Cisco HealthPresence Server Administration Guide

Version 2.0
October 31, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
http://www.cisco.com Tel: 408 526-4000

Support: 877-871-7255 or 512-340-3793
Web portal: https://ros.cisco.com/Portal
E-mail: healthpresence-support@cisco.com

Text Part Number: **OL-25943-01**

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco HealthPresence is intended for use by licensed healthcare professionals with those certain independent third party medical devices listed as compatible in the Cisco Health Presence Instructions for Use. The user is to refer to the third party instructions for use concerning any further information about the use of those certain medical devices. Cisco HealthPresence is not intended to perform real-time, active, or online patient monitoring, and does not transmit or display any real-time data that is intended to alert the user of alarms or other conditions that require immediate action or response. The user is advised that Cisco Systems makes no representations or warranties concerning jurisdictional requirements related to the licensed practice of medicine or healthcare using Cisco HealthPresence.

Cisco HealthPresence Server Administration Guide
© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Introduction

Revised: October 31, 2011, OL-25943-01

This introduction explains the audience and purpose of this guide. It provides an overview of the Cisco HealthPresence solution from the end user's (medical worker's) point of view, and then explains how to get started on the system. Finally, it summarizes the configuration and service features, which are explained in greater detail later in the guide.

These topics are included in this chapter:

- About This Service Guide
- A Quick Summary of the Cisco HealthPresence Solution
  - The Attendant Begins the Appointment
  - The Provider Joins In
  - The Examination Begins
  - The Appointment Ends
- Basic System Tasks
  - Logging In to the System
  - Changing Your Password
  - Logging Out of the System
  - Finding the Service Administration Version Numbers
  - Getting Into and Out of Desk-Top Mode
- Overview of the Administration and Service Section
  - Configuration
  - Verification Utilities
  - Runtime Statistics
  - Historical Statistics
  - Serviceability

About This Administration and Service Guide

This guide is for those who update, reconfigure, troubleshoot, or otherwise configure and service the Cisco HealthPresence™ system after it has been installed. These users may be the health facility's IT personnel or they may be Cisco engineers. They are experienced computer professionals who have had some training on the service applications for the Cisco HealthPresence™ device. They may be working from an Attendant Appliance, a Provider Appliance, or another computer connected to the Cisco HealthPresence application through IE 8.

A Quick Summary of the Cisco HealthPresence Solution

The Cisco HealthPresence solution allows a healthcare Provider (usually a physician) to examine a patient regardless of the physical location of the patient. For example, Providers can see images from an ear, nose, and throat (ENT) scope just as they would if they were in the room with the patient. A special camera zooms in to allow the physician to get close ups.

To see an example of the system in a clinical setting, refer to Figure 1-1. The remainder of this section provides a summary of a typical medical session. All of these functions are described in detail in the *Cisco HealthPresence System User Guide.*

Figure 1-1 The Cisco HealthPresence Attendant Station

The Attendant Begins the Appointment

Step 1 The Attendant gets the patient's height and weight, seats the patient at the Attendant station, and fills in the patient's personal data.

Step 2 The Attendant displays a list of Providers, and selects a Provider.

Step 3 The Attendant takes the patient's vitals, transfers the vitals to the system, and then alerts the Provider that this consultation can begin. This appointment appears on the Provider's *Ready Appointments* list.

The Provider Joins In

Step 4 The Provider comes into the Provider station, logs in, and sees a list of all of the "ready" appointments that have selected him or her as a Provider.

Step 5 The Provider clicks the appointment he or she wants to join. The appropriate appointment screen automatically displays.

The Examination Begins

Step 6 The Attendant shares the patient's vitals with the Provider.

The Provider can now see the patient's vitals.

Step 7 Both the Attendant and the Provider join the conference.

The patient and the Attendant can see the Provider on the screen at the Attendant station. The Provider can see the patient and the Attendant on the screen at the Provider station.

Step 8 The Attendant uses one or more medical devices to examine the patient, and sends the data to the Provider.

Step 9 The Provider evaluates the data, and communicates with the patient and the Attendant.

The Appointment Ends

Step 10 The Provider exits the appointment.

Step 11 The Attendant does any necessary post-appointment work, such as saving or printing the patient data.

Step 12 The Attendant ends the appointment.

Basic System Tasks

This section explains how you log in to the system and perform other elementary system tasks.

Logging In to the Cisco HealthPresence System

When your system was installed, a Windows short cut was added to the Favorites Bar (see Figure 1-2).This short cut enables you to go directly to the CHP Server Administration login screen (Figure 1-3) without entering a URL. After you log in, you see the Service Administration menus, which are shown in Figure 1-4. Each of these menus lists one or more administration or service functions that are summarized in the next section of this chapter, and described in detail throughout this manual.

To log in:

1. Click the CHP Server Administration Short Cut in the Favorites Bar (see Figure 1-2).

   You will see a screen similar to the one shown in Figure 1-3.
2. Type in username *chpoperator* and your *Password* in the boxes provided.
3. Click the **Login** button.

Figure 1-2 CHP Server Administration Short Cut in Favorites Bar

Figure 1-3 The Cisco HealthPresence Login Screen (CHP Operator)

Figure 1-4 The Server Administration Window

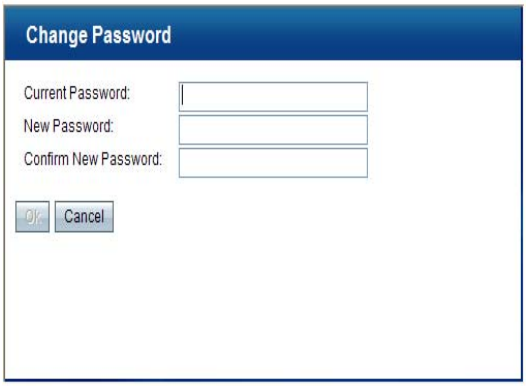
Changing Your Password

Figure 1-5 The Change Password Dialog Box

To change your password:

1. Click **Change Password** at the top right of the Server Administration window (shown in Figure 1-4 on page 1-4).

   You see a screen such as the one in Figure 1-5.
2. Fill in the old and new passwords in the boxes provided.
3. Click **OK**.



Logging Out of the System

To log out:

1. Click **Logout** at the top right of the Service Administration window (shown in Figure 1-4 on page 1-4).

   You see the confirmation message shown in Figure 1-6.
2. Click **Yes**.

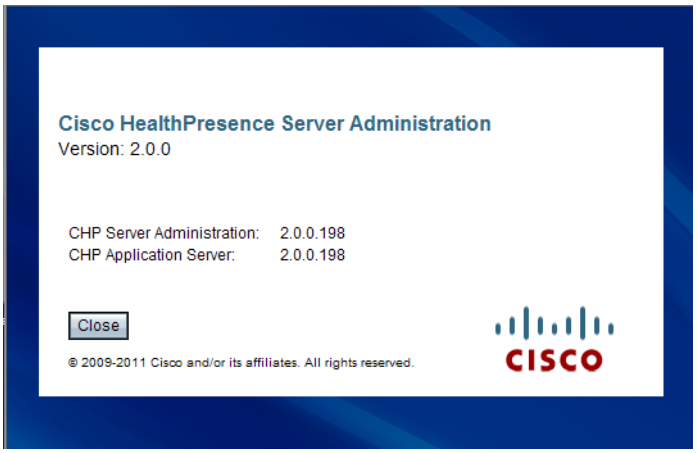
Figure 1-6 Logout Message

Finding the Application Server and Service Administration Version Numbers

To see the Cisco HealthPresence Application Server and Server Administration version numbers, click on the *About* selection in the upper right-hand corner of the Service Administration window (see Figure 1-4 on page 1-4). You will see a screen similar to the one shown in Figure 1-7.

The servers associated with your system will be listed here with their version numbers.

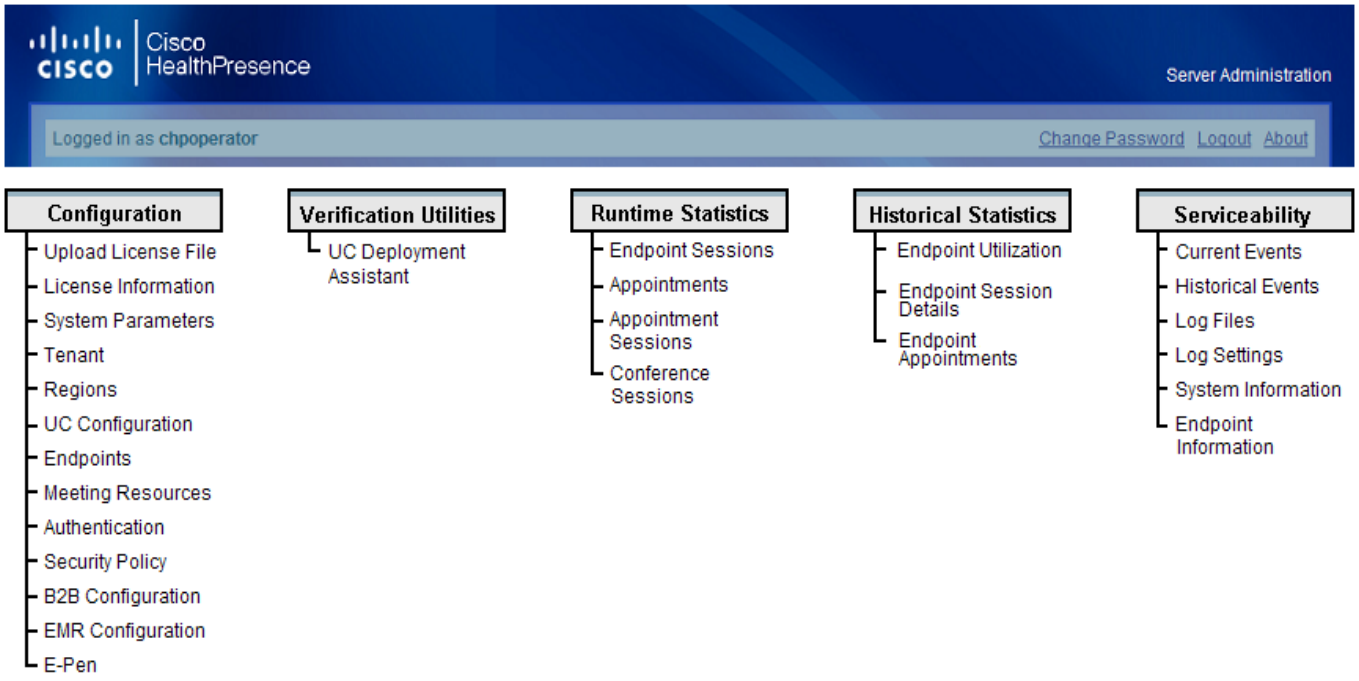
Figure 1-7 Server Administration Version Numbers



Overview of the Server Administration Section

This part of the chapter provides an overview of the administration and service section of the Cisco HealthPresence system. The five Server Administration menus are shown in Figure 1-8.

Figure 1-8 The Server Administration Menus



Quick Summary of the Configuration Tasks

The *Configuration* menu allows you to configure or reconfigure various aspects of the system. Many of these features will be configured at the time the system is installed, but can be adjusted as needed. For complete information, see Chapter 2, "The Configuration Tasks."

Quick Summary of the Verification Utilities

The *Verification Utilities* menu includes only one option (using the *UC Deployment Assistant* to create a bridge to test a recently configured multi-point bridge). It is not covered in this document because it is not required for most systems (it is only required when using Cisco hosting services) and it is also only required during the initial system installation.

Quick Summary of the Runtime Statistics Options

The *Runtime Statistics* menu allows you to see what is going on with the system at the current time. All of the information displayed on these screens is for sessions that are still active. For complete information, see Chapter 3, "The Runtime Statistics."

Quick Summary of the Historical Statistics Options

The Historical Statistics menu allows you to display information for activities that have already taken place. All of the information displayed on these screens is for sessions that have occurred in the past, and have been completed. For complete information, see Chapter 4, “The Historical Statistics.”

Quick Summary of the Serviceability Features

The Serviceability menu includes features that allow you to display information that can be useful for tracking active and past events, viewing detailed logs, and troubleshooting system problems. For complete information, see Chapter 5, “The Serviceability Options.”

CHAPTER 2

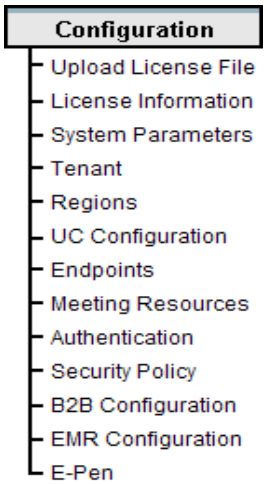
The Configuration Tasks

Revised: October 31, 2011, OL-25943-01

This chapter explains the tasks that you can do using the *Configuration* menu from the Cisco HealthPresence *Server Administration* window. The configuration screens allow you to configure various aspects of the Cisco HealthPresence Application Server (CHPAS). Many of these features will have been configured when this system was installed, but you have the option of altering the settings later, if your needs change.

These topics are included in this chapter:

- Working with License Files
  - Uploading License Files
  - Viewing License Information
- Working with System Parameters
- Working with Tenant Settings
  - Viewing Tenant Settings
  - Changing Tenant Settings
- Working with Regions
  - Displaying a List of Regions
  - Deleting a Region
  - Updating a Region
  - Adding a Region
- Configuring Unified Communications (UC)
  - Displaying Current UC Settings
  - Changing UC Settings
- Working with Endpoints
  - Displaying a List of Endpoints
  - Deleting Endpoints
  - Updating Endpoints
  - Adding Endpoints
- Working with Meeting Resources
  - Displaying a List of Meeting Resources
  - Deleting Meeting Resources
  - Updating Meeting Resources
  - Adding Meeting Resources
- Choosing the Authentication Type
  - Displaying the Authentication Settings
  - Changing the Authentication Settings
- Setting Security Policy
- Configuring B2B Settings
- Configuring for EMR
- Setting Up the E-Pen Feature



Working with License Files

The Cisco HealthPresence system can include the license files listed here. Every license file that applies to this installation should have already been copied to the computer you are working on.

- Server – Locks the application to a specific hardware machine (MAC address).
- Resource – There is one license and it controls the maximum number of endpoints.

Uploading License Files

To upload a license file from the computer that you are working on to the Cisco HealthPresence Application Server:

1. Click *Upload License File* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-1 on page 2-2.
2. Click the *Browse* button, and browse to the location where the license files were copied.
3. Select the file that you want to upload, and click the *Upload* button.
4. Repeat steps 1 and 2 for every license file that you want to upload.
5. To view the license files that you just uploaded, or license files that have already been uploaded, click on the name of the license file.

   The file will look something like the one shown in Figure 2-2 on page 2-3.

Note The uploaded license files will not take effect until you click **Restart.**

Figure 2-1 The Upload License File Screen

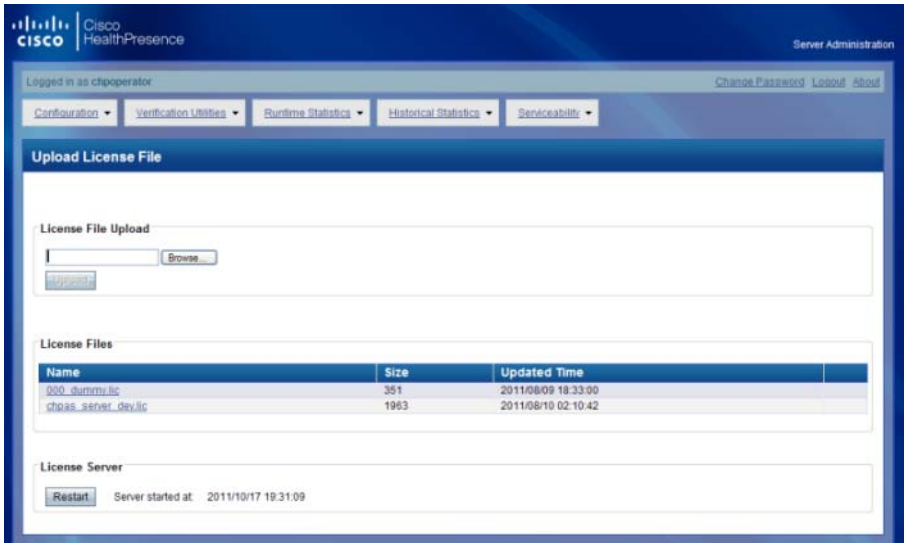
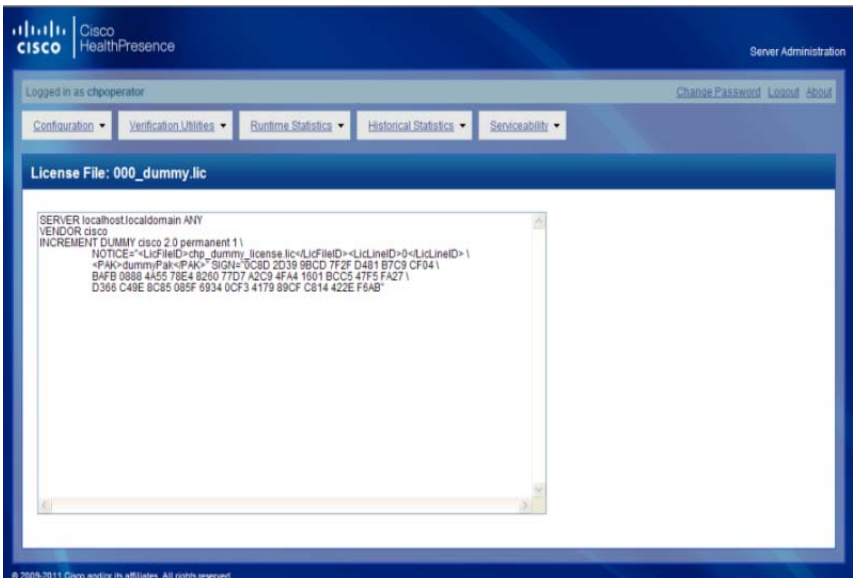
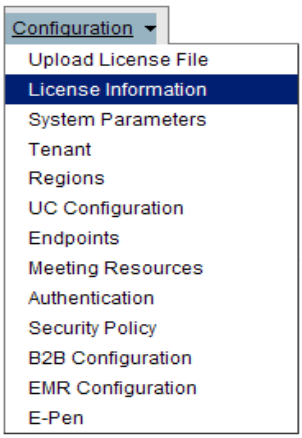


Figure 2-2 A Sample License File



Viewing License Information



To view information about the licenses that pertain to this system, click *License Information* on the *Configuration* menu.

