



## **Cisco HealthPresence Site Administration Guide**

V 2.1.1  
January 9, 2013

**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](mailto:healthpresence-support@cisco.com)

Text Part Number: OL-28683-01

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.

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 2.1.1 Site Administration Guide*  
© 2013 Cisco Systems, Inc. All rights reserved.





# CONTENTS

## CHAPTER 1

### Introducing the Cisco HealthPresence Solution 1-1

- About This Site Administration Guide 1-2
  - Site Administration Audience 1-2
  - Site Administration Scope 1-2
- An Overview of the Cisco HealthPresence Solution 1-3
- Understanding User Roles 1-5
- Understanding Provider Groups 1-6
- A Sample Workflow 1-6
  - The Attendant Begins the Appointment 1-6
  - A Provider Joins In 1-6
  - The Examination Begins 1-6
  - The Appointment Ends 1-7

## CHAPTER 2

### Getting Started as Site Administrator 2-1

- Site Administrator Tasks 2-1
- Things the Site Administrator Should Know 2-2
  - About Authentication 2-2
    - Dedicated (Cisco HealthPresence) Authentication 2-2
    - External Authentication 2-2
    - Mixed Authentication 2-3
  - About Your User Account 2-3
  - About the Security Option Defaults 2-3
    - Forced Password Change 2-4
    - Account Inactivity 2-4
    - Strong Passwords 2-4
    - Password Expiration 2-4
    - Password Reuse 2-4
    - User lockout 2-4
  - Cisco HealthPresence User Names 2-4
  - Cisco HealthPresence Provider Group Names 2-5
- Getting Started on the System 2-5
  - Gaining Access to the System (If Necessary) 2-5
    - Using the CHP Portal Quick Link 2-5
    - Windows 7 User Login 2-6

Log Off and then On Again	2-6
Logging In to the Cisco HealthPresence System	2-6
When You Have More Than One Role	2-7
Changing Your Password	2-8
Locking and Unlocking the Application	2-8
Lock the Application When You Leave	2-8
Unlock the Application When You Return	2-8
Logging Out of the System	2-10
Getting Into and Out of Desk-Top Mode	2-10
Getting Into Desk-Top Mode	2-10
Getting Back Into Browser Mode	2-10

## CHAPTER 3

### Site Administration Tasks 3-1

Getting Started	3-2
Site Administrator Tasks	3-2
Adding a New User Account	3-3
Deleting a User Account	3-5
Enabling a User Account	3-5
Disabling a User Account	3-6
Updating a User Account	3-6
Unlocking a User Account	3-7
Configuring Provider Groups	3-8
General Characteristics	3-8
Provider Group Naming Considerations	3-9
Adding Provider Groups	3-9
Updating Provider Groups	3-10
	3-11

## CHAPTER 4

### Troubleshooting User Problems 4-1

Problem with Login or Password	4-2
Problem with Conferencing?	4-2
If You Can't See Anything on the Screen	4-2
If You Can't Hear the Presenter or Participants	4-2
Problem Accessing Data?	4-3
If the Provider Cannot Access Data	4-3
No Vitals Data?	4-3
No Video Image?	4-3
No Stethoscope Sounds?	4-3

No ECG Data?	4-3
If the Attendant Cannot Access Data	4-4
No Vitals Data?	4-4
No Video Image?	4-4
Blurry Video Image?	4-4
Video Image Stopped?	4-4
No Stethoscope Sounds?	4-4
No ECG Data?	4-5
Problem with Medical Devices?	4-6
Double-Checking the Vital Signs Monitor Status	4-6
Checking the Individual Device Status	4-7
Contact Support?	4-7

---

**APPENDIX A**
**Worksheets A-1**

Adding Providers	A-1
Enabling Providers	A-1
Adding Attendants	A-2
Enabling Attendants	A-2
Adding Provider Groups	A-3

---

**APPENDIX B**
**Types of Audio Equipment B-1**


---

**GLOSSARY**





# CHAPTER 1

## Introducing the Cisco HealthPresence Solution

---

**Revised: January 9, 2013, OL-28683-01**

This introduction explains the audience, purpose, and scope of *Cisco HealthPresence 2.1.1 Site Administration guide*. It provides an overview of the Cisco HealthPresence 2.1.1 solution, and then describes the users and their workflow.

Topics in this chapter include:

- About This Site Administration Guide
  - Site Administration Audience
  - Site Administration Scope
- An Overview of the Cisco HealthPresence Solution
- The Importance of User Roles
- A Sample Workflow
  - The Attendant Begins the Appointment
  - The Provider Joins In
  - The Examination Begins
  - The Appointment Ends

# About This Site Administration Guide

This section describes this guide, and explains who should use it, what it includes, and what it doesn't include.

## Site Administration Audience

This Administration Guide is for the user who is responsible for maintaining the user accounts on the Cisco HealthPresence™ system. At some sites, more than one person may have this responsibility. This user role is called “Site Administrator,” or “Site Admin,” for short. It has a special, unique type of user account.

## Site Administration Scope

This guide provides an overview of the Cisco HealthPresence system, and explains the tasks appropriate for the Site Administrator as described in [Site Administrator Tasks, page 2-1](#). There is also a rudimentary troubleshooting section so that the Site Administrator can handle simple user issues.

Other users who have maintenance responsibilities are described below. Instructions for these tasks are NOT included here.

**Computer Security Maintenance:** Maintaining the computer security aspects of the Cisco HealthPresence solution is critical, but it is outside the scope of the Site Administrator responsibilities, and hence is not covered in this document. Security maintenance includes the following tasks:

- Update the Windows Security as needed.
- Update the McAfee DAT files.

**Medical Equipment Testing:** Instructions for this task are covered in the *Cisco HealthPresence 2.1.1 User Guide for Neurosynaptic*. This document can be found at: [http://www.cisco.com/en/US/products/ps11966/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps11966/products_user_guide_list.html).

**Configuring Cisco HealthPresence Endpoints:** Instructions for this task are covered in the *Cisco HealthPresence 2.1.1 Data Server Installation and Administration Guide*. This document can be found at: [http://www.cisco.com/en/US/products/ps11966/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11966/prod_installation_guides_list.html).



# An Overview of the Cisco HealthPresence Solution

The Cisco HealthPresence solution allows a health care Provider to evaluate 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. An Attendant can use an exam camera to enable the Provider to see close ups of a patient's throat. Also, an Attendant can place a stethoscope on a patient's chest, and the physician can hear the heartbeat from a remote location.

The system allows patients to consult with specialists without traveling to the specialist's location. If the multi-party feature has been implemented, the specialist and the attending physician can both participate in the same patient conference.

To see an example of the system in a clinical setting, refer to [Figure 1-1](#). The table ([Table 1-1](#)) on the following page explains the roles and components shown in the illustration.

