file is assigned a unique name, which consists of a date code and identifier, as in this server log example:

20060823-10261650.log

To view server logs, follow these steps:

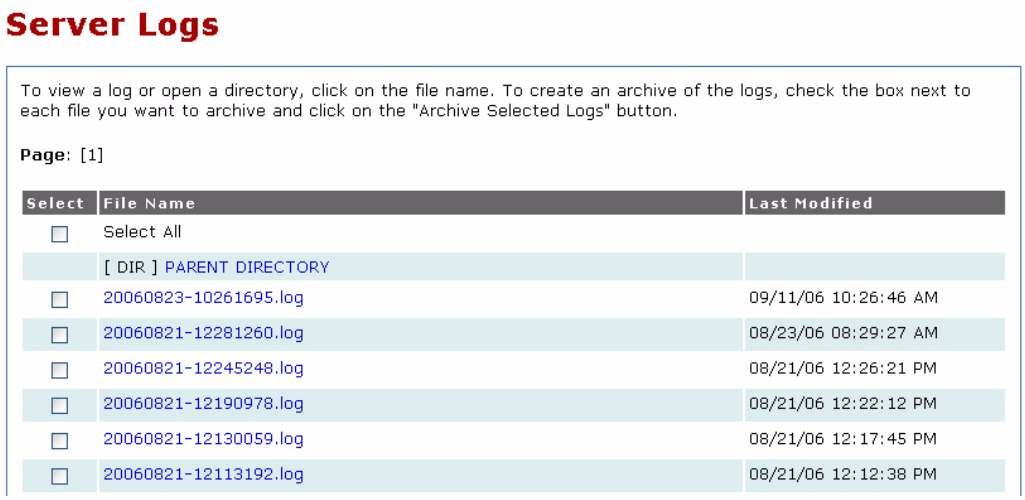
Procedure

Step 1 From the Main Control Panel page, click **Server Logs**.

Step 2 The Server Logs page opens.

Step 3 Click the underlined log name to display the list of log files for that server. Figure 5-1 shows an example excerpt from the AppServer log.

Figure 5-1 AppServer Log Files



Step 4 Click an underlined log file name to display the file contents. If the log list takes up multiple pages, use the links at the bottom of the page for navigation.

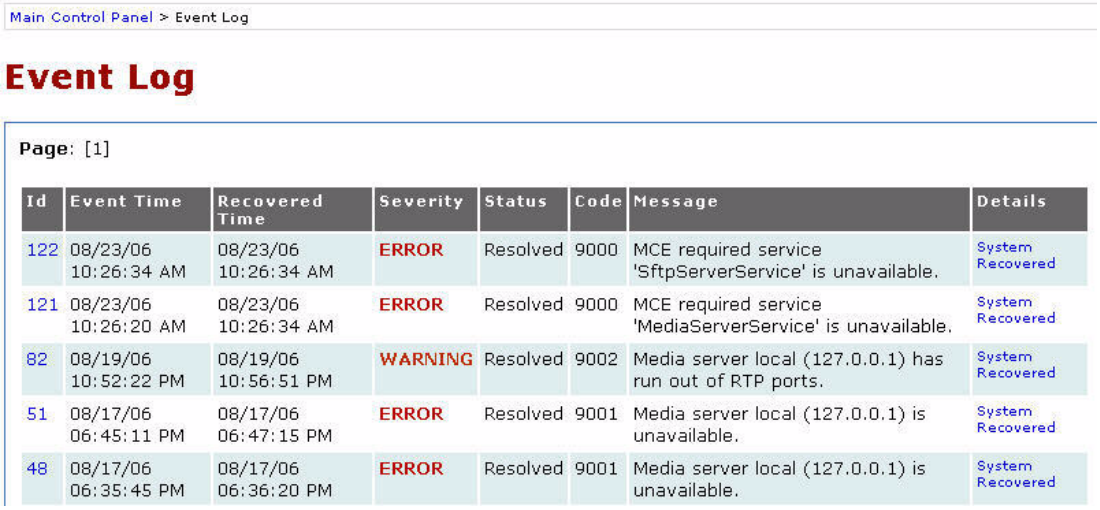
To view event or audit logs, follow these steps:

Procedure

Step 1 From the Main Control Panel page, click **Event Log** or **Audit Log**.