The system displays a screen similar to the one shown in Figure 2-3.

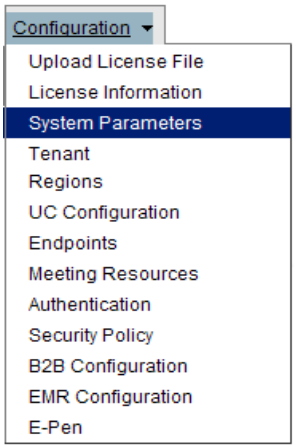
This screen lists the applicable system features by name and by "key," which is a shortened version of the name. The software version number and the expiration date, if any, are supplied.

This screen also lists resources belonging to this system by name and by key. Software version number and expiration date, if any, are provided. In addition, this table lists how many of each type of resource are allowed, and how many are currently in use.

Figure 2-3 The License Information/Details Screen

Working with System Parameters

System parameters are system-wide values that apply throughout the Cisco HealthPresence Data Center. These values were assigned when your system was installed, and, in most cases, should not be changed.



1. To display the existing system parameters, click *System Parameters* on the *Configuration* drop-down menu.

   The system displays a screen similar to the one shown in Figure 2-4.

2. If you need to change any of these values, type over whatever is in the field.

   The definitions for these fields are provided in Table 2-1 on page 2-6.

3. When you are finished, click the *Save* button at the bottom of the screen.

Figure 2-4 The System Parameters Screen

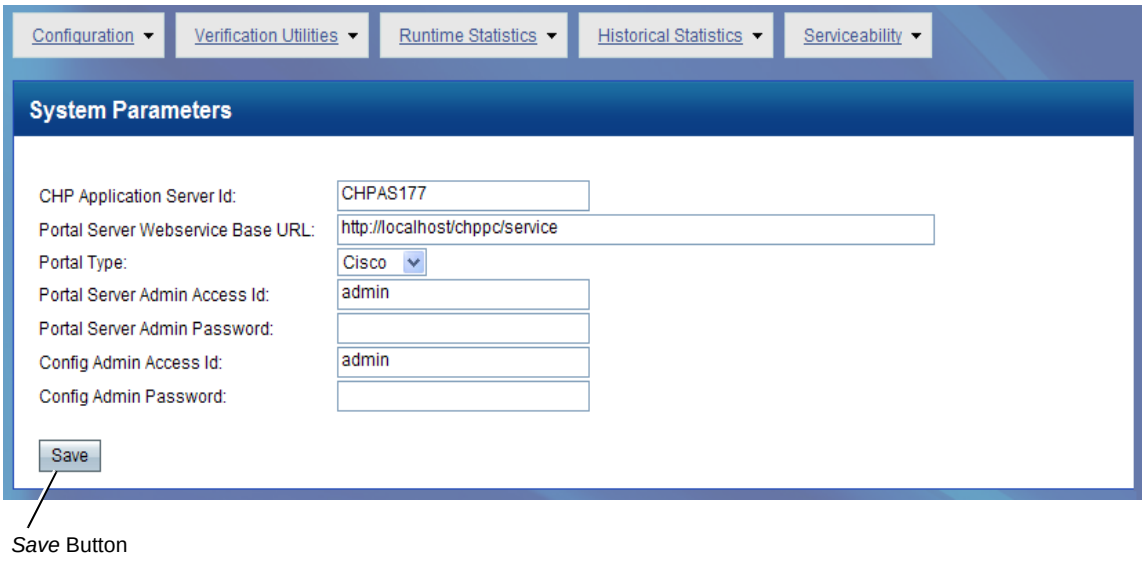


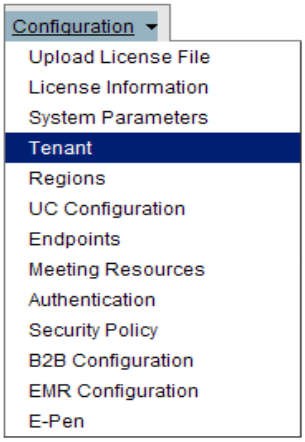
Table 2-1 Fields on System Parameters Screen

Field	Definition
CHP Application Server Id	A unique identification code using letters, numbers, dashes, or underscores. This ID must be unique among all of the businesses that use the same B2B Manager. Potential or future collaboration was considered when this ID was configured.
Portal Server Webservice Base URL	Where the Portal Server is running. Uses this format – http://localhost/chppc/service. If the portal type is Cisco, this field will be populated automatically.
Portal Type	The type of Portal. For Release 2.0, this must be Cisco.
Portal Server Admin Access Id	The identification code that enables the Portal server to talk to the Application server. (Not used for Release 2.0.)
Portal Server Admin Password	This is specified in the ID and password tab of the NIP under Portal Server Admin. (Not used for Release 2.0.)
Config Admin Access Id	The identification code that the CHP Admin Server uses to authenticate itself to the CHPAS for configuration operations.
Config Admin Password	The password that the CHP Admin Server uses to authenticate itself to the CHPAS for configuration operations.

Working with Tenant Settings

A tenant is a single instance of the Cisco HealthPresence Connect Server residing in its own virtual machine on a physical server.

Viewing Tenant Settings

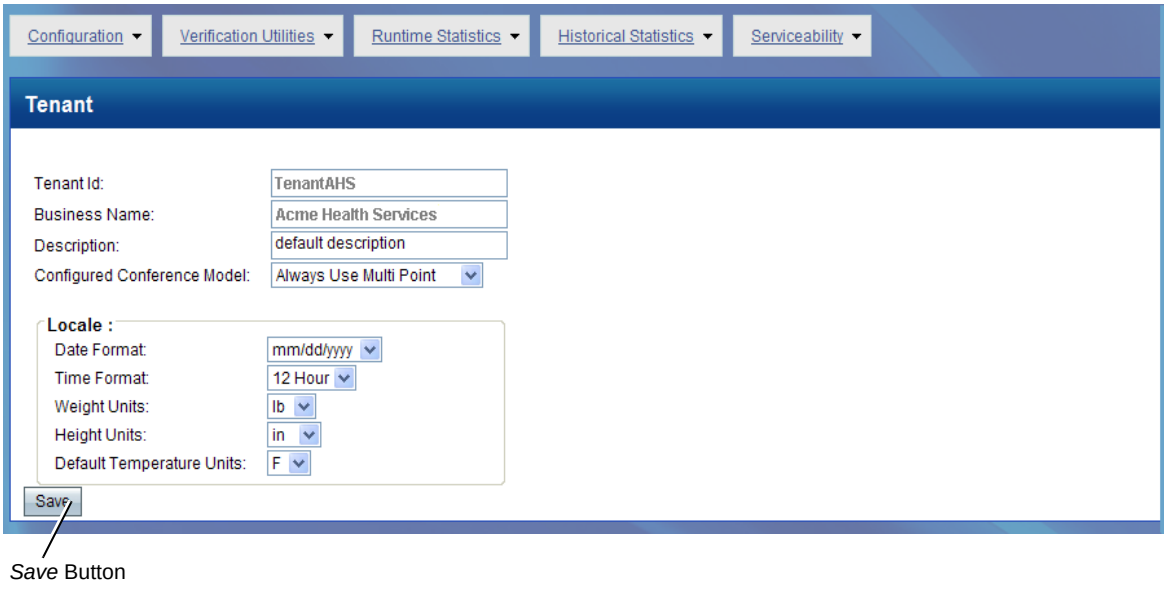


To view the current tenant settings, click *Tenant* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-5.

The tenant configuration controls how the screens will appear to the medical end users. This includes the conference model (point-to-point, multi-point, or user-selectable), the time and date formats, and how the measurement units that will appear at the Provider and Attendant stations.

These features were configured when your system was installed, but they can be changed if necessary. See "Changing Tenant Settings" on page 2-8. The fields are defined in Table 2-2 on page 2-8.

Figure 2-5 The Tenant Screen

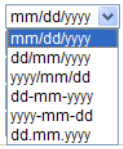


Note For a B2B appointment, if the Attendant tenant and the Provider tenant are configured differently, the selections made for the Attendant tenant will be the ones that show up on both Attendant and Provider screens.

Changing Tenant Settings

If you need to change any of the tenant settings, type over the data in the first three fields, and/or use the drop-down menus to select different settings for the remainder of the fields. When you have finished, click the *Save* button at the bottom left of the screen. All of these fields are defined in Table 2-2.

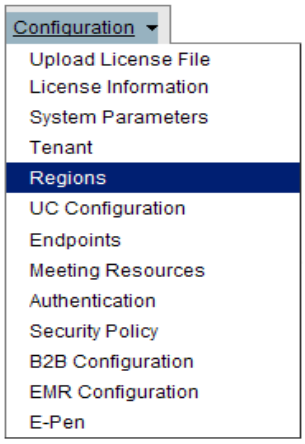
Table 2-2 Fields on the Tenant Screen

Field	Definition
Tenant Id	Can be any combination of numbers, letters, dashes, or underscores. Must be unique among all of the Tenant Ids for tenants using the same B2B manager.
Business Name	A descriptive identifier of the business. For example, "Smith Hospital Consortium" or "Jones Cardiology Group." For B2B appointments, this value will appear as the Business Name in the *Select Provider* dialog box.
Description	Can be anything that clarifies the purpose of the business. For example, "Cardiologists in the Atlanta Metropolitan area who have agreed to provide consultations for Agnes General Hospital."
Configured Conference Model	The choices here are *User Selectable*, *Multi-Party*, or *Two-Party*. If your system is not configured for multi-point calls, choose *Two-Party*. Multi-Point is required for appointments with three or more participants. Multi-Point appointments always use a multi-point bridge, which may be CTMS, CUVC, or the Codian MCU. If you have a large number of sites that will have concurrent appointments, and if those appointments typically involve only two parties (but sometime require multi-party), choose *User Selectable*. This allows multi-point when required, but uses point-to-point for all other calls, minimizing the bandwidth required at the data center. If you have adequate data center bandwidth to handle all appointments concurrently, and/or if a significant number of the appointments will be multi-point, you can choose *Always Use Multi-Point*, which simplifies the screen for the Attendant.
Date Format 	The date format shown at the Attendants' and Providers' stations.The choices are shown in the illustration to the left. Note that some of these choices differ only by punctuation.
Time Format	The time format shown at the Attendants' and Providers' stations. The choices are 12-hour or 24-hour.
Weight Units	The weight measurement unit. The choices are lb (pounds) or kg (kilograms).
Height Units	The height measurement unit. The choices are in (inches) or cm (centimeters).
Default Temperature Units	The default temperature measurement unit. The choices are F (Farenheit) or (C) Celsius. Regardless of what is specified here, if the Attendant is using an AMD temperature probe, he or she can modify the setting using the switch on the probe. If the Attendant is using a Neurosynaptics probe, the temperature units are always F.

Working with Regions

By default, all endpoints managed by a single Cisco HealthPresence system belong to the default region. If you have geographically dispersed multi-point bridges (CTMS's, CUVC's, or Codian MCU's), you may want to group the endpoints into regions based on geographical location or proximity to the bridges to minimize latency. You can also group your endpoints into regions just to partition the work load across multiple bridges.

Displaying a List of Regions

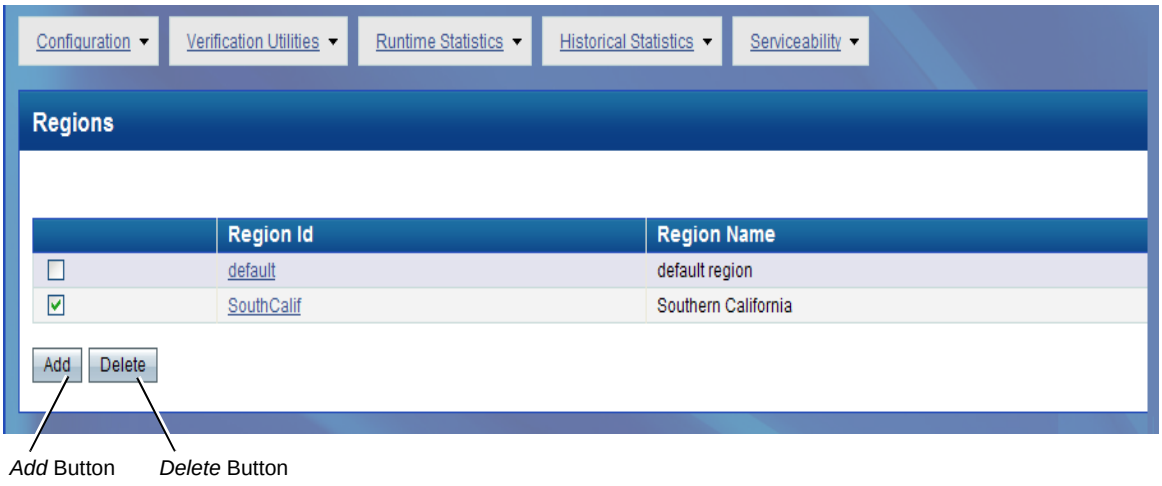


To display a list of regions, click *Regions* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-6.

This screen lists all of the regions configured for this system by Region Name (complete name) and Region Id (shortened version of name).

These settings were configured when your system was installed, but you can change them as required. See "Deleting a Region" on page 2-10, or "Updating a Region" on page 2-10, or "Adding a Region" on page 2-11.

Figure 2-6 The Regions Screen



Deleting a Region

To delete an existing region:

1. Click *Regions* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-6 on page 2-9.
2. Click the box to the far left of the region name.

   A checkmark appears in the box.
3. Click the *Delete* button.

Note The system will display an error message if you try to delete a region that is being used.

Updating a Region

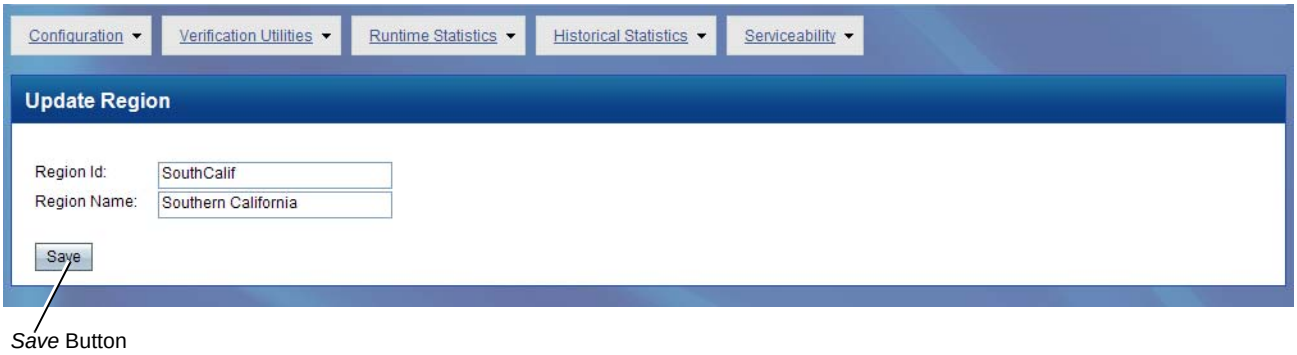
To update an existing region:

1. Click *Regions* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-6 on page 2-9.
2. Click on the name of the region you want to update.

   The system displays a screen similar to the one shown in Figure 2-7.
3. Type over the field or fields that you want to change.
4. Click the *Save* button.

Figure 2-7 The Update Region Screen



Adding a Region

To add a new region:

1. Click *Regions* on the *Configuration* menu.

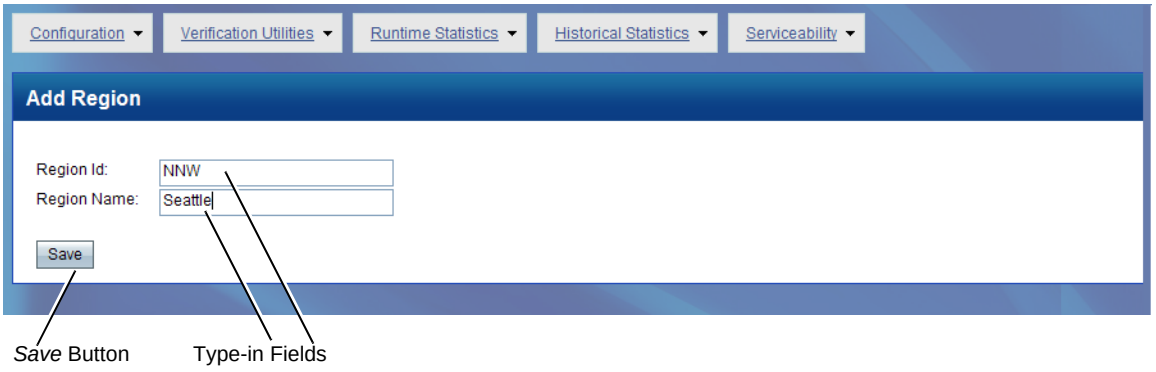
   The system displays a screen similar to the one shown in Figure 2-6 on page 2-9.
2. Click the box to the far left of the region name.

   A checkmark appears in the box.
3. Click the *Add* button.

   The system displays a screen similar to the one shown in Figure 2-8, but the fields will be blank.
4. Type in the Region Id you want to use.
5. Type in the Region Name you want to use.
6. Click the *Save* button.

   Your new region will appear on the list.

Figure 2-8 The Add Region Screen

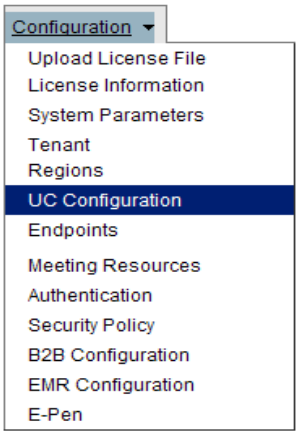


Configuring for Unified Communications (UC)

The Unified Communications (UC) settings control the video conferencing systems.