**Figure 1-1 The Cisco HealthPresence Solution Attendant Station**



**Table 1-1 Components and Roles in a Clinical Setting**

Item	Explanation
Attendant	The licensed health care professional who attends the patient. This role includes greeting the patient, taking the patient's vitals, and using the Interoperable Medical Devices <sup>1</sup> to assist the Provider in evaluating the patient. An Attendant can be a medical technician, a nurse, a nurse practitioner, or a physician.
Attendant Station	The place where the patient and the Attendant meet. This area contains the Interoperable Medical Device(s) used by the Attendant, the video conferencing system, and the Cisco HealthPresence Attendant Appliance or personal computer.
Interoperable Medical Device	The third-party medical devices, tested and validated for compatibility by Cisco, that take and report certain medical information from the patient and provide it directly, in electronic form, to the Cisco HealthPresence Solution.
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.

Item	Explanation
Provider Station	The place where the Provider sits during the Cisco HealthPresence appointment. This area contains the video conferencing system and the Cisco HealthPresence Provider Appliance or personal computer..

1. NOTE: Interoperable Medical Devices are available only from the manufacturer of such devices or its authorized resellers and distributors. Cisco is not a reseller or distributor of such devices. Interoperable Medical Devices are not available in all countries. To find out if the Interoperable Medical Devices are available in your country, contact the manufacturer or the seller of the Interoperable Medical Device. For information on how to use any Interoperable Medical Device see the instructions for use provided with that device. Cisco makes no representations or warranties regarding the features, functionality or intended use of the Interoperable Medical Devices.

# Understanding User Roles

A user's role determines which screens that user will see, and which functions he or she 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. As the Site Administrator, it is your responsibility to assign and maintain these user accounts.

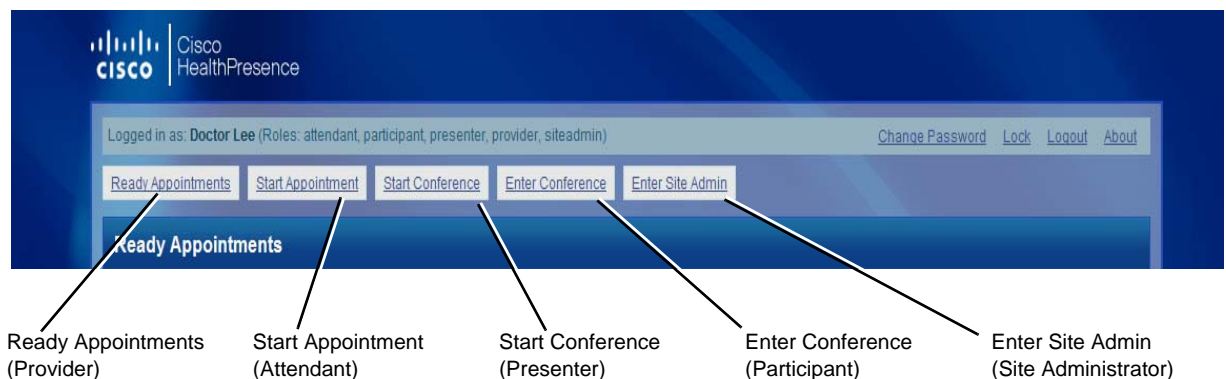
The five different user roles are listed in [Table 1-2](#). The roles are ranked in the order shown in the table. For example, someone with both a Provider and Presenter role would default to the Provider pathway. As another example, if the Site Administrator is also a Presenter, the default would be Presenter, which is higher up on the list.

When you log in, you see the main screen for your highest level user role; however, you can move to another screen by clicking the appropriate link. The screen selections for each user role are shown in [Figure 1-2](#). In the example, the user has access to all five screens. The window displayed is the Ready Appointments window, as the Provider role is the highest in the list.

**Table 1-2 Five Possible User Roles**

User Role	Primary Screen
Provider	The physician or other medical professional who evaluates the patient data begins with the <i>Ready Appointments</i> screen.
Attendant	The medical professional who attends the patient begins with the <i>Start Appointment</i> screen.
Presenter	The person who initiates the conference begins with the <i>Start Conference</i> screen.
Participant	A person who joins a conference begins with the <i>Enter Conference</i> screen.
Site Administrator	The person who maintains user accounts on the system begins with the <i>Enter Site Admin</i> screen.

**Figure 1-2 Task Links Appropriate to Each User Role**



## Note

If you have only one user role, you will not see the links for the other screens; you will go directly to the screen that is appropriate for your tasks.

# Understanding Provider Groups

Provider Groups allow an Attendant to queue a patient appointment to a number of providers, thereby allowing the first available Provider to take the appointment. This is especially useful for unscheduled appointments (drop-ins) or for consultations with a specialist.

## A Sample Workflow

This section provides a summary of a typical medical session.

### The Attendant Begins the Appointment

Think of this section as an executive summary. You aren't expected to try to read the details of the screens shown in these illustrations. If you want to know more about these functions, see the User Guide, which includes full-sized versions of all of these screens.

- 
- 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 or Provider Groups, and selects a Provider or Provider Group.
  - 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 Ready Appointments list of every Provider in a selected Provider Group or if a single Provider was selected, just one Provider's Ready Appointments list.

### A Provider Joins In

- Step 4** A Provider comes into the Provider station, logs in, and sees a list of all of the "ready" appointments.
- Step 5** A 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 teleconference.  
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** At any point in the appointment, the Attendant can invite a consult into the appointment (if the system was installed with that capability enabled).
- Step 10** The Provider evaluates the data, and communicates with the patient and the Attendant.

## The Appointment Ends

- Step 11** The Provider exits the appointment.
- Step 12** The Attendant does any necessary post-appointment work, such as saving or printing the patient data.
- Step 13** The Attendant ends the appointment.





## CHAPTER 2

# Getting Started as Site Administrator

---

**Revised: January 9, 2013, OL-28683-01**

This chapter includes information that enables a Site Administrator to make better-informed configuration decisions. It also enables the Site Administrator to assist end users if they have trouble accessing the system.

Topics in this chapter include:

- Site Administrator Tasks
- Things the Site Administrator Should Know
  - About Authentication Types
  - About Security Option Defaults
  - About Naming Conventions
- Getting Started on the System
  - Gaining Access to the System (If Necessary)
  - Logging In to the Cisco HealthPresence System
  - When You have Multiple User Roles
  - Changing Your Password
  - Locking and Unlocking the Application
  - Logging Out of the System
  - Getting Into and Out of Desk-Top Mode

## Site Administrator Tasks

The Site Administrator tasks vary based on which options are configured in the system. The following list of tasks is a complete list, but the tasks required at your site may be a subset of these tasks.

- Add users to the system
- Enable (externally-authenticated) users to access the system
- Update user accounts
- Delete user accounts
- Disable (externally-authenticated) users from accessing the system
- Unlock user accounts
- Reset passwords
- Add Provider Groups
- Update Provider Groups
- Delete Provider Groups

# Things the Site Administrator Should Know

This section provides background information that will help you understand how to best perform the Site Administration Tasks.