Step 2 The Event Log or Audit Log page opens. Figure 5-2 shows an example excerpt from the Event log.

Figure 5-2 Event Log



Step 3 To open the Details page for the event, click the underlined ID or Details link. If the log list takes up multiple pages, use the links at the bottom of the page for navigation.

You can archive or delete server log folders from the list of server logs or individual log files from the individual server log pages.

To archive log folders or files, follow these steps:

Procedure

Step 1 From the Main Control Panel page, click **Server Logs** to display the list of server logs.

Step 2 Select folders or files to archive:

- To archive log folders, use the checkboxes to select one or more log folders, or choose **Select All** to select all of the log folders.
- To archive log files, first click the underlined log name to open the log folder. Then use the checkboxes to select one or more log files, or choose **Select All** to select all of the log files.

Step 3 Click **Archive Selected Logs**.

The archive is created and a download page opens.

Step 4 Click **Download Archive File** or **Download Log Archive** download the files or folders to your computer.

To delete log files or the contents of log folders, follow these steps:

Note When you delete a log folder, the entire folder and all contents are deleted, provided that the service that uses the folder is stopped. If the service is running when the folder delete occurs, the folder and the currently open log remain. The folder will be automatically recreated when the first log is generated by the service.

Procedure

Step 1 From the Main Control Panel page, click **Server Logs** to display the list of server logs.

Step 2 Select folders or files to delete:

- To delete the contents of log folders, use the checkboxes to select one or more log folders, or choose **Select All** to select all of the log folders.
- To delete log files, first click the underlined log name to open the log folder. Then use the checkboxes to select one or more log files, or choose **Select All** to select all of the log files.

Step 3 Click **Delete Selected Logs**.

The logs are deleted. There is no confirmation message.

Troubleshooting

Follow these high level tasks when troubleshooting application server problems:

1. Check the AppServer log folder (choose **Server Logs > AppServer** from the Main Control Panel).
1. The default logging level for most components is Warning. To aid in diagnosing a problem, choose a higher logging level, such Verbose (see the "Configuring Core Components" section on page 3-38). The Verbose setting allows all inner components to log freely according to their own log level settings.

   Specifically, if the application server is not under heavy load, turn up the master log filter for the Log Server to Verbose (**Core Components > Logger > Log Server Sink Log Level = Verbose**). The Verbose setting allows all inner components to log freely according to their own log level setting. Also set the Telephony Manager component log level to Verbose (**Core Components > Telephony Manager > Log Level = Verbose**).
2. Run the application again to generate logs under the verbose conditions.