Displaying Current UC Settings

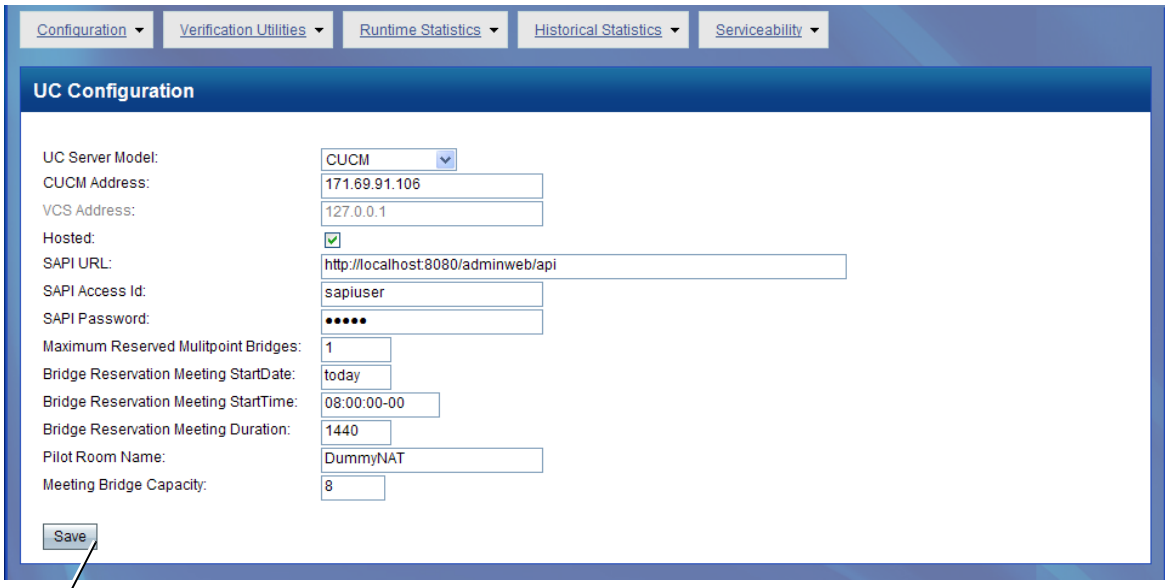
To view the current UC configuration settings, click *UC Configuration* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-9.



These settings were configured when your system was installed, but they can be changed if necessary (see "Changing the UC Settings" on page 2-13.)

The fields applicable to a hosted installation are defined in Table 2-3 on page 2-13.

Figure 2-9 The UC Configuration Screen



Changing the UC Settings

To make changes to the UC configuration:

1. Click *UC Configuration* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-9.
2. If necessary, select a different UC server model (CUCM, VCS, or CUCM and VCS).
3. If necessary, type in the CUCM address and the VCS address.
4. If this is or has become a hosted installation, click the check box next to *Hosted*.
5. If necessary, enter the applicable information in the *Hosted* fields as defined in Table 2-3.
6. Click the *Save* button.

Table 2-3 Fields on the UC Configuration Screen

Field	Definition
SAPI URL	Scheduling API (SAPI) url at the hosted site, as specified in the CTX tab of the Network Implementation Plan.
SAPI Access Id	Refer to the NIP. Typically *sapiuser*.
SAPI Password	Refer to the NIP.
Maximum Reserved Multi-point Bridges	Maximum number of concurrent TelePresence conferences permitted.
Bridge Reservation Meeting Start Date	Today.
Bridge Reservation Meeting Start Time	The earliest time of day that HealthPresence appointments will start. This start time should be specified in Greenwich Mean Time (GMT). For example, a default value of 08:00:00-00 refers to eight hours behind GMT, that is, Pacific Daylight Time.
Bridge Reservation Meeting Duration	Number of minutes that the HealthPresence system needs to be available. For example, if the system needs to be available for ten hours, specify 600. The default value of 1440 maps to 24 hours, which is the maximum length of time.
Pilot Room Name	Pilot room name(s) as configured in CTX. You can enter multiple names, separated by a pipe symbol (|). ***Note***: Multiple bridges (set in parameter Maximum Reserved Multi Point Bridges) are likely to require multiple room names.
Meeting Bridge Capacity	The default value of eight maps to four bridges each for two endpoints.

Working with Endpoints

In order for the Cisco HealthPresence Application Server to manage video calls, the Telepresence attributes of each video endpoint must be defined in the system. You use this screen to manage telemetry device parameters for the endpoint as well. In addition, you must specify the device aggregation (DA) type, if applicable for this endpoint.

Displaying a List of Endpoints

To view a list of current endpoints, click *Endpoints* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-10.

Endpoints that existed at the time your system was installed will probably already be configured and will appear on this list. However, as you add new endpoints, each of them will need to be configured here. You can also update the information for existing endpoints, if necessary.

See "Deleting an Endpoint" on page 2-15, or "Updating an Endpoint" on page 2-15, or "Adding an Endpoint" on page 2-16.

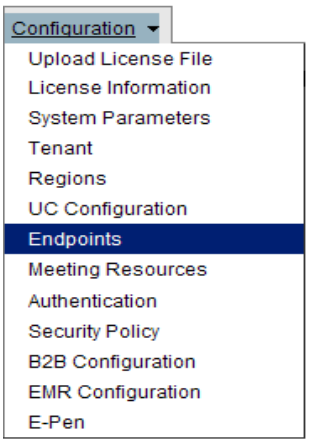
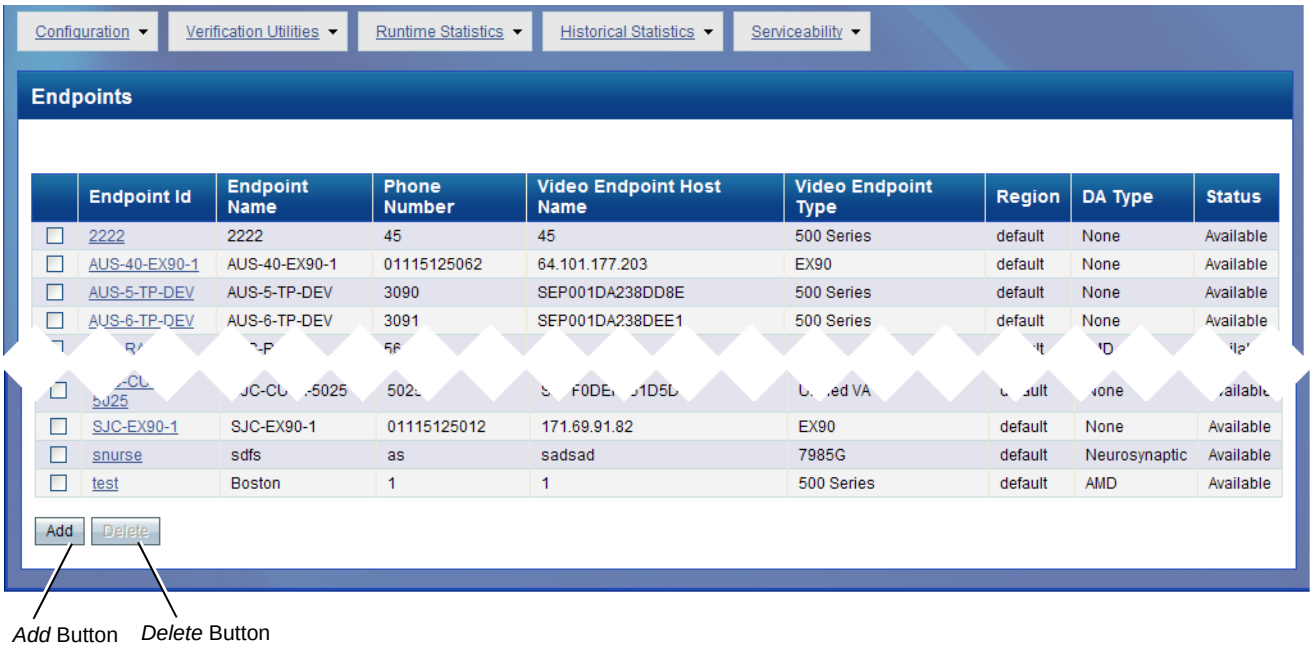


Figure 2-10 The Endpoints Screen



Deleting an Endpoint

To delete an existing endpoint:

1. Click *Endpoints* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-10 on page 2-14.
2. Click the box to the far left of the *Endpoint Id.*

   A checkmark appears in the box.
3. Click the *Delete* button.

Note The system will display an error message if you try to delete an endpoint that is being used.

Updating an Endpoint

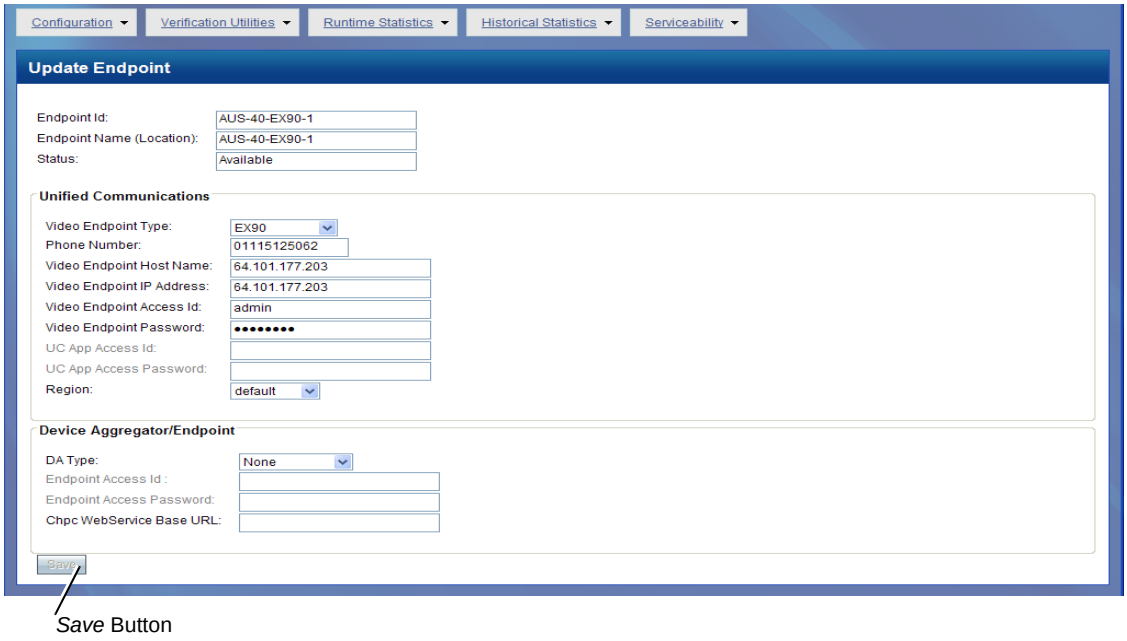
To update an existing endpoint:

1. Click *Endpoints* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-10 on page 2-14.
2. Click on the Endpoint Id of the endpoint you want to update.

   The system displays a screen similar to the one shown in Figure 2-11.
3. Type over the field or fields that you want to change. If necessary, make appropriate selections from the drop-down menus.
4. Click the *Save* button.

Figure 2-11 The Update Endpoint Screen



Adding an Endpoint

To add a new endpoint, there are three things that need to be done.

1. You must add a new endpoint in the Cisco HealthPresence Administration Server as described in Adding an Endpoint to the Cisco HealthPresence Administration Server, page 2-16.
2. From the Attendant station, you must all configure the endpoint ID in the Cisco HealthPresence Portal Server as described in Setting the Endpoint ID in the Cisco HealthPresence Portal Server, page 2-18.
3. Finally, if the endpoint is an AMD Attendant endpoint, then from the Attendant Station, you must configure the endpoint information in CHPC as described in Configuring AMD Attendant Endpoint Information in Cisco HealthPresence Client Administration, page 2-20

Adding an Endpoint to the Cisco HealthPresence Administration Server

To add a new endpoint to the Cisco HealthPresence Administration Server:

1. Click *Endpoints* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-10 on page 2-14.
2. Click the *Add* button.

   The system displays a screen similar to the one shown in Figure 2-12.
3. Complete the fields as described in Table 2-4 on page 2-18, and in the CHP Endpoints tab of the *CHP Network Implementation Plan*.

   Some fields are not required for some endpoints, in which case, they will be dimmed once the endpoint is selected.
4. Click the *Save* button.

Figure 2-12 The Add Endpoint Screen

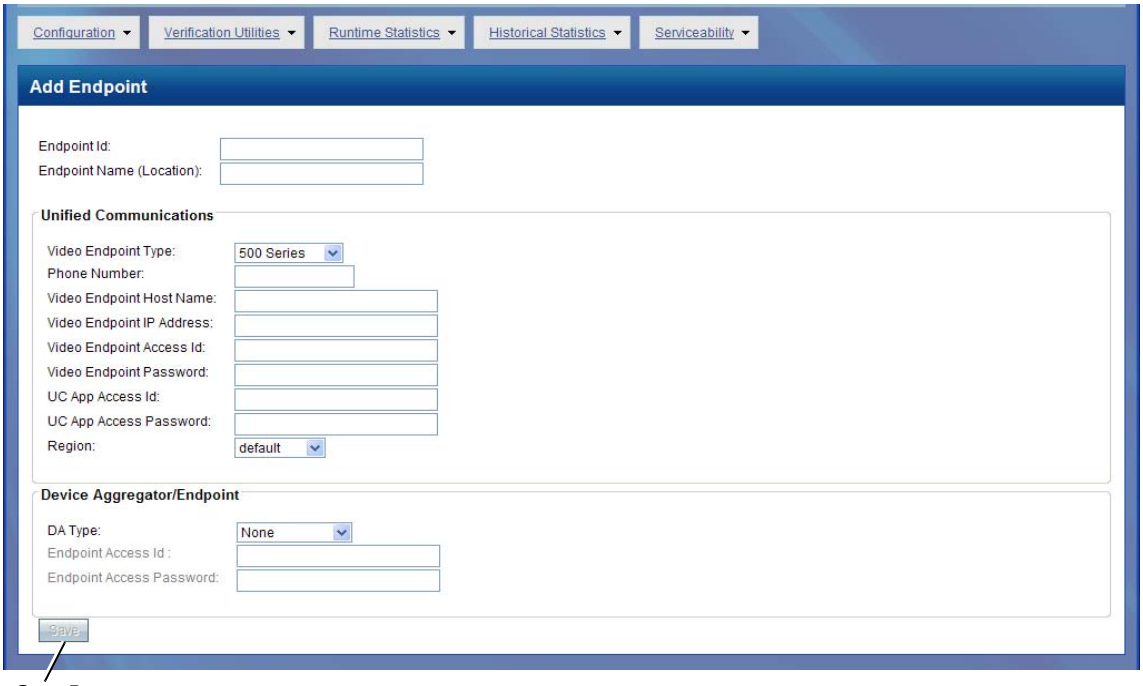


Table 2-4 Fields on the Add Endpoints Screen

Field	Definition
Endpoint Id	Must be unique among the endpoints communicating within a tenant. May include alphanumeric characters, dashes, and underscores.
Endpoint Name (Location)	Will appear on the Provider's *Ready Appointments* screen. There are no restrictions on characters.
Unified Communications	
Video Endpoint Type	The possible video endpoint types are listed on the menu
Phone Number	Phone number of the Video Endpoint
Video Endpoint Host Name	The name given to the endpoint at the Attendant (host) station
Video Endpoint IP Address	IP address of the Video Endpoint
Video Endpoint Access Id	Access ID of the Video Endpoint
Video Endpoint Password	Access Password of the Video Endpoint.
UC App Access Id	UC App Access ID of the Video Endpoint
UC App Password	UC App Password of the Video Endpoint
Region	Endpoints sorted into groups based on geographical location or proximity to the bridges.
Device Aggregator/Endpoint	
DA Type	This can be AMD, Neurosynaptic or None
Endpoint Access Id	Required only if AMD is specified. This must match what was specified in the Client Administration configuration, as outlined Configuring AMD Attendant Endpoint Information in Cisco HealthPresence Client Administration, page 2-20.
Endpoint Access Password	Required only if AMD is specified. This must match what was specified in the Client Administration configuration, as outlined Configuring AMD Attendant Endpoint Information in Cisco HealthPresence Client Administration, page 2-20

Setting the Endpoint ID in the Cisco HealthPresence Portal Server

To set the Endpoint ID in the browser, complete the following steps from the endpoint you are configuring.

Step 1 Open a browser window and enter *https://[chp-application-server-ip-address]/chppc/* in the browser's address field.

Step 2 Log in to the portal server by entering appropriate login information similar to the following sample:

- Username = *endpointadmin*
- Password = *as provided when the system was installed*

The Endpoint Id Configuration Screen displays, as in Figure 2-13.

Figure 2-13 Cisco HealthPresence Endpoint ID Configuration Screen

Step 3 From the Endpoint ID Configuration screen, enter the Endpoint ID of this Endpoint (as specified in Adding an Endpoint to the Cisco HealthPresence Administration Server, page 2-16). Click **Set Endpoint ID.**

Step 4 Click Get Endpoint ID to verify it was set correctly.

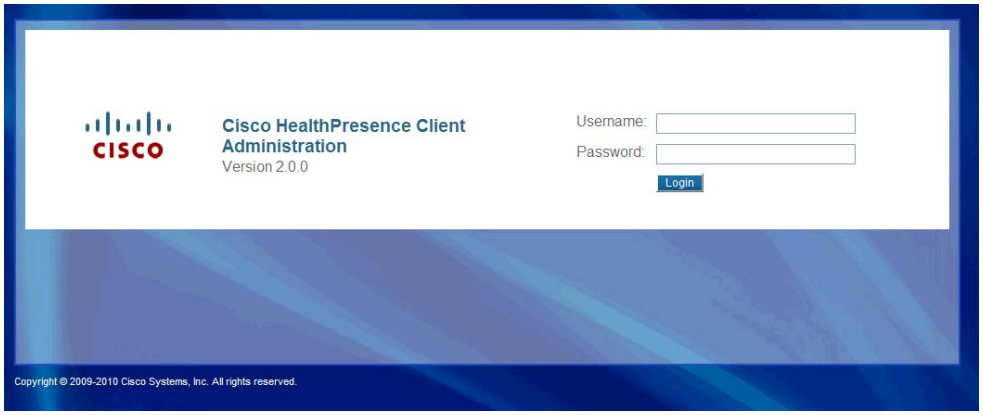
Configuring AMD Attendant Endpoint Information in Cisco HealthPresence Client Administration

Note This is only required for AMD Attendant endpoints.