This section describes:

- Authentication – Determines who has access to the system.
- Your User Account – How and why it is unique.
- Security Options – Allow you to maintain the integrity of the system that you set up.
- Naming Conventions – Enable you to organize the user accounts or Provider Groups in a logical way.

## About Authentication

The Cisco HealthPresence System uses three types of authentication. Depending on the authentication used, the Site Administrator Tasks vary.

### Dedicated (Cisco HealthPresence) Authentication

With this type of authentication, all usernames, passwords, and user attributes are stored in a dedicated Cisco HealthPresence directory. When using dedicated authentication, the Site Administrator does the following tasks:

- Add users
- Update users
- Delete users
- Unlock users
- Reset passwords

### External Authentication

Cisco HealthPresence supports authentication of user names using an external directory. Two types of directories are supported:

- Directories that supports the Lightweight Directory Access Protocol (LDAP)<sup>1</sup>. This type of authentication allows a single user name and password to be used for access to the Cisco HealthPresence system and any other systems that use the external LDAP directory for authentication. When users change their passwords on the external directory, the same password works for access to Cisco HealthPresence.
- Directories that support the Cisco HealthPresence Authentication Connector. This connector allows third party applications and Cisco HealthPresence to use a common (non-LDAP) directory to authenticate users.

If your site uses external authentication, users are authenticated against an external directory. However, attributes that are specific to the Cisco HealthPresence system are stored in a dedicated directory.

1. LDAP is an Internet protocol used to look up encryption certificates and other directory-like information on a network.



When using external authentication, the Site Administrator does the following tasks:

- Enable users
- Update users
- Disable users

## Mixed Authentication

With this type of authentication, usernames can be authenticated against either the Cisco HealthPresence directory or an external directory. When using mixed authentication, the Site Administrator does the following tasks:

- Add users (if the user should be authenticated against the dedicated Cisco HealthPresence directory)
- Delete users (if the user was Added)
- Enable users (if the user should be authenticated against an external directory)
- Disable users (if the user was Enabled)
- Update users
- Unlock users (if the user should be authenticated against the dedicated Cisco HealthPresence directory)
- Reset passwords (if the user should be authenticated against the dedicated Cisco HealthPresence directory)

## About Your User Account

As a security precaution, the Site Administrator account is always authenticated against the local Cisco HealthPresence directory, regardless of the type of authentication used for other user accounts. This account is also not locked out for account inactivity.

## About the Security Option Defaults

The Security Options described here are available to sites that use the Dedicated Cisco HealthPresence Authentication type and the Mixed Authentication type. How these options are implemented is determined when the product is installed. The Site Administrator cannot change these settings (but the Cisco HealthPresence Server Administrator can). They are described here so that you can answer questions from the users, if necessary.

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.
- Strong Passwords – Seven-character minimum, two types of symbols.
- Password Expiration – After ninety days.
- Password Reuse – Checks last four passwords.
- User Lockout – After six unsuccessful attempts.

## Forced Password Change

By default, when a new user account is created or when the password is changed by somebody other than the actual user, the user must change the account password the first time that he or she logs into the system. This feature can be turned off.

## Account Inactivity

By default, accounts that have been inactive for ninety days will be automatically disabled. The Site Administrator must unlock the account before it can be used. This feature can be turned off, and the inactivity time can be configured when the system is installed. This policy is not applied to the Site Admin account.

## Strong Passwords

By default, passwords must be at least seven characters long, and must include at least two character types (upper case, lower case, numbers, symbols). This policy can be turned off, and the minimum length and minimum number of characters types can be configured.

## Password Expiration

By default, passwords will expire and have to be changed after ninety days. This feature can be turned off, and the expiration time can be configured.

## Password Reuse

By default, the system saves four old passwords, and does not allow the user to use them again. This feature can be turned off, and the number of saved passwords can be configured.

## User lockout

By default, after six unsuccessful login attempts, an account will be locked. The Site Administrator can unlock these accounts. This policy can be turned off, and the number of unsuccessful login attempts can be configured.

## Cisco HealthPresence User Names

The Cisco HealthPresence usernames, display names and passwords can be up to thirty characters long and can include letters, numbers, dashes, and underscores. Passwords are case-sensitive. Usernames are not case sensitive; however, the system will not allow you to use two names that differ only in that one is capitalized and one is not. For example, a user can type in NursePat, nursepat, or NURSEPAT, but no other user can have any of these for a username.

The precise requirements at your site will depend on what choices were made when your system was installed. (See [“About the Security Option Defaults”](#) on page 2- 3).

**Tip**

When assigning usernames, you will need to strike a balance regarding the length of the name. You will need to consider the size of your organization and be sure to use enough characters to insure that each username is unique. But, you do not want to create lengthy usernames, as the medical professionals often log in several times daily, and they will not appreciate having huge strings of characters to type.

## Cisco HealthPresence Provider Group Names

The Cisco HealthPresence Provider Group names can be up to thirty characters long and can include letters, numbers, dashes, and underscores. Provider Group names are not case sensitive; however, the system will not allow you to use two names that differ only in that one is capitalized and one is not.

## Getting Started on the System

Most of the instructions here apply to all types of users, yourself included. Special notes have been inserted when the information is pertinent to the Site Administrator only. If you want to know exactly what the users know about using the system, refer to the *Cisco HealthPresence Users Guide*. You can also, if appropriate, refer a user to that manual.

## Gaining Access to the System (If Necessary)

Normally, you will begin your sessions from the Cisco HealthPresence *Login* screen (shown in [Figure 2-4 on page 2-7](#)); however, if you don't see that screen:

- You may need to click the CHP Portal quick link.
- You may need to log in to Windows.
- You may need to log off and log in again.

**Note**

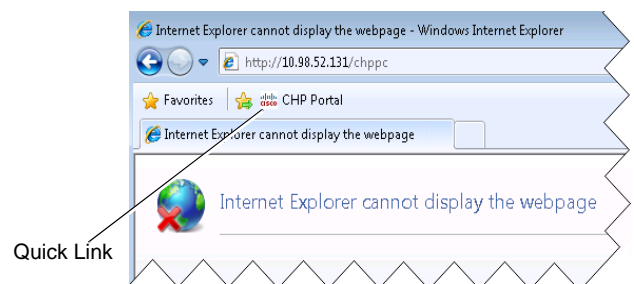
If the suggestions provided here don't work, see [“Contact Support?” on page 4- 7](#).

## Using the CHP Portal Quick Link

If you see the message *Page Not Found*, *Service Unavailable*, or something similar, click the CHP Portal quick link (see [Figure 2-1](#)).