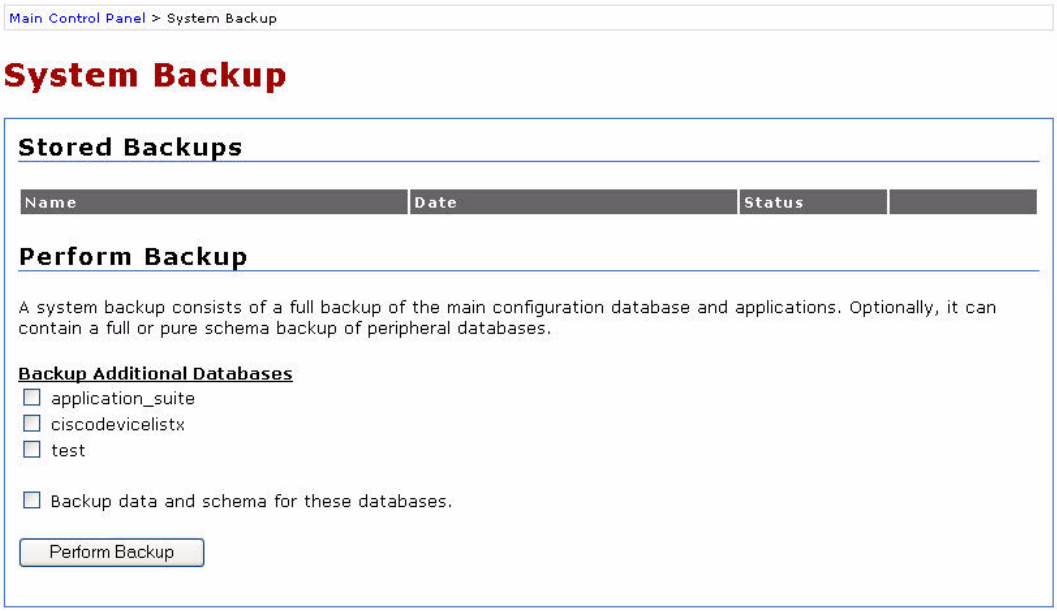
Backing Up the System

Use the system backup feature to take a snapshot of the current configuration settings in the management console, to save applications, and save application configurations. A system backup generates a tar file that can then be stored in a safe location.

Note A backup can only be used to restore a system of the same version.

Cisco recommends backing up systems regularly to prevent data loss in the unlikely event of system failure. Use the System Backup page (Figure 5-3) to perform backup operations. See the "Restoring the System" section on page 5-6 for instructions on restoring a previously backed up system.

Figure 5-3 System Backup Page



To perform system backups, follow these steps:

Procedure

Step 1 From the Main Control Panel page, click **System Backup.**

Step 2 Select the application databases to back up. To back up both the databases and database schema, select **Backup data and schema for these databases**.

Note The system database is automatically backed up during the backup process. If you do not need to back up the databases, leave the application databases unchecked.

Step 3 Click **Perform Backup**.

The Performing a Backup page opens.

Step 4 Click **Start**, and then click **Next Step**.

The system provides status updates while the backup is in progress.

Step 5 When the page indicates that the backup is complete, click **Finish**.

You can perform the following actions with a system backup:

- To download the backup file, click **Download**.
- To delete the backup file, click **Delete**.
- To view a history of all backups, click **All Backups**.

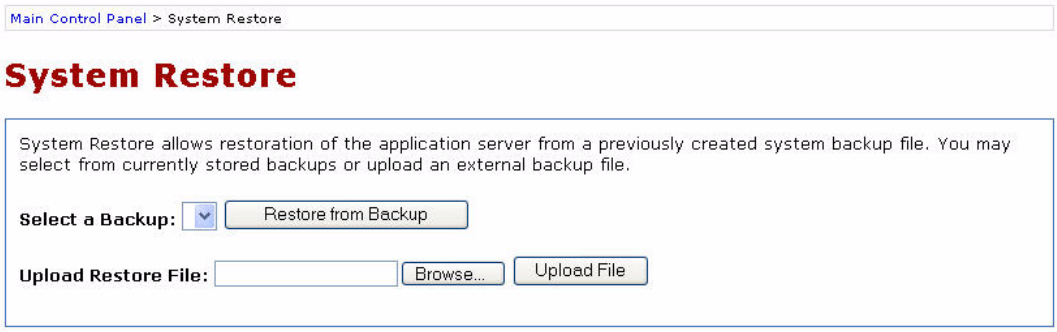
Restoring the System

Use the system restore feature to install and activate a previously-generated system backup file, as described in the "Backing Up the System" section on page 5-4.

Caution The configuration contained in the backup file overwrites the current configuration. Once started, the process cannot be stopped or undone.

Open the System Backup page (Figure 5-3) to restore system and database files that were previously backed up.

Figure 5-4 System Restore Page



To restore a previous backup, follow these steps:

Procedure

Step 1 From the Main Control Panel, click the **System Restore**.

Step 2 Perform either of the following actions:

- To restore from a previous backup that is stored on the server, select the back up, then click **Restore from Backup**.
- To restore from a local drive, click **Browse** button and highlight the file, and then click **Upload File**.

Reinitializing the Server

Use the two DVDs that are shipped with the MCS-7845H-1 server to re-image the system back to the factory settings.

One of the DVDs contains the base operating system, and the other contains the Cisco Unified Application Environment software. The Cisco Unified Application Environment DVD contains a readme.txt file in the root directory. Follow the instructions in this file to reinitialize the server.

After the server is reinitialized, you can use the System Restore feature to restore the server back to its previous backed up state. See the "Restoring the System" section on page 5-6.

A

C

D

E

F

H

I

J

L

M

N

P

R

S

T

U

V

W