To configure Attendant Endpoint information in Cisco HealthPresence Client Administration, complete the following steps from the Attendant Endpoint.

Step 1 Open a browser window and enter *https://localhost/chpc*. The Cisco HealthPresence Client Administration Login window displays, as shown in Figure 2-14.

Figure 2-14 Cisco HealthPresence Client Administration Login Window

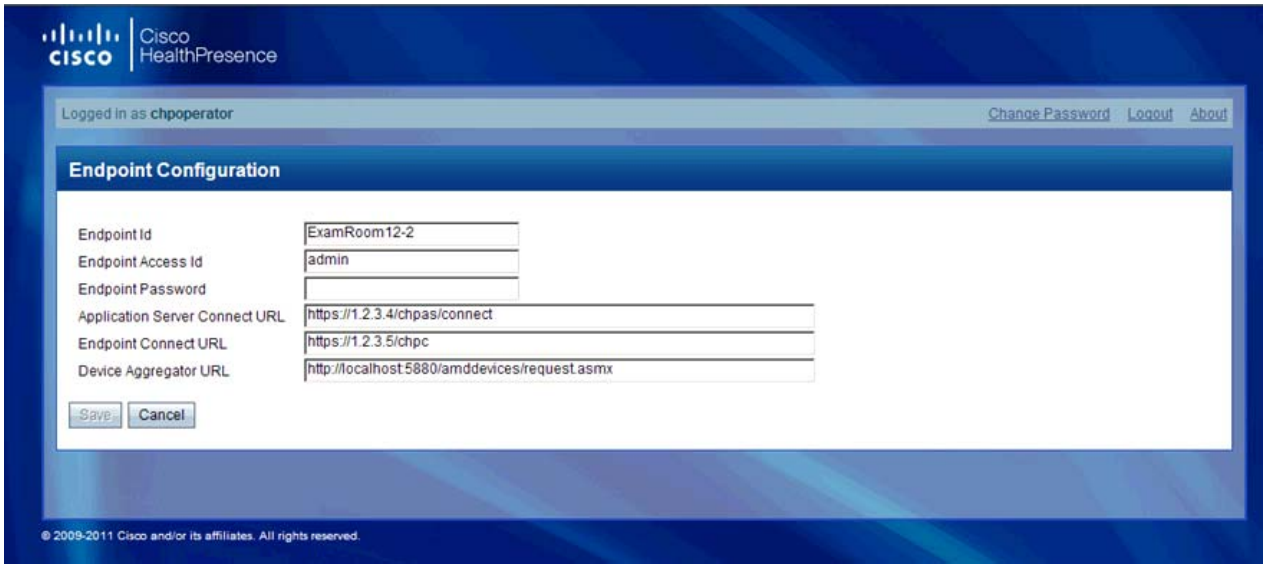


Step 2 Log in as:

- Username = *chpoperator*
- Password = *as provided when the system was installed*

Step 3 The Endpoint Configuration window displays as shown in Figure 2-15.

Figure 2-15 Endpoint Configuration Window



Step 4 Specify the Endpoint Id that was specified in Adding an Endpoint to the Cisco HealthPresence Administration Server, page 2-16.

Step 5 Specify the Endpoint Access Id and Password that were specified in the Adding an Endpoint to the Cisco HealthPresence Administration Server, page 2-16.

Step 6 Specify the Application Server Connect URL. It is of the format *https://ip_addr_chpas/chpas/connect*.

Step 7 Specify the Endpoint connect URL used by the CHP Server Administration to connect to this CHP Appliance. It is of the format *https://localhost/chpc*.

Step 8 Specify the Device Aggregator URL (if applicable). It is of the format *https://localhost:5880/amddevices/request.asmx*.

Step 9 **Click Save**.

Working with Meeting Resources

Meeting resources are used to enable multi-point video conferences.

Note This procedure is not applicable if **Always Use Point to Point** was selected as the Conference Connection Mode when the system parameters were configured.

Displaying a List of Meeting Resources

To view a list of current meeting resources, click *Meeting Resources* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-16.

If you configured meeting resources when your system was installed, they will appear on this list. However, you can add new meeting resources or adjust existing meeting resources, as necessary.

See "Deleting a Meeting Resource" on page 2-22, or "Updating a Meeting Resource" on page 2-23, or "Adding a Meeting Resource" on page 2-23.

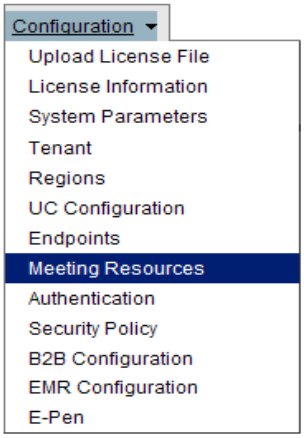
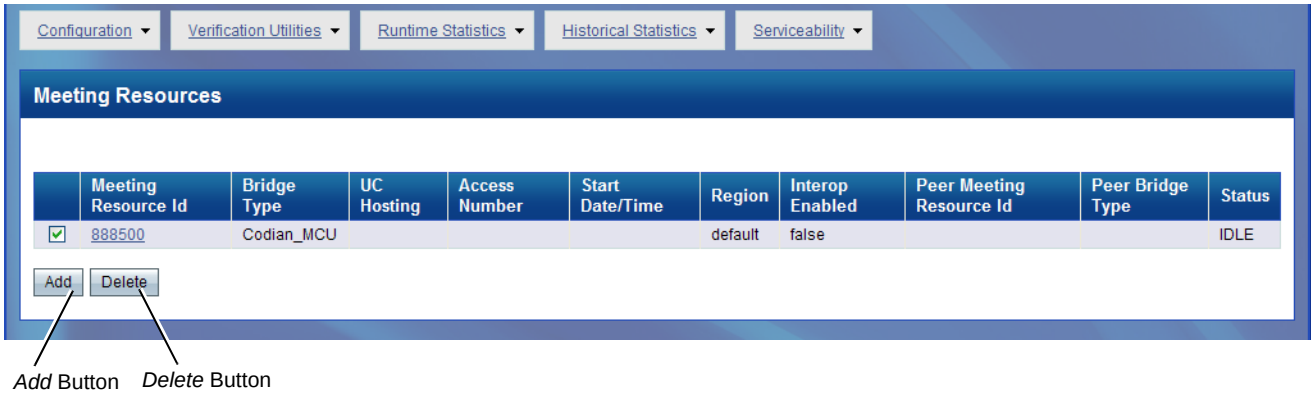


Figure 2-16 The Meeting Resources Screen



Deleting a Meeting Resource

To delete an existing meeting resource:

1. Click *Meeting Resources* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-16.

2. Click the box to the far left of the *Meeting Resource Id.*

   A checkmark appears in the box.

3. Click the *Delete* button.

Updating a Meeting Resource

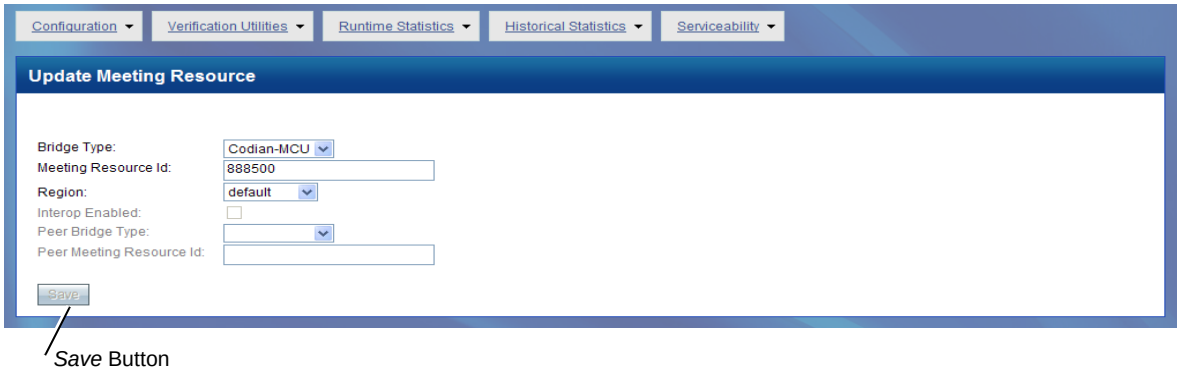
To update an existing meeting resource:

1. Click *Meeting Resources* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-16 on page 2-22.
2. Click on the Meeting Resource Id of the resource you want to update.

   The system displays a screen similar to the one shown in Figure 2-17.
3. Type over the field or fields that you want to change.
4. If necessary, make appropriate selections from the drop-down menus.
5. Click the *Save* button.

Figure 2-17 The Update Meeting Resources Screen



Adding a Meeting Resource

To add a new meeting resource:

1. Click *Meeting Resources* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-16 on page 2-22.
2. Click the *Add* button.

   The system displays a screen similar to the one shown in Figure 2-18 on page 2-24.
3. Complete the fields as described in Table 2-5 on page 2-24.
4. Click the *Save* button.

Figure 2-18 The Add Meeting Resource Screen

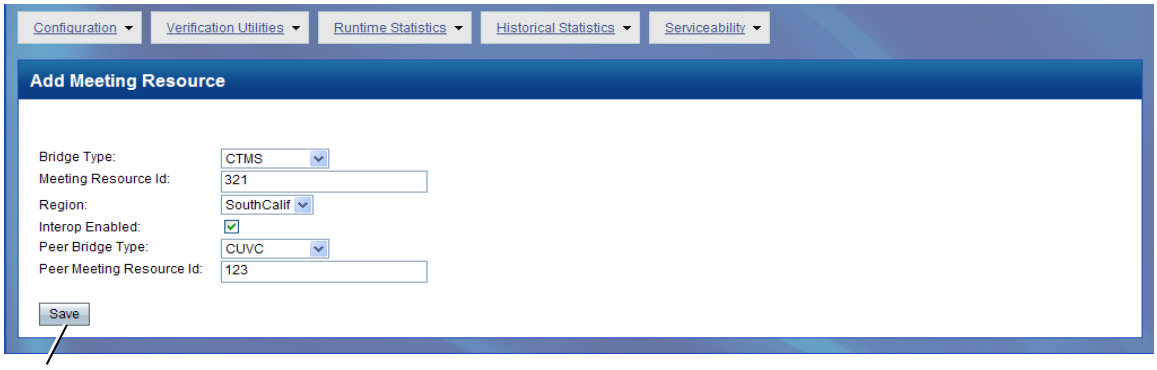


Table 2-5 Fields on the Add Meeting Resource Screen

Field	Definition
Bridge Type	Choose CTMS, CUVC or Codian MCU.
Meeting Resource Id	Access number configured in CTMS.
Region	If this enterprise uses regions, specify the region for this meeting resource. Otherwise, leave it as *default*.
Interop Enabled	If this bridge type will interoperate with another bridge type, check this box. This box cannot be checked if Codian MCU is chosen.
Peer Bridge Type	This is filled in automatically.
Peer Meeting Resource Id	Access code configured for the peer bridge.

Choosing the Authentication Type

The purpose of authentication is to make certain that everybody who uses the system has access to the features that he or she needs, while ensuring that unauthorized users cannot access protected information. The Cisco HealthPresence system uses the three types of authentication described below.

- **Dedicated (Cisco HealthPresence) Authentication** – All usernames, passwords, and user attributes are stored in a dedicated Cisco HealthPresence directory.
- **External Lightweight Directory Access Protocol (LDAP) Authentication –** When using external LDAP authentication, users are authenticated against the LDAP server instead of a dedicated Cisco HealthPresence directory. The LDAP common name is used as the Cisco HealthPresence display name. The LDAP user ID is enabled as the user name in Cisco HealthPresence. The Cisco HealthPresence display name and last name properties are synchronized with LDAP common name and sort name attributes.
- **Mixed Authentication –** The Site Administrator can configure users with either Dedicated Authentication or LDAP Authentication.

Displaying the Authentication Settings

To view the current authentication settings, click *Authentication* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-19.

The authentication type will have been set when the system was installed, but if it needs to be changed or updated, you can follow the procedure described here. See "Changing the Authentication Settings" on page 2-26.

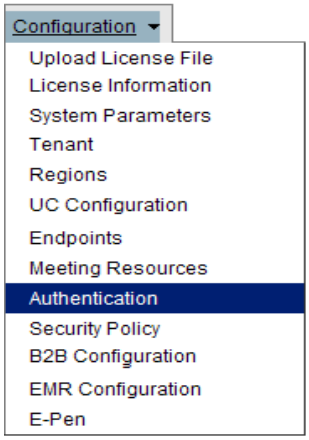
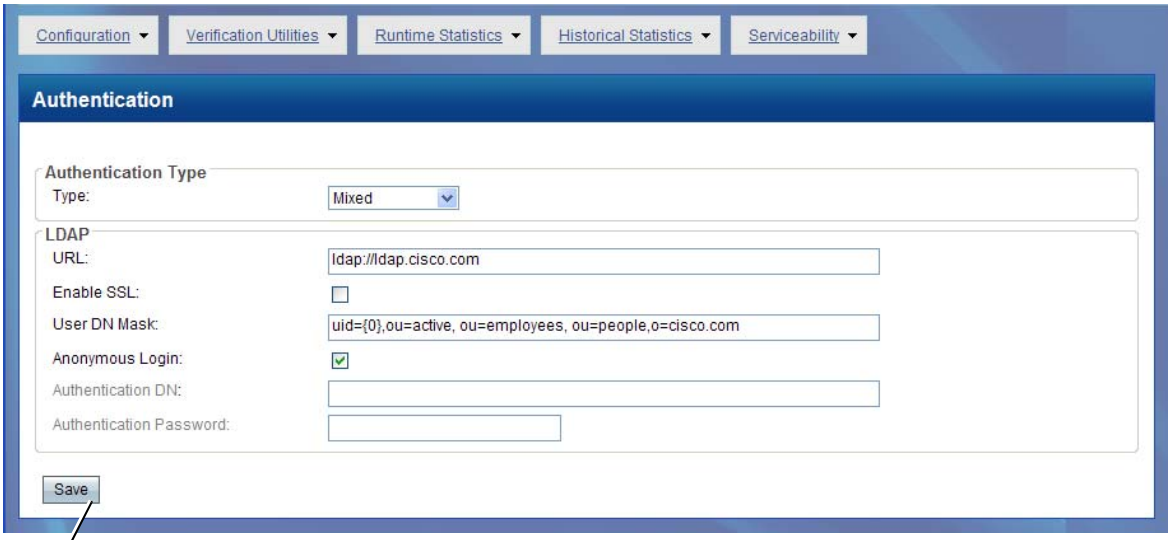


Figure 2-19 The Authentication Screen



Changing the Authentication Settings

If you need to change the authentication configuration:

1. Click *Authentication* on the *Configuration* menu.

   The system displays a screen similar to the one shown in Figure 2-19 on page 2-26.

2. Choose the *Authentication Type*.

   If you choose *Dedicated*, all *LDAP* parameters will be dimmed.

   If you choose LDAP, any users configured to the Cisco HealthPresence system will be deleted, including the users configured for testing and training when the product was shipped. If you want to keep the pre-configured training user accounts, but want to use *LDAP* for other users, specify *Mixed*.

3. If you choose *Mixed* or *LDAP*, specify the url for the LDAP server.

4. If you want to use SSL for this connection, click the *Enable SSL* box.

   If you use SSL, the Cisco HealthPresence system will trust the certificate of the server so no other certificates need to be configured.

5. Specify the Distinguished Name (DN) Mask.

   The DN Mask controls the format of the Distinguished Name (DN) that will be used to authenticate the user with the LDAP server. The username replaces the {0} in this mask. For example, if the mask is: uid={0},ou=active, ou=employees, ou=people,o=companyxyz.com, when “nursepat” logs in, the DN of uid=nursepat,ou=active, ou=employees, ou=people,o=companyxyz.com is sent to the LDAP server for authentication.

6. Click *Anonymous Login* if you want the system to use anonymous login to enable a user when the LDAP connection is made.

   If this is not checked, the authentication DN and password are used to authenticate with the LDAP server when a user is enabled.

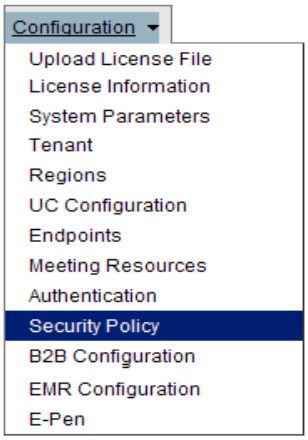
7. Click **Save**.

Setting Security Policy

The Security options described here are available to sites that use the Dedicated Cisco HealthPresence Authentication type or the Mixed Authentication type. Account Inactivity and User Lockout may also be available with LDAP Authentication. How these options are implemented was determined when the system was installed.