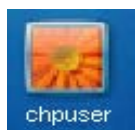
If you are logged in, and you see a *You have been logged out...* message, and, when you click *OK*, you see *Page Not Found*, *Service Unavailable*, or a similar message, click the CHP Portal quick link (see [Figure 2-1](#)) every minute or so for about five minutes. If service is not restored, see [“Contact Support?” on page 4- 7](#).

**Figure 2-1 The CHP Portal Quick Link**



## Windows 7 User Login

**Figure 2-2** A Sample Windows 7 User Icon



If your system has been powered off, either deliberately or accidentally, you will need to click on *chpuser* (see [Figure 2-2](#)), and then enter the Windows password for your installation. You will then see the Cisco HealthPresence login screen.



**Note**

**Note for the Site Administrator:** You may be expected to know the Windows password. This will have been assigned when your system was installed.

## Log Off and then On Again

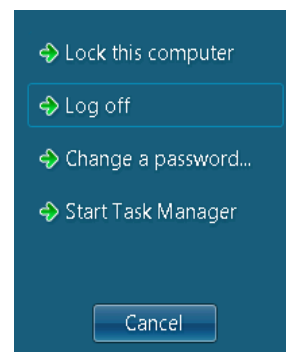
If you see a blank screen, it may be because someone has accidentally closed the Internet Explorer browser. If this happens:

1. Press the Ctrl + Alt + Del keys on your keyboard.  
You will see a screen like the one shown in [Figure 2-3](#).

2. Click on the **Log off** selection.

The system will display the Cisco HealthPresence *Login* screen (see [Figure 2-4](#)).

**Figure 2-3** The Log Off Selection



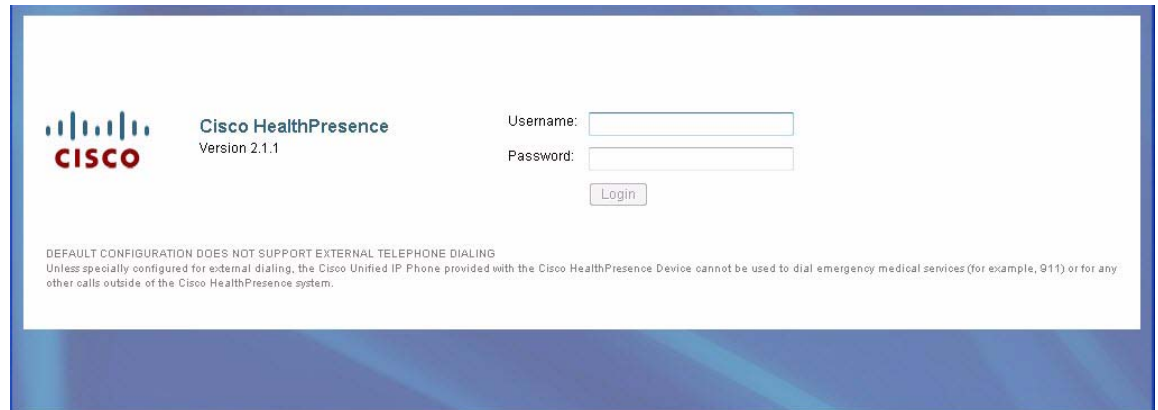
**Note**

**Note for the Site Administrator:** This is the standard Windows operating system procedure for logging on and off, but some of your users may not be familiar with it. What isn't standard is that Internet Explorer automatically launches when someone logs in at the Cisco Health Presence login screen.

## Logging In to the Cisco HealthPresence System

When you see the *Login* screen:

1. Type your *Username* and *Password* in the boxes provided.
2. Click the **Login** button.

**Figure 2-4** The Cisco HealthPresence Login Screen


The screenshot shows the Cisco HealthPresence login interface. On the left is the Cisco logo. To its right, it says "Cisco HealthPresence Version 2.1.1". On the right side, there are two input fields: "Username:" and "Password:". Below these is a "Login" button. At the bottom, there is a disclaimer in small text: "DEFAULT CONFIGURATION DOES NOT SUPPORT EXTERNAL TELEPHONE DIALING. Unless specially configured for external dialing, the Cisco Unified IP Phone provided with the Cisco HealthPresence Device cannot be used to dial emergency medical services (for example, 911) or for any other calls outside of the Cisco HealthPresence system."

**Note**

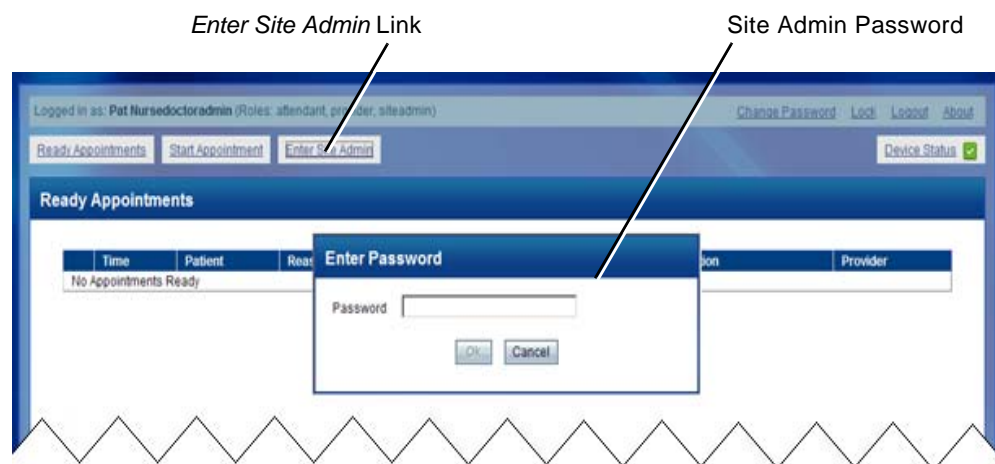
**Note for the Site Administrator:** You will be responsible for assigning the username and the first password. Each user will later supply his or her own password.

## When You Have More Than One Role

Once you have logged in, if you have more than one role, you will see the starting screen for the role with the highest priority. In the example shown in [Figure 2-5 on page 2-7](#), the user has Provider, Attendant, and Site Admin roles, and so the *Ready Appointment* screen is displayed.

1. If necessary, click the *Enter Site Admin* link.
2. Type your password (the same one that you used before) in the *Enter Password* box, and click **OK**.

The next screen that you see will depend on what type of authentication has been implemented at your site. For all three types of authentication, a user list will be the first screen, but the links and the actions will be different for the different types (for an example, see [Figure 2-5 on page 2-7](#)).

**Figure 2-5** Log in for Site Admin with Multiple Roles


The screenshot shows the Cisco HealthPresence interface after login. At the top, it says "Logged in as: PatNursedocloradmin (Roles: attendant, provider, siteadmin)". There are links for "Change Password", "Lock", "Logout", and "About". Below this are buttons for "Ready Appointments", "Start Appointment", and "Enter Site Admin". The "Enter Site Admin" button is highlighted with an arrow labeled "Enter Site Admin Link". Below these buttons is a "Ready Appointments" section with a table showing "No Appointments Ready". Overlaid on this is a dialog box titled "Enter Password" with a "Password" input field and "OK" and "Cancel" buttons. An arrow labeled "Site Admin Password" points to the password input field.

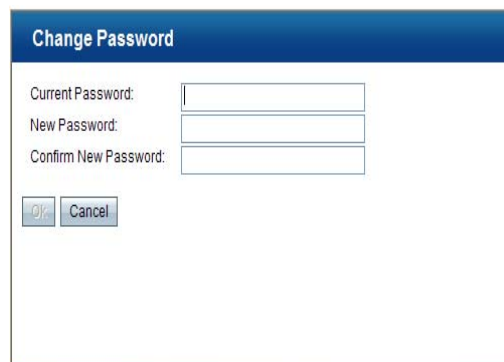
## Changing Your Password

To manage your own account, you should change the password so that it is no longer the password supplied for the Site Administrator when your system was installed.

**Figure 2-6** The Change Password Dialog Box

If you see a *Change Password* link at the top right of your screen (shown in [Figure 2-7](#)), your user account is authenticated by the Cisco HealthPresence system. You can change your password with these steps:

1. Click **Change Password** at the top right of the screen.  
You see a screen such as the one in [Figure 2-6](#).
2. Fill in the old and new passwords in the boxes provided.
3. Click **OK**.



## Locking and Unlocking the Application

If you leave your station, you should be careful to lock the application before you go. This prevents unauthorized access. You can unlock the application, returning to the same window, when you come back.



### Warning

**If you do not lock the application, and you leave it unattended for a certain length of time (determined when your system was configured), the system will log you out automatically. However, while the screen is locked, automatic logout does not apply.**

## Lock the Application When You Leave

To lock the application:

1. Click **Lock** at the top right of the screen (shown on the left in [Figure 2-7](#)).
2. In the *Lock* confirmation message dialog box (shown in the center of [Figure 2-7](#), click **Yes**.

The *Unlock* window displays. It contains your *Username* and a place for your *Password*. (A portion of this screen is shown at the right in [Figure 2-7](#).)

## Unlock the Application When You Return

To unlock the application, type in your *Password* (your *username* will already be entered), and click **Unlock**.



### Tip

Keep in mind that while you are gone another user can type over your name, and log into this station. If that happens, you will be automatically logged out.

**Figure 2-7** Locking and Unlocking the Application



## Logging Out of the System

You should log out of the system:

- At the end of the day.
- If you will not be the next person to use this station.
- If you will be gone for some time.

To log out:

1. Click **Logout** at the top right of the window (shown in [Figure 2-7](#)).  
You see the confirmation message shown in [Figure 2-8](#).
2. Click **Yes**.

**Figure 2-8** Logout Message



## Getting Into and Out of Desk-Top Mode

The Cisco HealthPresence Provider and Attendant Appliances are normally in browser mode, that is, the application launches the Internet Explorer browser automatically. However, you may need to get into desk-top mode for some reason.

### Getting Into Desk-Top Mode

To get into desk-top mode, follow these steps:

1. Press the Ctrl + Alt + Del keys on your keyboard.
2. Click on the **Task Manager** selection.
3. Click **New Task**.
4. Clear existing text, if any, and type **explorer**.
5. Click **OK**.

### Getting Back Into Browser Mode

Once you are in desk-top mode, to return to browser mode, follow these steps:

1. Log off using the *Log Off* command in the *Start* menu.
2. Log in again using the *chpuser* Windows login. (See [“Windows 7 User Login”](#) on page 2- 6.)





## CHAPTER 3

# Site Administration Tasks

---

**Revised: January 9, 2013, OL-28683-01**

This chapter describes the tasks performed by the Cisco HealthPresence system Site Administrator. (At some sites, more than one person may have this role.) The tasks listed here depend on the type of authentication used at your installation.

Topics in this chapter include:

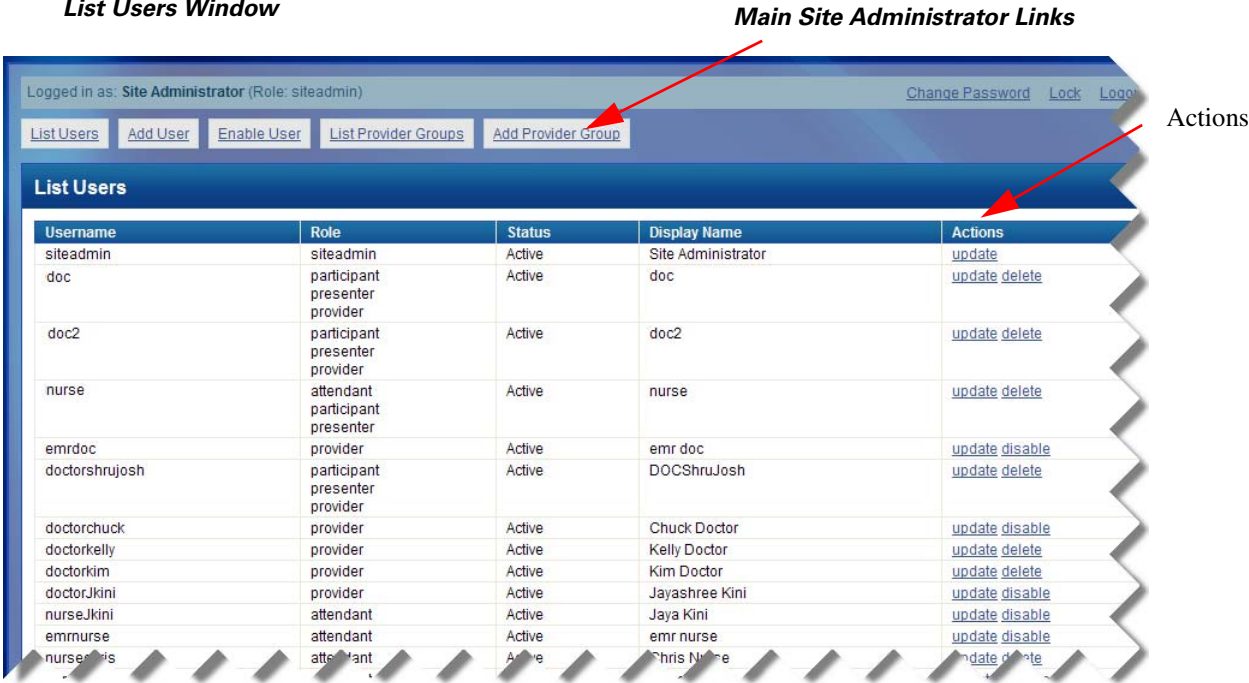
- Getting Started
- Adding a User
- Deleting a User
- Enabling a User
- Disabling a User
- Updating a User
- Unlocking a User
- Configuring Provider Groups

As described in [About Authentication, page 2-2](#), the tasks that need to be completed depend on the authentication used.