Displaying Current Security Settings

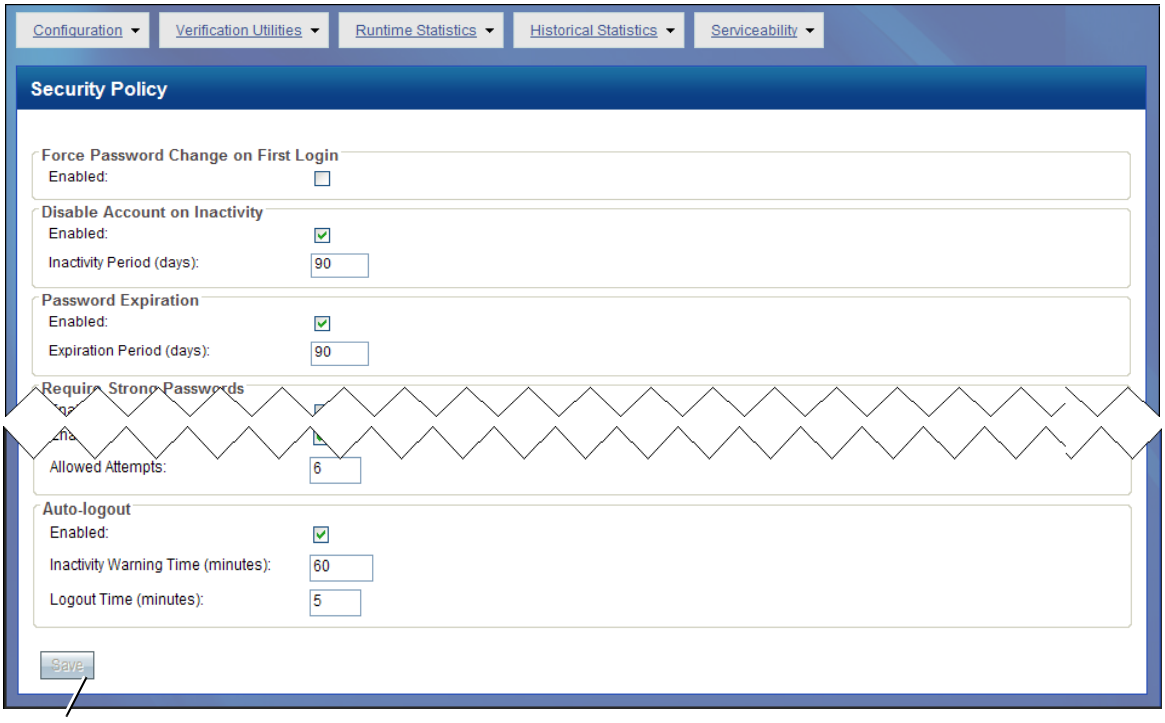
To view the current security settings, click *Security Policy* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-20.



These are the options and their default settings:

- Forced Password Change – Required with first log in.
- Account Inactivity – Disable or Lock out after ninety days.
- Password Expiration – After ninety days.
- Strong Passwords – Seven-character minimum, two types of symbols.
- Password Reuse – Checks last four passwords.
- User Lockout – After six unsuccessful attempts.
- Auto-Logout – 60 minutes before a warning is displayed; five additional minutes before the end user is logged out.

Figure 2-20 The Security Policy Screen



Save Button

Changing the Security Settings

If you want to change one or more of the security settings, follow the instructions below. Note that the specifications that concern passwords apply only to passwords for users with Dedicated Authentication, that is, for user accounts authenticated by Cisco HealthPresence and not by an external directory.

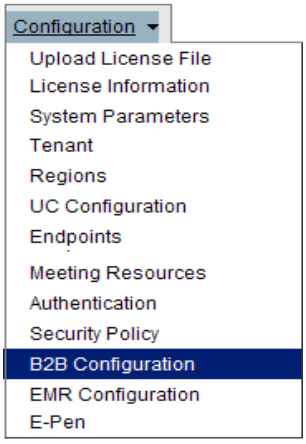
To change the security settings:

1. **Force Password Change on First Login**
   Click the *Force Password Change Enabled* box if you want to force a password change on the first login.
2. **Disable Account on Inactivity**
   Click the *Disable Account on Inactivity Enabled* box if you want to disable an account if the user does not log in for a certain number of days. If enabled, specify the inactivity period. The inactivity days can range from 1 to 730.
3. **Password Expiration**
   Click the *Password Expiration Enabled* box if you want passwords to expire after a certain number of days. If enabled, specify the expiration period. The expiration days can range from 1 to 999.
4. **Require Strong Passwords**
   Click the *Require Strong Passwords Enabled* box if you want to require strong passwords. If enabled, specify the minimum password length and the minimum number of character types. The length of strong passwords can be between 1 and 15 characters with a minimum of character types ranging from 1 to 4.
5. **Prevent Password Reuse**
   Click the *Prevent Password Reuse Enabled* box if you want to prevent password reuse. If enabled, specify the number of saved passwords (a number between 1 and 20).
6. **User Lockout**
   Click the *User Lockout Enabled* box if you want to prevent repeated attempts at password entry. If enabled, specify the number of passwords that can be entered (a number between 1 and 20).
7. **Auto-Logout**
   Click the *Auto-Logout Enabled* box if you want to automatically log out a user for inactivity during a session. If enabled, specify the inactivity warning time and logout time.
   - The Inactivity Warning is a warning message that appears after a specified number of minutes of no activity (pressing enter, clicking a mouse key, etc.,) during a session. The time between activity and when the inactivity warning message appears is can be set from 1 to 999 minutes.
   - The Logout time is the amount of time AFTER the Inactivity Warning before the end user is logged off. It can be between 1 and 60 minutes.
8. When you have finished, click the *Save* button.

Note Changes will not affect users who are currently logged in. Changes will only impact user logins that occur after the change is made.

Configuring B2B Settings

The B2B settings specify the url of the B2B manager used by the specified Cisco HealthPresence Application Server for business-to-business appointments.



To view the existing B2B settings, click *B2B Configuration* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-21.

Unless you are changing the B2B manager or adding a B2B manager, do not change the settings specified during installation.

Figure 2-21 The B2B Configuration Screen

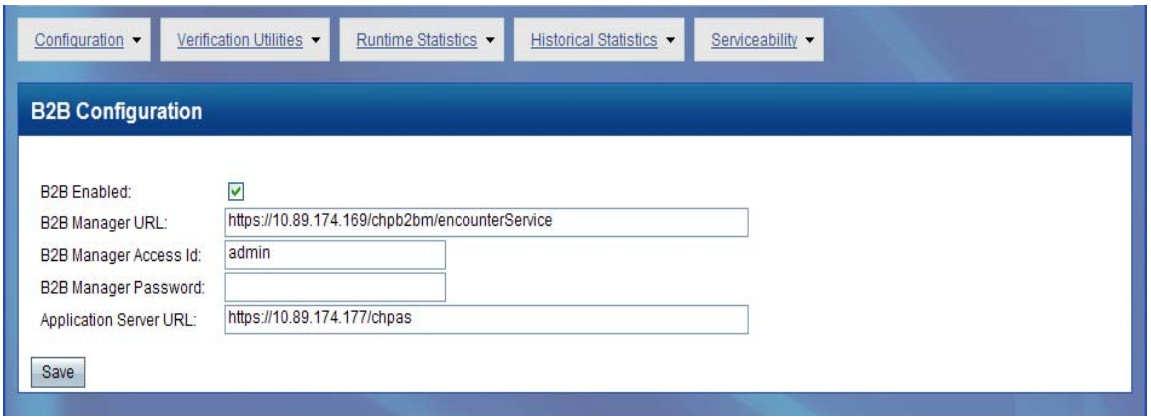


Table 2-6 Fields on the B2B Configuration Screen

Field	Definition
B2B Enabled	This box is checked if this system is configured for Business-to-Business conferences.
B2B Manager URL	The URL for the server that manages Business-to-Business communications.
B2B Manager Access Id	The B2B Manager Access ID. Typically this does not need to be changed after the initial installation.
B2B Manager Password	The B2B Manager Password.Typically this does not need to be changed after the initial installation.
Application Server URL	The URL for the server that manages the Cisco HealthPresence system.

Configuring for Electronic Medical Records (EMR)

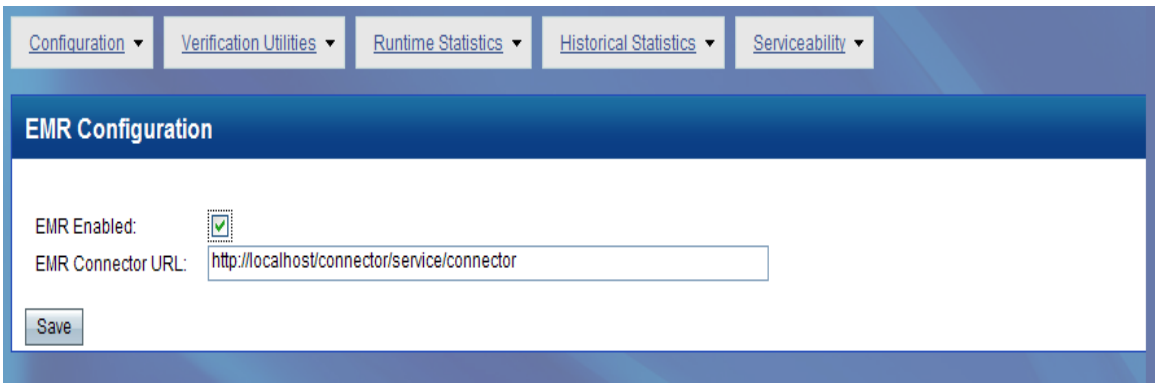
Electronic Medical Records (EMR) store patient information securely. The Cisco HealthPresence system does not connect directly to EMR; however, it works with integration engines to make communication possible.

There are several steps required to enable the Cisco HealthPresence system to work with an integration engine. This only describes the final steps in a process that must take place on another system before this connection will work.

To view the EMR configuration settings, click *EMR Configuration* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-22.

If you have done all the steps required to enable EMR, check the *EMR Enabled* box and specify the URL where the EMR Connector is located. It is of the format displayed in Figure 2-22.

Figure 2-22 The EMR Configuration Screen



Setting Up the E-Pen Feature

If your site supports the E-Pen feature, a physician can write prescriptions on the Cisco HealthPresence system using an E-Pen. Providers write prescriptions on the *Write Prescription* tab (which doesn't appear on the Attendant's screen), and Attendants (and other participants) view these prescriptions from the *View Prescription* tab (see Figure 2-25 on page 2-33). Either can print the prescription.

You can use this configuration screen to add both a header and a footer to the prescription using graphic files that you select. You can select a header, a footer, or one of each. The files must have a .jpg file extension.

To view the settings for the E-Pen feature, click *E-Pen* on the *Configuration* menu. The system displays a screen similar to the one shown in Figure 2-23. In this example, no graphics have yet been selected.

To add or change graphics:

1. Click the first *Browse* button, and locate the graphic that you want to use for the header (if any).
2. Click the second *Browse* button, and locate the graphic that you want to use for the footer (if any).
3. Click the *Save* button at the bottom of the screen.

   The screen will look something like the sample shown in Figure 2-24 on page 2-33. To see how this prescription looks to the user, refer to Figure 2-25 on page 2-33.

Figure 2-23 The E-Pen Screen

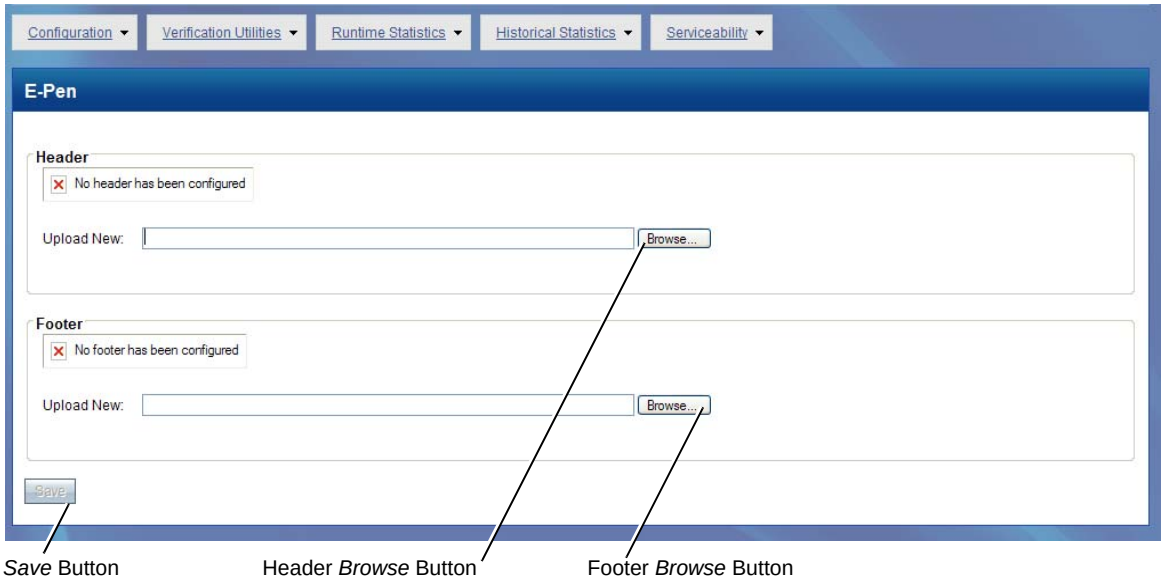


Figure 2-24 The E-Pen Screen with Graphics

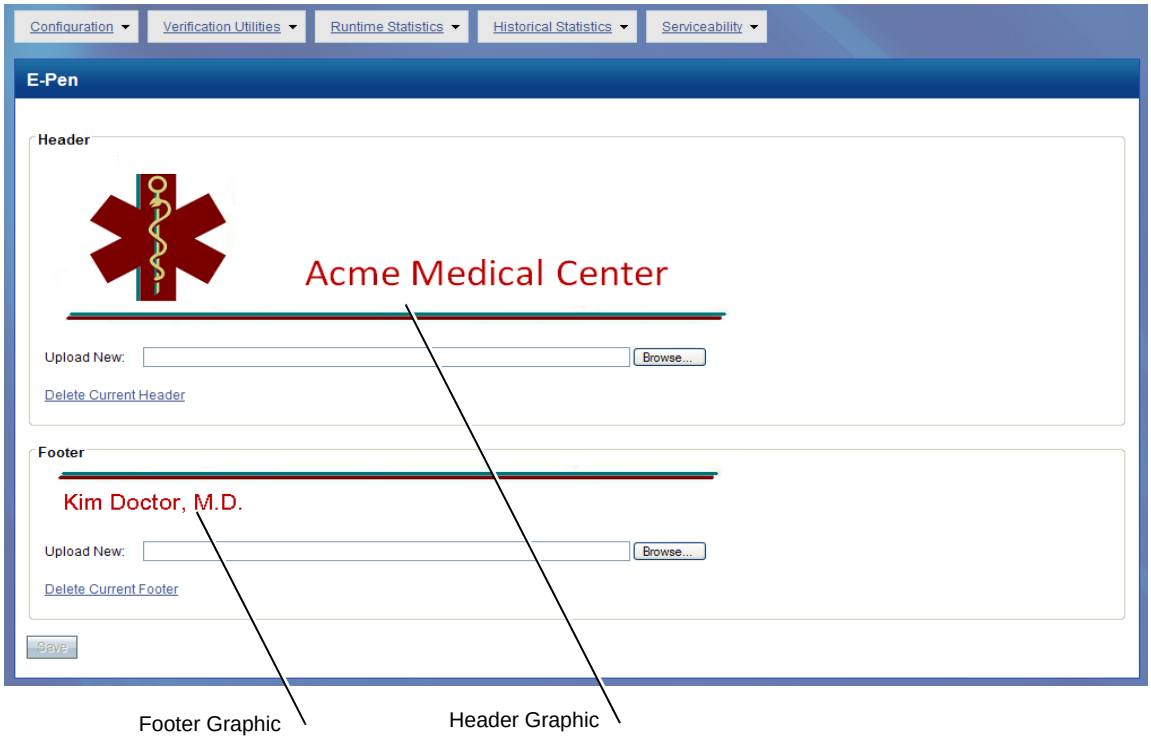
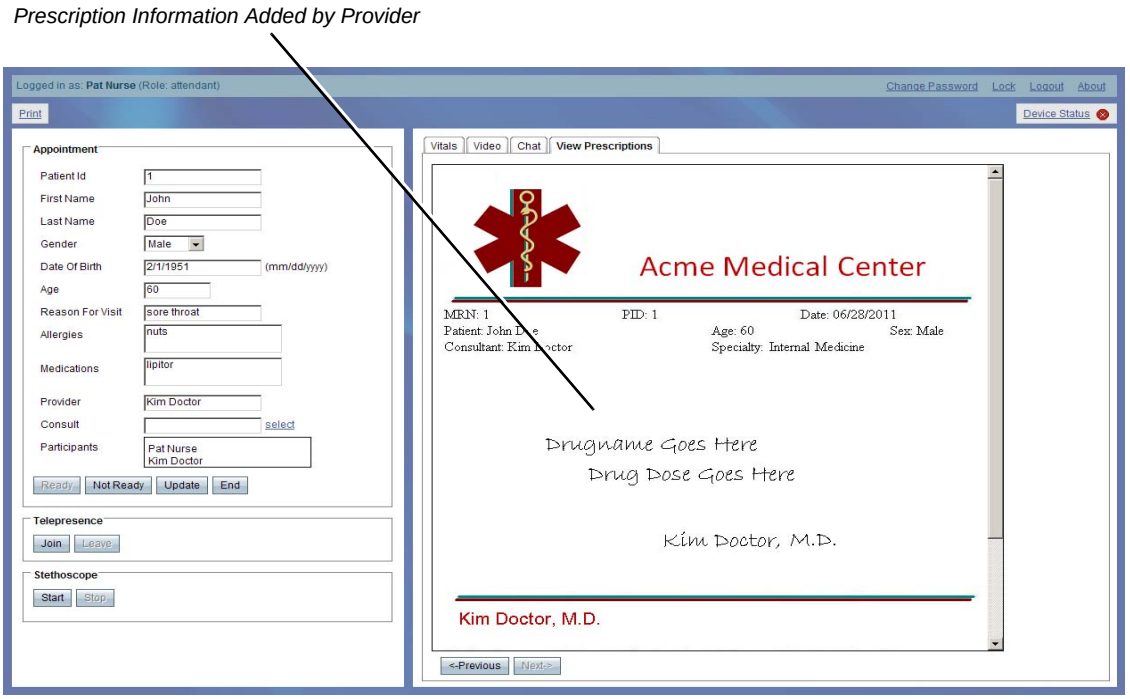


Figure 2-25 Viewing a Prescription From the Attendant Station



CHAPTER 3

The Runtime Statistics

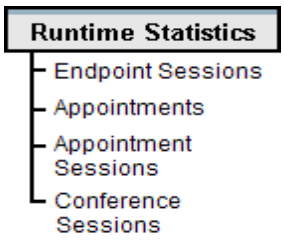
Revised: October 31, 2011, OL-25943-01

This chapter explains the tasks that you can do using the *Runtime Statistics* menu from the Cisco HealthPresence *Server Administration* window.

The runtime statistics allow you to view information about what is currently taking place on the system. All of the screens available from this menu provide information about what is happening at the time that you display the screen. You can view statistics about active Cisco HealthPresence Endpoints, Appointments, Appointment Sessions, and Conferences.

These topics are included in this chapter:

- Viewing a List of Active Endpoint Sessions
- Viewing a List of Active Appointments
- Viewing a List of Active Appointment Sessions
- Viewing a List of Active Conference Sessions



Viewing a List of Active Endpoint Sessions

An endpoint is the Cisco HealthPresence Connect software running in the Attendant or Provider Appliance. When an end user (Provider, Attendant, Presenter, Participant, or Site Administrator) logs in to the Cisco HealthPresence system, a session is initiated between the endpoint and the Cisco HealthPresence Connect Server.

This feature is useful if you want to see which endpoints are in use, or if you want to know if a particular endpoint is in use.

To display a list of currently active endpoint sessions, click *Endpoint Sessions* on the *Runtime Statistics* menu. The system displays a screen similar to the one shown in Figure 3-1.

To refresh the screen at any time, reselect the *Endpoint Sessions* from the drop down menu.

If necessary, you can use the *Reset* button to forcibly log out the user. Select one of the displayed entries, click the *Reset* button, and then confirm by clicking *Yes*.

The fields on the Endpoint Sessions Screen are defined in Table 3-1.

Figure 3-1 The Endpoint Sessions Screen

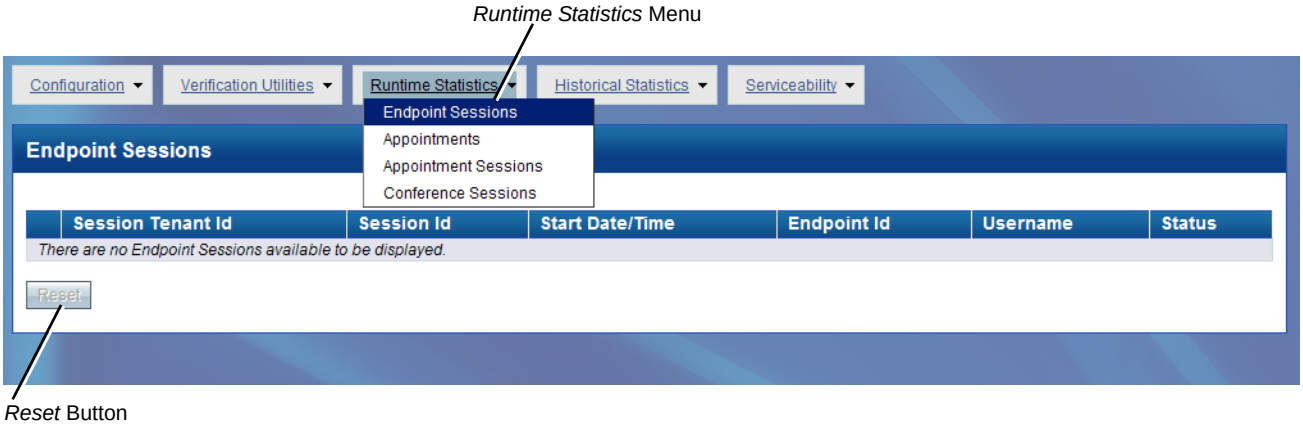


Table 3-1 Fields on the Endpoint Sessions Screen

Field	Definition
Session Tenant Id	The identification code of the business that initiated this session (if applicable).
Session Id	An automatically assigned code that is unique to this session.
Start Date/Time	When this session was first started, that is, when the system accepted the login request of the portal client.
Endpoint Id	The identification code assigned to this endpoint when the system was configured.
Username	The login name of the user who began this session.
Status	If the device appears, the status is Active.

Note Only applicable fields will be displayed. For example, “Session Tenant Id” will only appear on systems that have the B2B capability.

Viewing a List of Active Appointments

Appointments include all individual appointments and conferences. To display the list, click *Appointments* on the *Runtime Statistics* menu. The system displays a screen similar to the one shown in Figure 3-2.

The fields in the list of currently active appointments are defined in Table 3-2.

Figure 3-2 The Appointments Screen

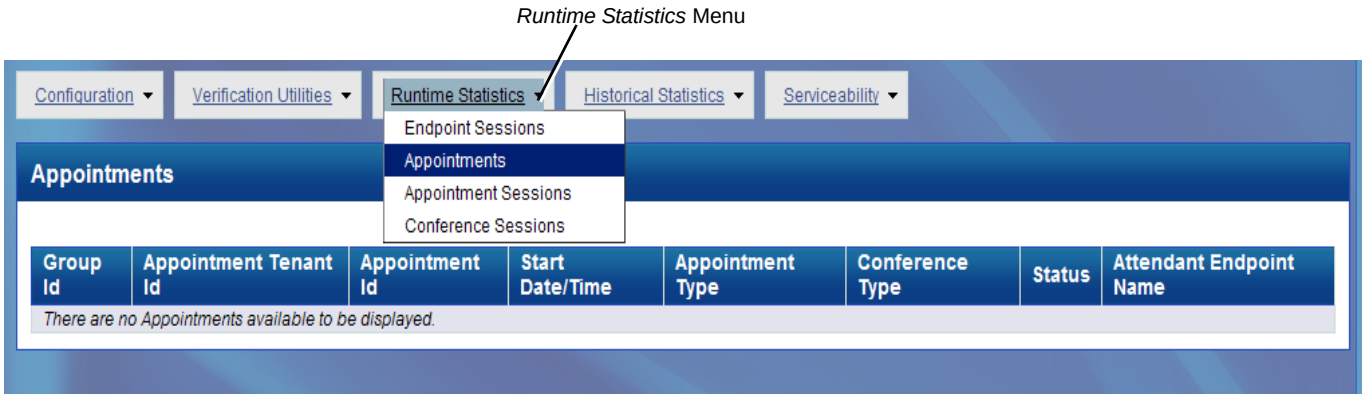


Table 3-2 Fields on the Appointments Screen

Field	Definition
Group Id	The identification code of the B2B Group (if applicable).
Appointment Tenant Id	The identification code of the business that initiated this appointment (if applicable).
Appointment Id	An automatically assigned code that is only valid for this appointment (if applicable).
Start Date/Time	When this appointment was first started.
Appointment Type	Can be Business-to-Business (B2B) or nonB2B.
Conference Type	Can be two-party or multi-party.
Status	Not Ready – The appointment has been started, but the Attendant has not yet clicked the *Ready* button. Ready – the Attendant has clicked the *Ready* button so that the appointment appears on the Provider's screen. Shared – the telemetry data is being shared.
Attendant Endpoint Name	The name given to the endpoint at the Attendant station.

Note Only applicable fields will be displayed. For example, "Group Id," "Appointment Tenant Id," and "Appointment Id" will only appear on systems that have the B2B capability.

Viewing a List of Active Appointment Sessions

An appointment session is the user connection to an appointment. In a typical Attendant and Provider appointment, there will be a single appointment entry, but there will be two appointment session entries, one for the Attendant and one for the Provider.

To display a list of currently active appointment sessions, click *Appointment Sessions* on the *Runtime Statistics* menu. The system displays a screen similar to the one shown in Figure 3-3.

The fields on the Appointment Sessions screen are defined in Table 3-3.

Figure 3-3 The Appointment Sessions Screen

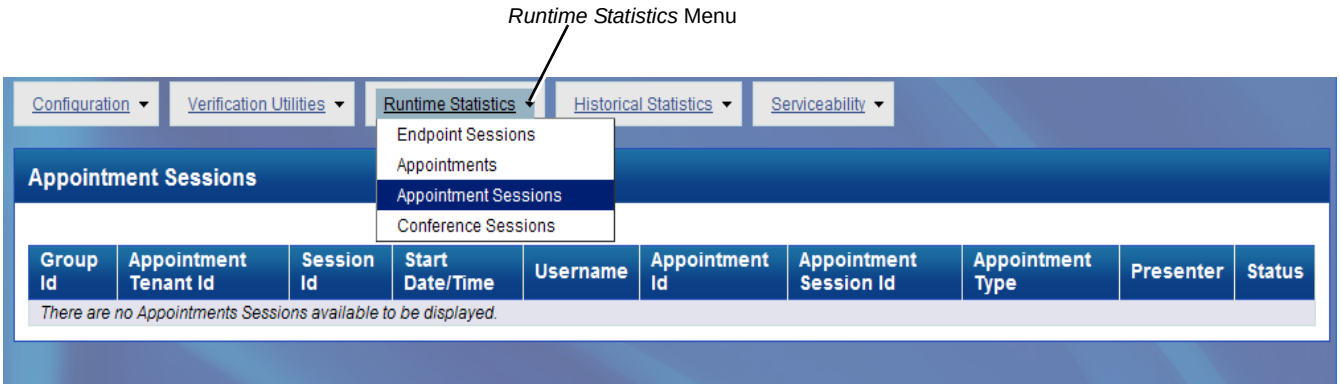


Table 3-3 Fields on the Appointment Sessions Screen

Field	Definition
Group Id	The identification code of the B2B Group (if applicable).
Appointment Tenant Id	The identification code of the business that initiated this appointment (if applicable).
Session Id	An automatically assigned code that is unique to this session (if applicable).
Start Date/Time	When this appointment session was first started.
Username	The login name of the user who began this appointment session.
Appointment Id	An automatically assigned code that is only valid for this appointment.
Appointment Session Id	An automatically assigned code that is unique to this appointment session.
Appointment Type	Can be B2B or nonB2B.
Presenter	The username of the user who initiated this conference.
Status	Not Ready – The appointment has been started, but the Attendant has not yet clicked the *Ready* button. Ready – The Attendant has clicked the *Ready* button, and the Provider has selected the appointment.

Note Only applicable fields will be displayed. For example, “Group Id,” “Appointment Tenant Id,” and “Appointment Id” will only appear on systems that have the B2B capability.

Viewing a List of Active Conference Sessions

Conference sessions are created when a Presenter starts a Telepresence conference or when a Participant enters a conference, whichever happens first.To display a list of currently active conference sessions, click *Conference Sessions* on the *Runtime Statistics* menu. The system displays a screen similar to the one shown in Figure 3-4.

If necessary, you can use the *Reset* button to forcibly log out the user. Select one of the displayed entries, click the *Reset* button, and then confirm by clicking *Yes*. The fields on the Conference Sessions screen are defined in Table 3-4.

Figure 3-4 The Conference Sessions Screen

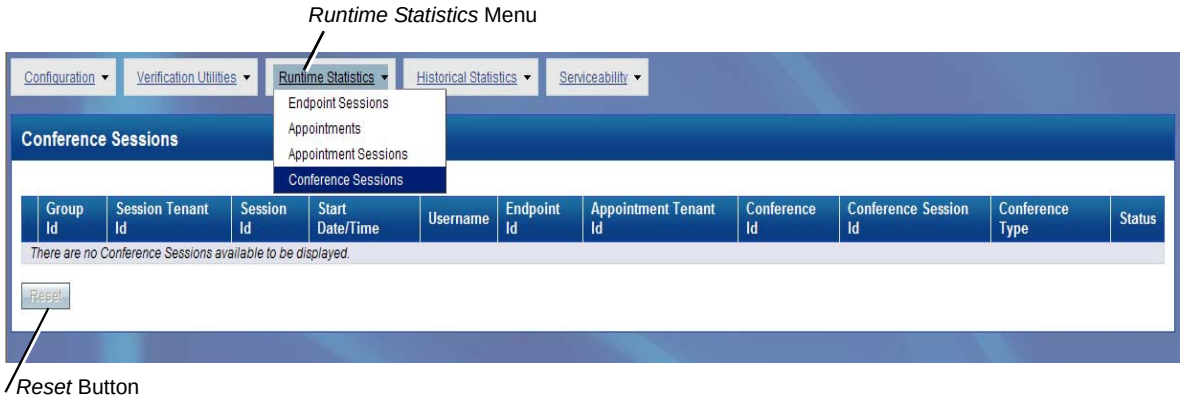


Table 3-4 Fields on the Conference Sessions Screen

Field	Definition
Group Id	The identification code of the B2B Group (if applicable).
Session Tenant Id	The identification code of the business that initiated this session (if applicable).
Session Id	An automatically assigned code that is unique to this session (if applicable).
Start Date/Time	When this session was first started, that is, when the system accepted the login request of the portal client.
Username	The login name of the user who began this conference session.
Endpoint Id	The identification code assigned to this endpoint when the system was configured.
Appointment Tenant Id	The identification code of the business that initiated this appointment.
Conference Id	The identification code devised by the Presenter, and entered by the conference Participants.
Conference Session Id	An automatically assigned code that is unique to this conference session.
Conference Type	Can be two-party or multi-party.

Field	Definition
Status	Idle – Conference session is not part of the conference Disconnected – Conference session was connected and is currently not connected or has left the conference Connected – Conference session has joined Failed – Conference session tried to connect but failed In Progress – Intermediate state between idle and connected.

Note Only applicable fields will be displayed. For example, "Group Id," "Appointment Tenant Id," and "Appointment Id" will only appear on systems that have the B2B capability.

CHAPTER 4

The Historical Statistics

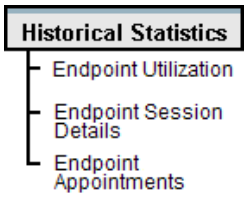
Revised: October 31, 2011, OL-25943-01

This chapter explains the tasks that you can do using the *Historical Statistics* menu from the Cisco HealthPresence *Server Administration* window.

The historical statistics allow you to view information for endpoint activities that have been completed.

These topics are included in this chapter:

- Viewing Information about Past Endpoint Usage
- Viewing Details about Past Endpoint Sessions
- Viewing Information about Past Endpoint Appointments



Viewing Information about Past Endpoint Usage

To display usage statistics for endpoints that have occurred in the past, click *Endpoint Utilization* on the *Historical Statistics* menu. The system displays a screen similar to the one shown in Figure 4-1.

1. Use the *Region* menu to select a particular region, or select *default*.
2. Click the calendar icon on the left to open a calendar and select a starting date.
3. Type the start time (HH:MM:DD).
4. Click the calendar icon on the right to open a calendar and select an ending date.
5. Type the end time (HH:MM:DD).
6. Click the *Go* button.

The fields on the Endpoint Utilization screen are defined in Table 4-1.

Figure 4-1 The Endpoint Utilization Screen

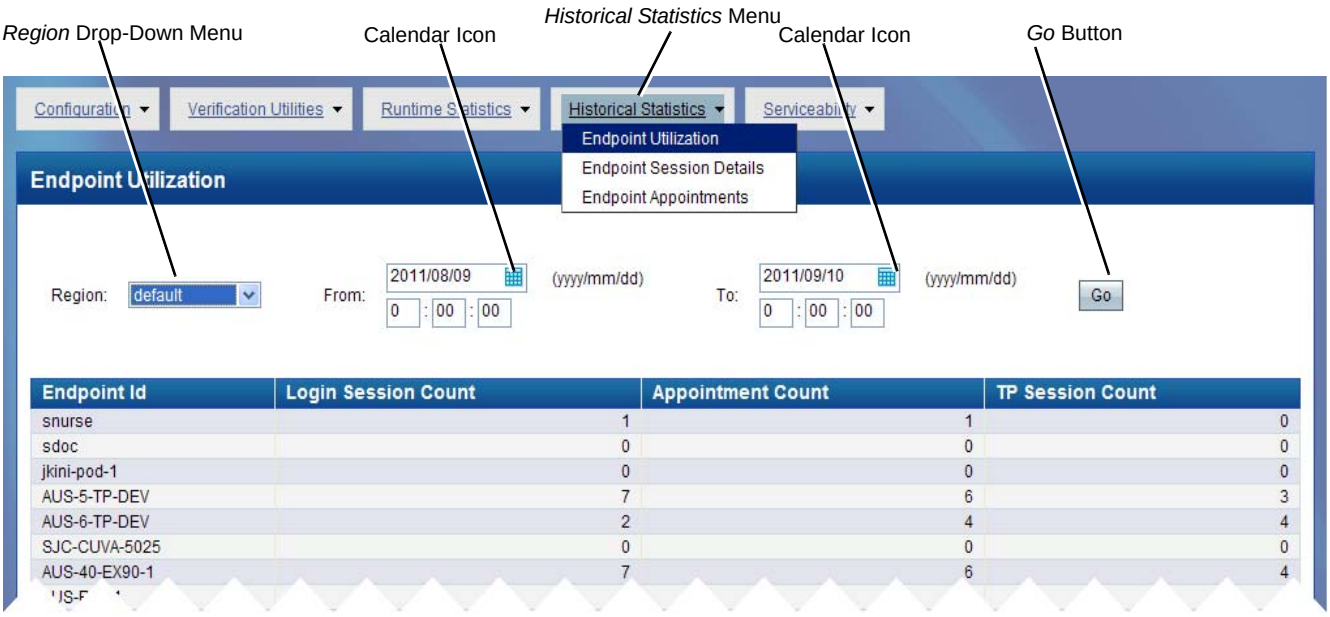


Table 4-1 Fields on the Endpoint Utilization Screen

Field	Definition
Endpoint Id	The identification code assigned to this endpoint when the system was configured.
Login Session Count	The number of login sessions that occurred during the specified time period.
Appointment Count	The number of appointments that occurred during the specified time period.
TP Session Count	The number of telepresence sessions that occurred during the specified time period.

Viewing Details about Past Endpoint Sessions

To display statistics pertaining to endpoint sessions that have occurred in the past, click *Endpoint Session Details* on the *Historical Statistics* menu. The system displays a screen similar to the one shown in Figure 4-2.

1. Use the *Endpoint* drop-down menu to select a particular endpoint.
2. Click the calendar icon on the left to open a calendar and select a starting date.
3. Type the start time (HH:MM:DD).
4. Click the calendar icon on the right to open a calendar and select an ending date.
5. Type the end time (HH:MM:DD).
6. Click the *Go* button.