# Getting Started

After you enter your password, you will see the List Users window as shown in Figure 3-1. This is the starting point for all of your administrative tasks.

Figure 3-1 List Users Window



## Site Administrator Tasks

The main Site Administrator tasks are initiated by clicking on the links at the top of any Site Administrator Window. These links are described in Table 3-1. Additional tasks can be performed by clicking on the **Action** url specific to the **username** you want to modify. These links are described in Table 3-2. This chapter describes how to do each of these tasks.

Table 3-1 Main Site Administrator Links

Link	Use
List Users	Click this link to display a list of users.
Add User	Click this link to add a new user. This link is present only if dedicated (Cisco HealthPresence) authentication is supported.
Enable User	Click this link to enable a new user. This link is present only if external authentication is supported.
List Provider Groups	Click this link to list configured Provider Groups. This link is present only if Provider Groups are enabled for this installation.
Add Provider Group	Click this link to add a Provider Groups. This link is present only if Provider Groups are enabled for this installation.

**Table 3-2**      **Action Links**

Link	Use
Update	Click this link to access the username account and modify displayed user account information.
Delete	Click this link to delete a user account that was previously added. This link is present only if this user name is authenticated against the Cisco HealthPresence directory.
Disable	Click this link to disable a user that was previously enabled. This link is present only if this user name is authenticated against an external directory.
Unlock	Click this link to unlock this user account. This link is present only if this user name is authenticated against the Cisco HealthPresence directory.

## Adding a New User Account

**Note**

Users should be **Added** to Cisco HealthPresence only if they are to be authenticated against the dedicated Cisco HealthPresence directory. See [About Authentication, page 2-2](#) for more information.

To add a new user to the system:

1. Click the **Add User** link.  
The system displays the Add User window (see [Figure 3-2](#)).
2. Complete the type-in fields as defined in [Table 3-3](#).
3. Click the check box(es) for the Role(s).
4. Click the appropriate radio button to indicate Active or Inactive status.
5. Click the check box(es) for Provider Group(s). These options are dimmed if the Provider check box is not checked or if Provider Groups are not configured for this installation.
6. When you have finished, click **Add User**.

**Figure 3-2 Add User Window**

Logged in as: **Site Administrator** (Role: siteadmin)

[List Users](#) [Add User](#) [List Provider Groups](#) [Add Provider Group](#)

### Add User

Username:

Password:

Confirm Password:

Display Name:

Last Name:

Specialty:

Role:

- ☒ provider
- ☐ attendant
- ☐ presenter
- ☐ participant
- ☐ siteadmin

Status:

- ☒ Active
- ☐ Inactive

Provider Groups:

- ☐ Dermatology (Dermatologists)
- ☐ On Call Providers (On Call Providers)
- ☐ WeekEndOnCall (January Week End On Call Providers)

**Table 3-3 User Fields On the List Users Window**

Field	Meaning
Username	The name that you have assigned to the user.
Password	You assign the first password for each user. The user then changes the password.
Confirm Password	You are required to retype the password that you assigned.
Display Name	The name that is displayed in the participant window. When entering the Display name, remember that the name may be visible to the patient.
Last Name	This is the last name of the user. It is used for sorting lists of users.
Speciality	This is the physicians speciality. The Attendant may want to select a Provider based on Specialty, so this field, while not required, should be completed.
Role	There are five possible roles that you can assign to any given user. For definitions of these roles see <a href="#">"Understanding User Roles" on page 1- 5.</a>

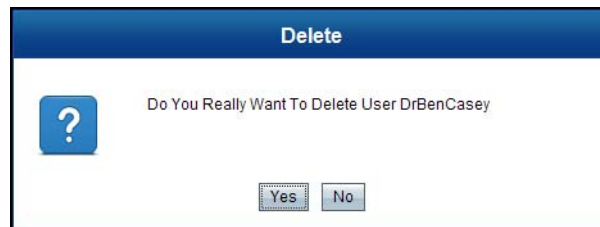
Field	Meaning
Status	You can assign a status of Active or Inactive to any account. For example, if you want to create a number of user accounts for later use, you can make them inactive until they are needed. Or, if you have training user accounts or other types of temporary user accounts, you can make them inactive when they are not needed, and active when they are needed.
Provider Group	Provider Groups, if configured for this installation, allow an Attendant to queue an appointment to a group of providers, thereby allowing the first available provider to take the appointment.

## Deleting a User Account

To delete a user account:

1. On the List Users window ([Figure 3-1](#)), find the name of the user that you want to delete.
2. Click **Delete** in the Actions column on the right.  
The system displays the Delete User confirmation dialog box (see [Figure 3-3](#)).
3. Click **Yes**.

**Figure 3-3** Delete User Confirmation Message



## Enabling a User Account



### Note

Users should be Enabled to use Cisco HealthPresence only if they are to be authenticated against an external directory. See [About Authentication, page 2-2](#) for more information.

To enable a new user on the system:

1. Click the **Enable User** link.  
The system displays the Enable User window (see [Figure 3-4](#)).
2. Type in the Username as it appears in the external directory.
3. If this user has a Provider role, type in the speciality. (This is shown on the Select Provider window when the Attendant selects a Provider.)
4. Click the check box(es) for the Role(s).
5. Click the appropriate radio button to indicate Active or Inactive status (see [Table 3-3 on page 3-4](#)).

6. Click the check box(es) for Provider Group(s). These options are dimmed if the Provider check box is not checked or if Provider Groups are not configured for this installation.
7. When you have finished, click **Enable User**.

**Figure 3-4**      **Enable User Window**

The screenshot shows the 'Enable User' window in the Cisco HealthPresence interface. At the top, it says 'Cisco HealthPresence' and 'Logged in as: Site Administrator (Role: siteadmin)'. Below this are navigation buttons: 'List Users', 'Add User', 'Enable User', 'List Provider Groups', and 'Add Provider Group'. The 'Enable User' button is highlighted. The main form has the following fields:

- Username:
- Specialty:
- Role: ☒ provider, ☐ attendant, ☒ presenter, ☒ participant, ☐ siteadmin
- Status: ☒ Active, ☐ Inactive
- Provider Groups: ☐ Cardiology (Cardiologists on CHP Rotation), ☐ Emergency Staff (Emergency Staff On Call)

At the bottom of the form is an 'Enable User' button. The footer of the window says '© 2009-2011 Cisco and/or its affiliates. All rights reserved.'

## Disabling a User Account

To disable a user account:

1. On the List Users window (Figure 3-1 on page 3-2), find the name of the user that you want to disable.
2. Click **Disable** in the Actions column on the right.  
The system displays the Disable confirmation dialog box.
3. Click **Yes**.

## Updating a User Account

All user accounts can be updated, whether they were added or enabled. If they were added, there are more fields for you to fill in.

If the user was added, that means their user name is authenticated against a dedicated Cisco HealthPresence directory and the *Update* window appears as shown in Figure 3-4 on page 3-7.

If the user was enabled, that means their user name is authenticated against an external directory, and therefore there are fewer fields that can be changed within Cisco HealthPresence. The *Update* window for a user who was enabled appears as shown in [Figure 3-6 on page 3-7](#).

To update a user account, do the following:

1. On the User List window, find the name of the user that you want to update.

2. Click **Update** in the Actions column on the right.

The system displays the Update User window (either [Figure 3-4](#) or [Figure 3-6](#)).

3. Make the required changes.
4. When you have finished, click **Update User**.

**Figure 3-5** Updating a Dedicated Directory User

Logged in as: Site Administrator (Role: siteadmin)

List Users Add User Enable User List Provider Groups Add Provider Group

### Update User

Username:

Password:

Confirm Password:

Display Name:

Last Name:

Specialty:

Role:

- ☒ provider
- ☐ attendant
- ☐ presenter
- ☐ participant
- ☐ siteadmin

Status:

- ☒ Active
- ☐ Inactive

Provider Groups:

- ☒ Cardiology (Cardiologists on CHP Rotation)
- ☐ Emergency Staff (Emergency Staff On Call)

**Figure 3-6** Updating an External Directory User

Logged in as: Site Administrator (Role: siteadmin)

List Users Enable User

### Update User

User Name:

Specialty:

Role:

- ☐ provider
- ☒ attendant
- ☐ presenter
- ☐ participant
- ☐ siteadmin

Status:

- ☒ Active
- ☐ Inactive

## Unlocking a User Account

If a user account is locked due to account inactivity or because of failed login attempts, the entry in the List Users window will be in italics, the status will show Locked, and there will be an Unlock action available in the Action column.

**Note**

This option is only available if the user account is authenticated against the Cisco HealthPresence directory (that is, this user account was *Added*.) Cisco HealthPresence cannot lock a user account that is authenticated against an external directory.

To unlock a user account:

1. On the List Users window (Figure 3-7), find the name of the user whose account is locked.
2. Click **Unlock** in the Actions column on the right (Figure 3-7).
3. Click **Yes** in the Confirmation dialog box.

**Tip**

For a list of the messages displayed to users, see “Problem with Login or Password” on page 4- 2

**Figure 3-7**      **Unlock User Account**

Logged in as: Site Administrator (Role: siteadmin)      Change Password    Lock    Logout    About

List Users    Add User

### List Users

Username	Role	Status	Display Name	Actions
siteadmin	siteadmin	Active	Site Administrator	<a href="#">update</a>
doctorkeilly	provider	Active	Kelly Doctor	<a href="#">update</a> <a href="#">delete</a>
doctorkim	provider	Active	Kim Doctor	<a href="#">update</a> <a href="#">delete</a>
doctornurse	attendant	Active	Pat Doctor-Nurse	<a href="#">update</a> <a href="#">delete</a>
	participant			
	presenter			
	provider			
testit1	attendant	Active	Test It	<a href="#">update</a> <a href="#">delete</a>
nursechris	attendant	Locked	Chris Nurse	<a href="#">update</a> <a href="#">delete</a> <a href="#">unlock</a>
nursepat	attendant	Active	Pat Nurse	<a href="#">update</a> <a href="#">delete</a>
nursedoctoradmin	attendant	Active	Pat Nursedoctoradmin	<a href="#">update</a> <a href="#">delete</a>
	provider			
	siteadmin			
participant	participant	Active	Shane Student	<a href="#">update</a> <a href="#">delete</a>
presenter	presenter	Active	Terry Trainer	<a href="#">update</a> <a href="#">delete</a>

© 2009-2011 Cisco and/or its affiliates. All rights reserved.

**Unlock Action**

# Configuring Provider Groups

## General Characteristics

If your site is using Provider Groups, you can do one of the following:

- Add Provider Groups and then add or enable the Providers. In this case, as you add or enable a Provider, you check the Provider Group(s) to which this Provider will be assigned. This may be the easier approach if you have a short list of Provider Groups but a large number of Providers.



- Add Providers and then add Provider Group. In this case, when you add the Provider Groups, you will check all the Providers that you want assigned to this Provider Group. This is useful if you are upgrading from a prior release and your Providers are already added or enabled.

## Provider Group Naming Considerations

There are several ways you can use Provider Groups, and as a result, several options for naming the Provider groups. Some options are described below:

- **Specialty:** If you are using Provider Group names to enable an Attendant to request a Consult by Specialty, then the Provider Group names should indicate the specialty.
- **Practice or Location:** You can also use Provider Group names to enable you to request Providers in a specific physical location or practice, in which case the location or practice should be included in the Provider Group name.
- **Language:** You may want a language based queue, so that patients can be seen by a Provider who speaks their native language. The Provider Group name should clearly list the language.
- **On Call:** Finally, you may also want a provider group that includes all the general practitioners who are available to take adhoc appointments, simply to minimize the time it takes for drop-ins to be seen and/or to maximize Provider productivity.

## Adding Provider Groups

To add Provider Groups, do the following:

- 
- Step 1** Click **Add Provider Group** from the options on the Site Administrator window as shown in [Figure 3-8](#).

**Figure 3-8** Site Administrator Options



- Step 2** Enter the Provider Group name and Description. If your providers are already configured in Cisco HealthPresence, check the box next to every Provider that will be part of this Provider Group as shown in [Figure 3-9](#).

- Step 3** Click **Add Provider Group**.
-

**Figure 3-9 Add Provider Group Window**

Logged in as: Site Administrator (Role: siteadmin)

[List Users](#) [Add User](#) [List Provider Groups](#) [Add Provider Group](#)

### Add Provider Group

Name:

Description:

Providers: ☐ doctorkelly (Kelly Doctor) ☐ doctorkim (Kim Doctor)

[Add Provider Group](#)

Add Provider Group

## Updating Provider Groups

To update a provider group, do the following:

- Step 1** Click **List Provider Group** from the options on the Site Administrator window. The List Provider Group Window displays as shown in [Figure 3-10](#).

**Figure 3-10 List Provider Group**

Cisco HealthPresence

Logged in as: Site Administrator (Role: siteadmin) [Change Password](#) [Lock](#) [Logout](#) [About](#)

[List Users](#) [Add User](#) [Enable User](#) [List Provider Groups](#) [Add Provider Group](#)

### List Provider Groups

Name	Description	Actions
Cardiology	Cardiologists on CHP Rotation	<a href="#">update</a> <a href="#">delete</a>
Emergency Staff	Emergency Staff On Call	<a href="#">update</a> <a href="#">delete</a>

- Step 2** Click **Update** next to the Provider Group you wish to update. The Update Provider Group Window displays as shown in [Figure 3-11](#).