The fields on the Endpoint Appointments screen are defined in Table 4-3.

Figure 4-2 The Endpoint Session Details Screen

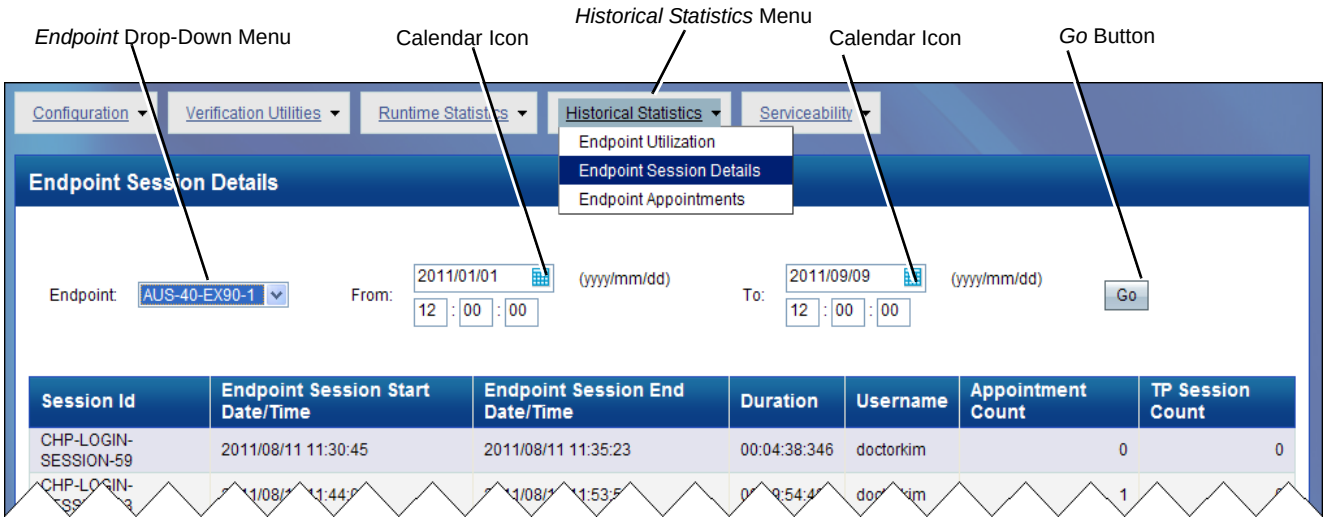


Table 4-2 Fields on the Endpoint Session Details Screen

Field	Definition
Session Id	An automatically assigned number that is unique to this session.
Endpoint Session Start Date/Time	The date and time that this endpoint session began.
Endpoint Session End Date/Time	The date and time that this endpoint session ended.
Duration	The hours, minutes, seconds, and thousandths of a second that this endpoint session lasted.
Username	The username of the user who initiated this endpoint session.
Appointment Count	The number of appointments that occurred during this endpoint session.
TP Session Count	The number of telepresence sessions that occurred during this endpoint session.

Viewing Information about Past Endpoint Appointments

To display a list of endpoint appointments that have occurred in the past, click *Endpoint Appointments* on the *Historical Statistics* menu. The system displays a screen similar to the one shown in Figure 4-3.

1. Use the *Endpoint* drop-down menu to select a particular endpoint.
2. Click the calendar icon on the left to open a calendar and select a starting date.
3. Type the start time (HH:MM:DD).
4. Click the calendar icon on the right to open a calendar and select an ending date.
5. Type the end time (HH:MM:DD).
6. Click the *Go* button.

The fields on the Endpoint Session Details screen are defined in Table 4-2.

Figure 4-3 The Endpoint Appointments Screen

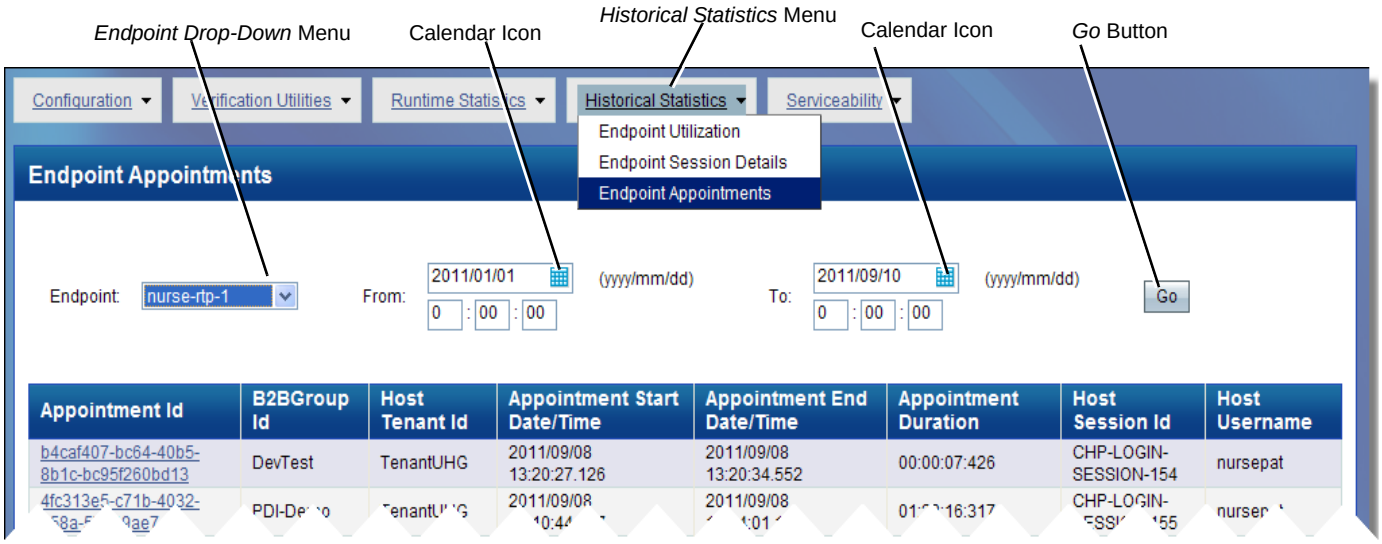


Table 4-3 Fields on the Endpoint Appointments Screen

Field	Definition
Appointment Id	An automatically assigned code that is only valid for this appointment (if applicable).
B2B Group Id	The identification code of the B2B Group (if applicable).
Host Tenant Id	The identification code of the tenant for the user who initiated this appointment.
Appointment Start Date/Time	The date and time that this appointment began. This occurs when the Attendant clicks **Start Appointment.**
Appointment End Date/Time	The date and time that this appointment ended. This occurs when the Attendant clicks on the *End* button at the Attendant station.
Appointment Duration	The hours, minutes, seconds, and thousandths of a second that this appointment lasted.
Host Session Id	The session identification code for the endpoint at which the session was initiated.
Host Username	The username of the user who initiated this appointment.

CHAPTER 5

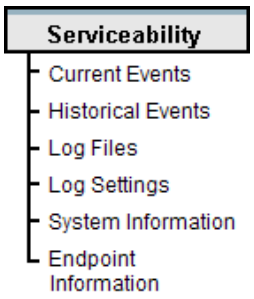
The Serviceability Options

Revised: October 31, 2011, OL-25943-01

This chapter explains the tasks that you can do using the *Serviceability* menu from the Cisco HealthPresence *Server Administration* window. The serviceability screens allow you to view current and past events, and to adjust some parameters.

These topics are included in this chapter:

- Viewing a List of Current Events
- Viewing a List of Historical Events
- Viewing Log Files
- Displaying and Adjusting Log Settings
- Viewing System Information
- Viewing Endpoint Information



Viewing a List of Current Events

Current events are notifications of occurrences or issues that recently occurred and have yet to be acknowledged. To display a list of current events, click *Current Events* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-1.

To change the status of a specific event, do the following:

1. Check the box next to the Event Id.
2. Choose the status in drop down menu for the event. Options are:

- Active - an event has occurred. An event will be in this state until you change it.
- Acknowledge - an event has occurred and been viewed
- Clear - delete the event

3. Then click **Save.**

Figure 5-1 The Current Events Screen

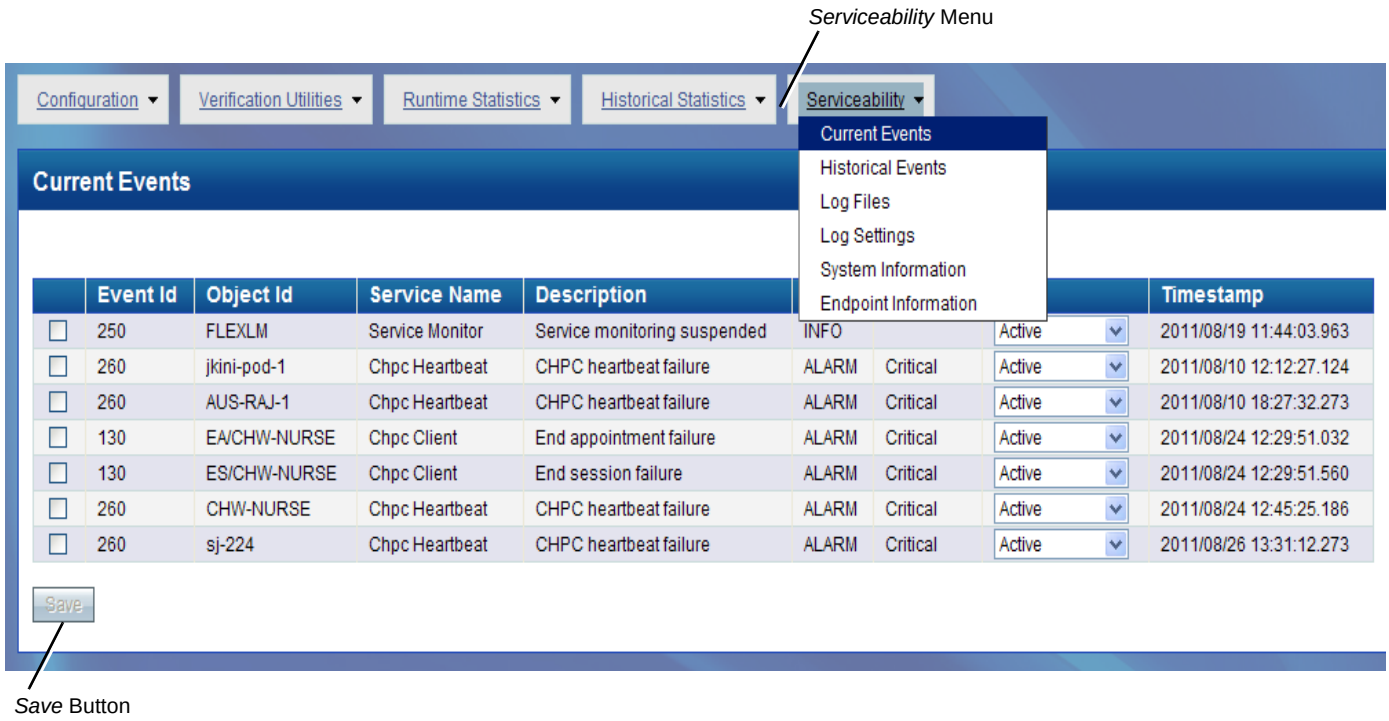


Table 5-1 Fields on the Current Events Screen

Field	Definition
Event Id	The sequential number assigned to this event by the system.
Object Id	The identifier of the object (for example, endpoint ID, data structure, etc.) that was involved in the event.
Service Name	The name of the service where this event occurred.
Description	A brief summary of the action that created the event.

Field	Definition
Type	Can be Alarm or Info. Informational events cannot be cleared. Alarms can be Acknowledged or Cleared.
Severity	This applies to Alarms only. It can be Critical, Major or Minor
State	Can be Active, Acknowledge, or Clear
Time Stamp	The date and time that this event occurred.

Viewing a List of Historical Events

Historical events are issues that have occurred in the past. These issues might include warnings, errors, information, or fatal errors.

To display a list of past events, click *Historical Events* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-2. The fields on the Historical Events screen are defined in Table 5-2.

Figure 5-2 The Historical Events Screen

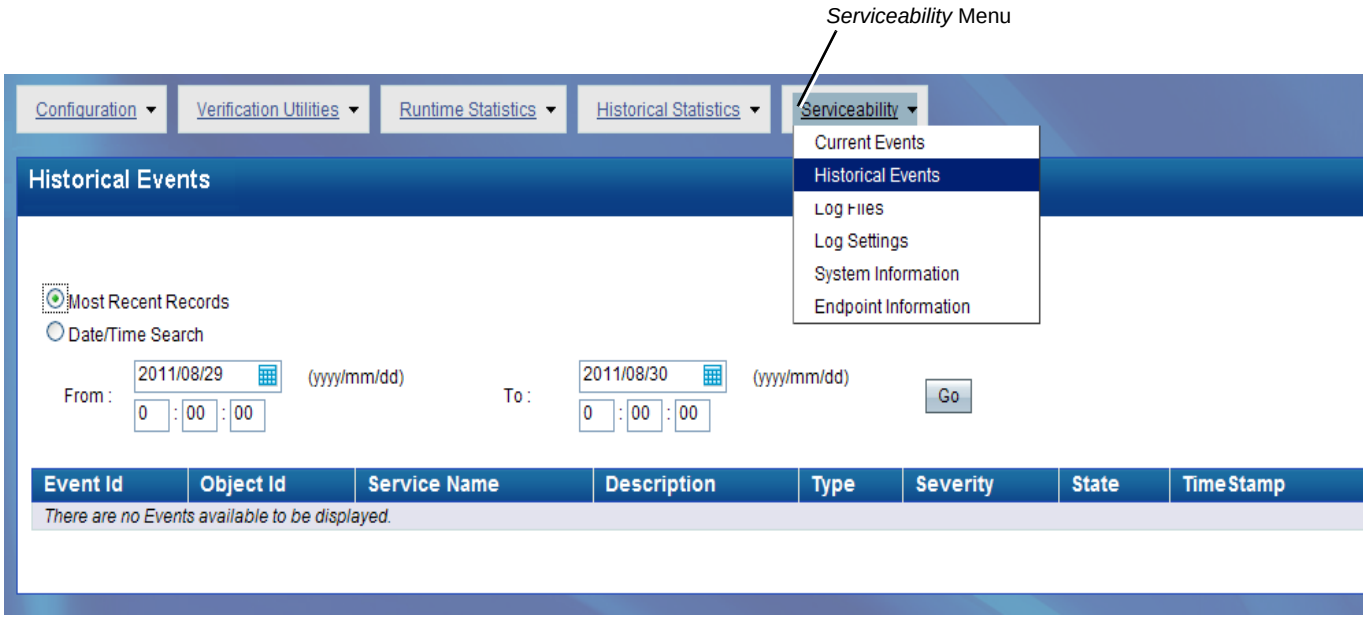


Table 5-2 Fields on the Historical Events Screen

Field	Definition
Event Id	The sequential number assigned to this event by the system.
Object Id	The identifier of the object that was involved in the event.
Service Name	The name of the service where this event occurred.
Description	A brief summary of the action that created the event.
Type	Can be Alarm or Info
Severity	Can be Critical, Major or Minor
State	Can be Active
Time Stamp	The date and time that this event occurred.

Viewing a List of Log Files

Log files are generated when certain events occur. You set the types of events that are logged by adjusting the log settings.

To display a list of log files, click *Log Files* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-3.

1. Use the *Subsystem* drop-down menu to select a particular Cisco HealthPresence module, or select *All*.
2. To download or delete selected files, first click the checkbox (or checkboxes) to the far left of the log(s), then click the appropriate button at the bottom of the page.
3. To view an individual log, click the log *Name* link. You will see a dialog box asking whether you want to view or save this file.
4. To view multiple logs, check the box next to each log that you want to view. Then click **Download.**

The fields on the Log File screen are defined in Table 5-3.

Figure 5-3 The Log Files Screen

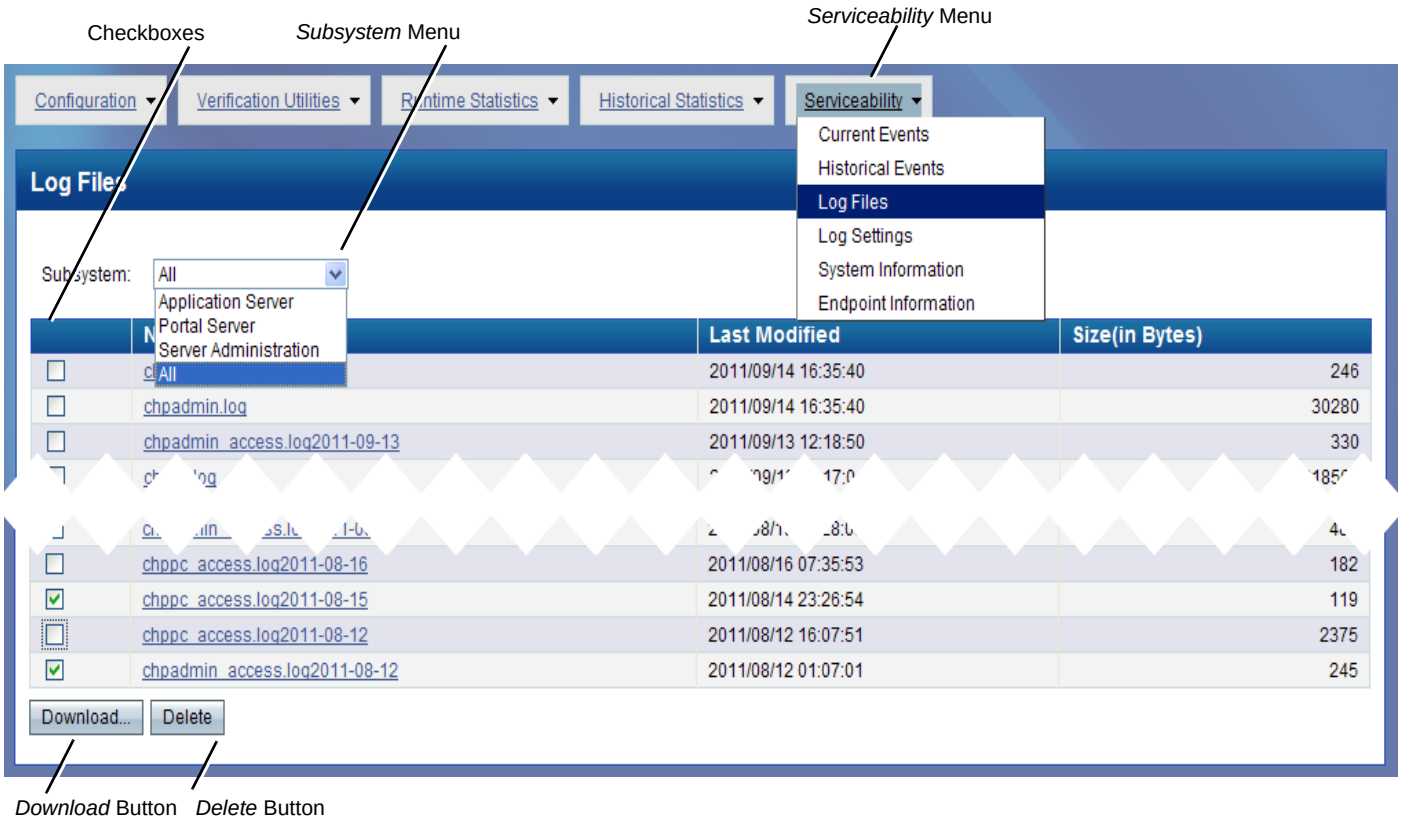


Table 5-3 Fields on the Log Files Screen

Field	Definition
Name	This name is assigned when the log file was created.
Last Modified	The date and time that this file was last modified.

Field	Definition
Size	The size of the log file.

Displaying and Adjusting Log Settings

Log settings control the types of information that is included in the log files. To display the log settings, click *Log Settings* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-4. The settings that you can choose for the listed servers are defined in Table 5-4.

Note The settings for Server Administration, Portal Server and Application Server are independent of one another. For example, Server Administration can be set to Debug, Portal Server can be set to Warning, and Application Server can be set to Error.

Figure 5-4 The Log Settings Screen

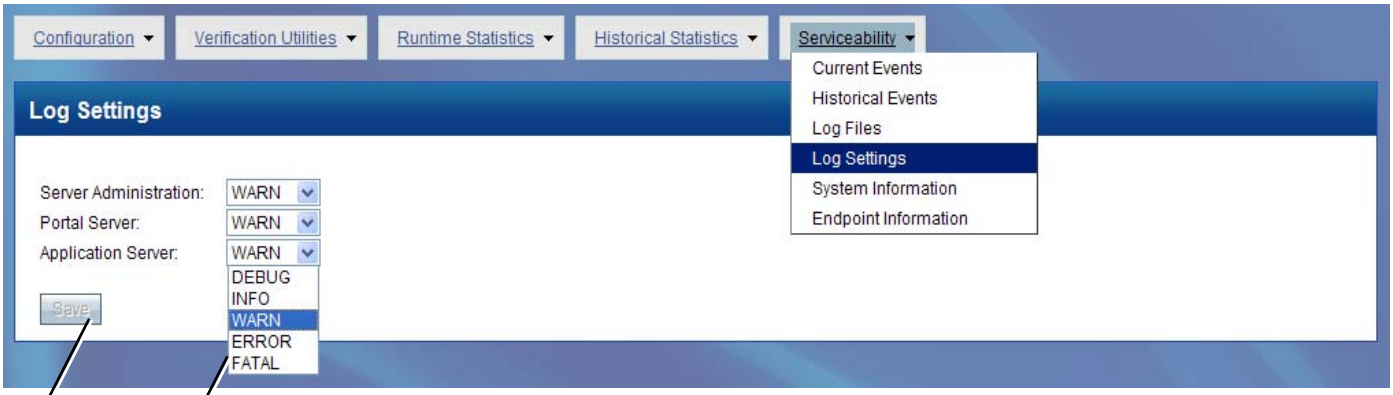


Table 5-4 Log Settings Options

Log Setting	Definition
Debug	Choose this option to display detailed debugging information to use for troubleshooting software bugs and other issues.
Info	Choose this option to log all informational messages, warning information, error information, and fatal errors.
Warn	Choose this option to log all warning information, error information, and fatal errors.
Error	Choose this option to log all error information including fatal errors.
Fatal	Choose this option to log only information about fatal errors.

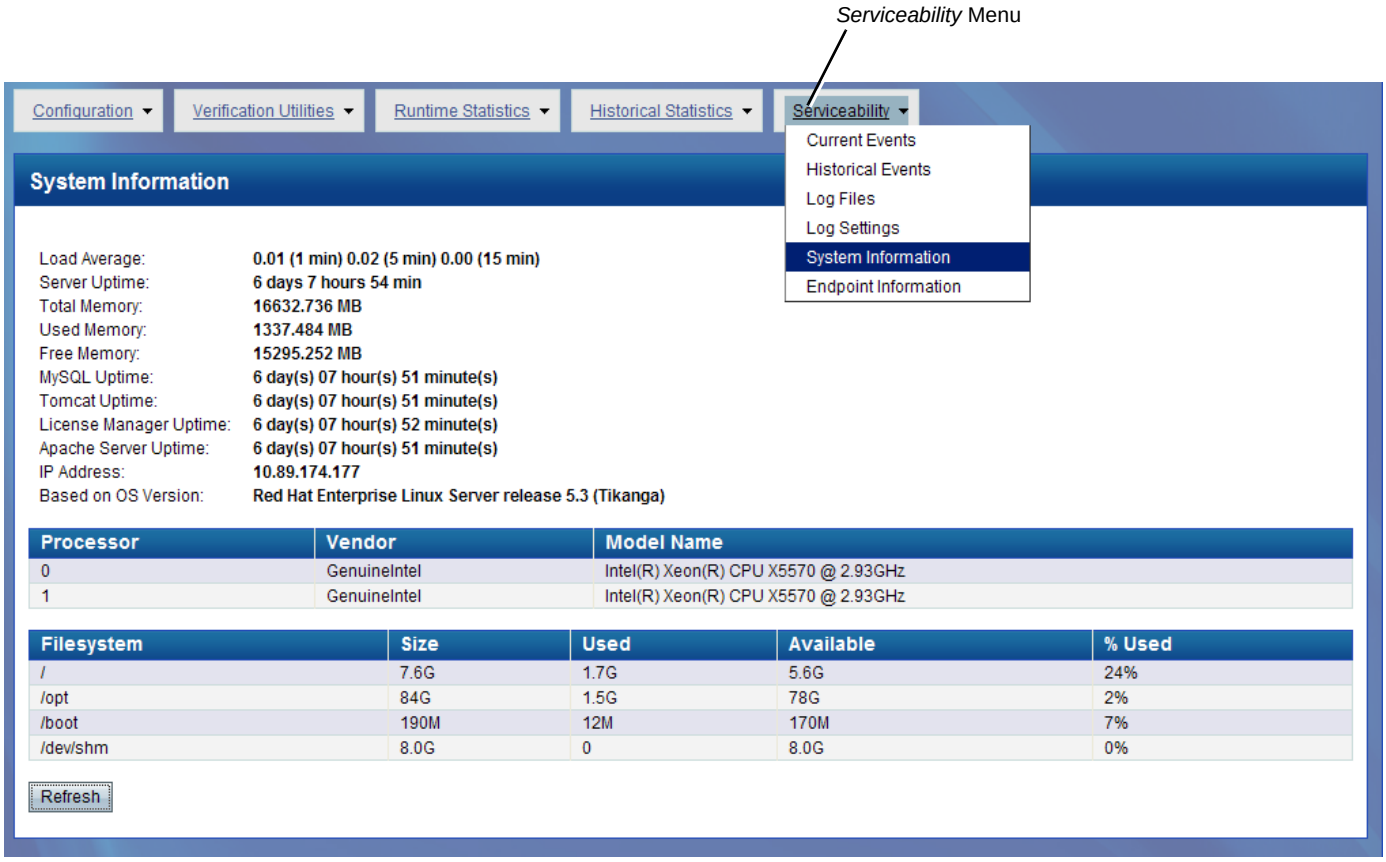
Viewing System Information

This screen provides information about the Cisco HealthPresence Connect Server, including memory and storage usage, uptime of various processes, and the IP address.

Note This screen provides a snapshot of the system at the time the information was requested. To get up to date information, click **Refresh** on the bottom left of the window.

To display system information, click *System Information* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-5.

Figure 5-5 The System Information Screen

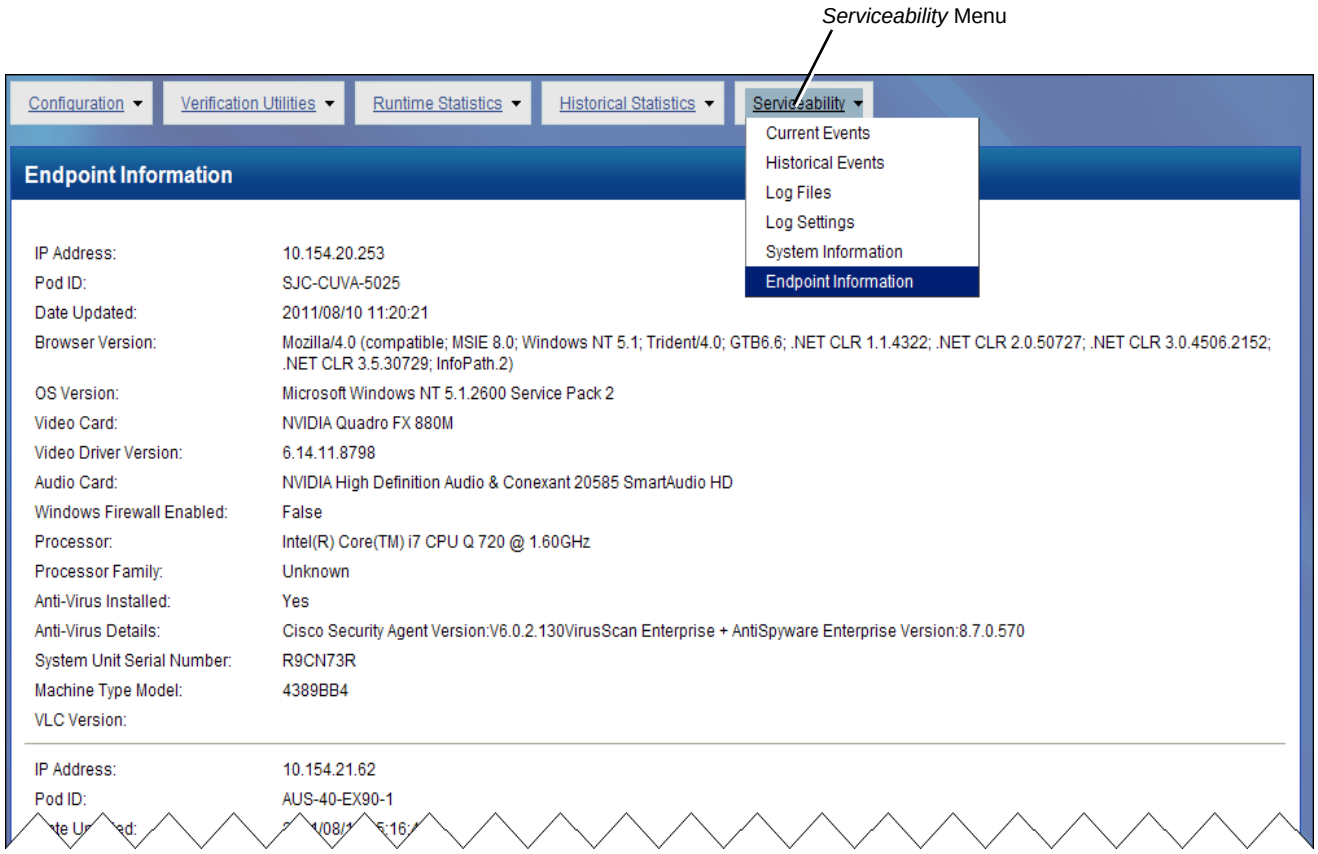


Viewing Endpoint Information

This screen provides information about the individual endpoints including the software that is running on the Cisco HealthPresence system, and details about the Cisco HealthPresence system hardware.

To display endpoint information, click *Endpoint Information* on the *Serviceability* menu. The system displays a screen similar to the one shown in Figure 5-6.

Figure 5-6 The Endpoint Information Screen



GLOSSARY

Revised: October 31, 2011

A

AMD — AMD Global Telemedicine. The company that provides the medical equipment for examinations.

Attendant — The licensed health care professional who attends the patient. This role includes greeting the patient, taking the patient's vitals, and using the medical devices to assist the Provider in evaluating the patient. An Attendant can be a medical technician, a nurse, a nurse practitioner, or a physician.

Attendant Appliance — The computer at the Attendant station. It runs the applicable Cisco HealthPresence software.

Attendant Station — The place where the patient and the Attendant meet. This area contains the medical device(s) used by the Attendant, the video conferencing system, and the Cisco HealthPresence Attendant Appliance. It may also contain special furniture offered by Cisco.

B

B2B — Business-to-Business. The Cisco HealthPresence system allows communication between stations in the same Business Entity, or from one Business Entity to another (B2B).

Business Entity — The Attendant and Provider stations managed by a single Cisco HealthPresence Application Server.

B2B Group — A group of business entities whose endpoints can participate in an appointment.

B2B Manager — A Cisco HealthPresence component that manages communication among different business entities.

C

Cisco HealthPresence Administration — The application used by the installation team to configure, administer, and manage the Cisco HealthPresence Application Server and the Cisco HealthPresence Portal.

Cisco HealthPresence Application Server (CHPAS) — The Cisco HealthPresence component that maintains the master information of resources and manages conferences, sessions, and appointments. CHPAS interfaces with CHP Admin, CHP Portal, Unified Communications (UC) servers, and the CHP Connect software at the endpoints. For B2B appointments and conferences, CHPAS interfaces with the B2B Manager.

Cisco HealthPresence B2B Administration — The application used by the installation team to configure, administer, and manage the B2B Manager.

Cisco HealthPresence B2B Manager — The application that manages conferences, sessions, and appointments among endpoints residing in different tenants.

Cisco HealthPresence Connect — The Cisco HealthPresence software that runs on the Appliance at both the attendant and provider endpoints.

Cisco HealthPresence Connect Server — The Cisco HealthPresence software that runs in a data center and manages appointments and conferences among Cisco HealthPresence endpoints.

Cisco HealthPresence Device — Refers to the Cisco HealthPresence Solution, as defined by the FDA.

Cisco HealthPresence Endpoint — A video endpoint, the Cisco HealthPresence software running on an Attendant or Provider appliance, and, optionally, medical devices.

Cisco HealthPresence Portal — The master portal that interfaces with the CHPAS and acts as a proxy for requests from the Attendant or Provider Appliances. It maintains the portal login sessions and provides the interface for the CHPAS to validate sessions.

Cisco HealthPresence Solution — A solution that combines video, medical devices, computer networking, and a graphical user interface to enable Providers to offer medical consultations to patients at remote Attendant stations.

Cisco Unified Communications Manager — The application that extends enterprise telephony features and capabilities to packet telephony network devices, such as IP phones and multimedia applications. Open telephony application interfaces make possible services such as multimedia conferencing and interactive multimedia response systems.

Codian MCU — A multi-point control unit (MCU) used to switch video from Tandberg video endpoints.

Conference — A teleconference using the Cisco HealthPresence solution. Can be a regular conference (between members of the same Business Entity), or a B2B Conference (between members of the same B2B Group).

D

Default Region — The region available on an install that includes all the resources controlled by this CHPAS. If your system does not require partitioning of resources, you do not need to configure additional regions.

E

E- Pen — Electronic Pen. Allows physicians to write online prescriptions. See "Setting Up the E-Pen Feature" on page 2-32.

Endpoint The Cisco HealthPresence Connect software running on the Attendant or Provider Appliance.

EMR Electronic Medical Records. If your system includes the necessary software and is configured to enable an EMR interface, then you can save data from the appointment to EMR. See "Configuring for Electronic Medical Records (EMR)" on page 2-31.

H

Hosted A software delivery model in which the Cisco HealthPresence software and associated client data reside in a central location managed by a hosting service, and are accessed by clients using a web browser.

M

Medical Devices Collection of medical devices used with the Cisco HealthPresence system.

Medical Telemetry The technology that allows the Attendant to measure and report medical information remotely.

Multi-Party An appointment option that allows you to include more than one Provider in an appointment. If your system is configured to support multi-party calls, the Attendant chooses whether the call is going to be a two-party call (a point-to-point call) or a multi-party call (a bridge call). May also be called "Multi-Point."

P

Participant The user role for the user who joins in a conference initiated by a Presenter.

Presenter The user role for the user who initiates a conference.

Provider The licensed medical professional who provides medical evaluations from a remote site. Most often this will be a physician, a physician's assistant, or a nurse practitioner.

Provider Appliance The computer located at the Provider station. It runs the applicable Cisco HealthPresence software.

Provider Station The place where the Provider sits during the teleconference. This area contains the video conferencing system and the Cisco HealthPresence Provider Appliance. It may also contain special furniture offered by Cisco.

R

Region A subset of endpoints and multi-point bridges controlled by a single Cisco HealthPresence Application Server or Tenant. See "Working with Regions" on page 2-9.

S

Site Admin Site Administrator. The person who maintains user accounts on the Cisco HealthPresence system.

T

Telehealth Appointment A Cisco HealthPresence medical appointment in which the Attendant can share patient vitals, video streams, and audio streams, with a Provider in a different location.

Telemetry The technology that allows a health care professional to measure patient medical data locally, and report the information to a physician in a different location.

Tenant An instance of the Cisco HealthPresence software running on a physical server in its own virtual machine. See "Working with Tenant Settings" on page 2-7.

U

User Role Your user role determines which screens you see, and which functions you can perform. User Accounts are configured so that users with a particular role (or roles) see only the screens and options appropriate to that job description. Any given user can have from one to five roles within one User Account. The Site Administrator configures the User Accounts.

W