**Figure 3-11**      **Update Provider Group**

The screenshot shows the Cisco HealthPresence web interface. At the top, the Cisco logo and 'Cisco HealthPresence' text are visible. Below this, a status bar indicates 'Logged in as: Site Administrator (Role: siteadmin)'. A navigation bar contains links: 'List Users', 'Add User', 'Enable User', 'List Provider Groups', and 'Add Provider Group'. The main content area is titled 'Update Provider Group'. It contains three sections: 'Name:' with a text box containing 'Cardiology'; 'Description:' with a text box containing 'Cardiologists on CHP F'; and 'Providers:' with a list of five providers, each with a checkbox. The checkboxes for 'Chuck Doctor' and 'Kelly Doctor' are checked, while the others are unchecked. At the bottom of the form is a button labeled 'Update Provider Group'. A footer at the very bottom reads '© 2009-2011 Cisco and/or its affiliates. All rights reserved.'

Providers:
<input type="checkbox"/> DOCSHruJosh
<input checked="" type="checkbox"/> Chuck Doctor
<input checked="" type="checkbox"/> Kelly Doctor
<input type="checkbox"/> Kim Doctor
<input type="checkbox"/> Jayashree Kini

- Step 3** Check Providers to add them to the Provider Group. Uncheck Providers to delete them from the Provider group.
- Step 4** Click **Update Provider Group**.
-





## CHAPTER 4

# Troubleshooting User Problems

---

**Revised: January 9, 2013, OL-28683-01**

Although troubleshooting user problems is not strictly speaking part of the Site Administrator role, you may know more about the system and how it works than other users, and people may come to you for answers. This chapter provides some suggestions for handling common user errors.

These topics are included here:

- Problem with Login or Password?
- Problem with Conferencing?
  - If You Cannot See Anything on the Screen
  - If You Cannot Hear the Presenter or Participants
- Problem Accessing Data?
  - If the Provider Cannot Access Data
  - If the Attendant Cannot Access Data
- Problem with Telemetry Devices?
  - Double-Checking the Vital Signs Monitor Status
  - Checking the Individual Device Status
- Contact Support?

## Problem with Login or Password

If users need to have their accounts re-enabled, or if they are trying to use passwords that the system will not accept, they will see an error message with an explanation and a suggestion. These messages are shown in [Table 4-1](#).

**Table 4-1 Login and Password User Messages**

Message	Action
<i>Your account has been locked due to inactivity. Please contact the site administrator to have your account re-enabled.</i>	The Site Administrator needs to unlock this user's account (see <a href="#">"Unlocking a User Account" on page 3-7</a> ).
<i>Your account has been locked due to repeated unsuccessful login attempts. Please contact the site administrator to have your account re-enabled.</i>	The Site Administrator needs to unlock this user's account (see <a href="#">"Unlocking a User Account" on page 3-7</a> ).
<i>Invalid password. Passwords must be at least &lt;n&gt; characters long and must contain at least &lt;m&gt; of the following: upper case letters, lower case letters, numbers, and special characters. Please try again by entering a new password that meets these rules.</i>	The Site Administrator should not need to become involved for this type of error.
<i>Invalid password. The password that you entered has been used recently. Please try again by entering a new password that has not been recently used.</i>	The Site Administrator should not need to become involved for this type of error.

## Problem with Conferencing?

The problems in this section can occur as users try to start or join a conference.

### If You Can't See Anything on the Screen

If you attempt to join a conference and the video screen is blank:

- Verify that the video display has power (a green light should be visible).
- Verify that at least one other participant has already joined the conference.
- Try logging out of the Cisco HealthPresence system and logging in again.

### If You Can't Hear the Presenter or Participants

If you start or join a conference and you cannot hear the attendees, adjust the volume using the control on the phone, the remote control, or the keypad, depending on what type of equipment you have. (See [Appendix B, "Types of Audio Equipment"](#).)

Assure that mute is off. (See [Appendix B, "Types of Audio Equipment"](#).)

# Problem Accessing Data?

When your system was installed, Cisco engineers verified that all of the devices were properly connected and worked as expected. Tests insured that the vitals data could be transmitted to both the Attendant and Provider stations. If one of the users has a problem later, it might be a loose connection or it might be user error.

The following guidelines will help you eliminate some of the more common user problems.

## If the Provider Cannot Access Data

This section describes instances in which the Provider cannot see the medical data, or hear the stethoscope sounds being transmitted from the Attendant station.

### No Vitals Data?

If the Provider does not see the vitals data, verify that the Attendant has clicked the **Share** button.

### No Video Image?

If the Provider does not see the output of the Exam Camera or the Scope Camera:

- Verify that the Attendant can see the video at the Attendant station. If the Attendant cannot see the video, have the Attendant click **Start**.

### No Stethoscope Sounds?

If the Provider does not hear the stethoscope sounds from the headphones:

- Verify that the Attendant has started the stethoscope and has it in position.

### No ECG Data?

If your site uses an Interoperable Medical Device that supports ECGs, and the Provider does not see the ECG images:

- Verify that the Attendant has clicked the Start button.
- Verify that the leads are properly placed.

## If the Attendant Cannot Access Data

This section describes instances in which the Attendant cannot see the data or hear the stethoscope sounds. It only addresses potential issues with how Cisco HealthPresence is interoperating with Interoperable Medical Devices<sup>1</sup>. For issues with the medical devices themselves, see the instructions for use supplied with the medical devices.

### No Vitals Data?

If the Attendant clicks the **Get** button and the patient's vitals do not appear on the window at the Attendant station:

If the interoperable vital signs monitor has a display:

- Verify that the vitals data is visible on the vitals signs monitor display.
- Remove the oximeter and thermometer and click **Get** again.
- If this does not resolve the problem, check the Device Status (see [“Problem with Medical Devices?” on page 4- 6](#)).

### No Video Image?

If the Attendant cannot see an image from an attached interoperable video device, verify that the Attendant has clicked the **Start** button. If that does not resolve the problem, verify that the camera is operational referring to the instructions for use that came with the video device.

### Blurry Video Image?

If the camera image is blurry or unclear:

- Verify that the lenses are clean and intact.
- Refer to the instructions for use supplied with the video device.

### Video Image Stopped?

If the video at the Attendant station stops, and an error message indicates that streaming has stopped:

- Verify that the camera is properly connected to the system.
- Try to restart the streaming using the **Start** button.

### No Stethoscope Sounds?

With some interoperable stethoscopes, only the Provider can hear stethoscope sounds.

If the Attendant has headphones for use with the stethoscope and has clicked the **Start** button, but no sound comes from the headphones:

1. NOTE: Interoperable Medical Devices are available only from the manufacturer of such devices or its authorized resellers and distributors. Cisco is not a reseller or distributor of such devices. Interoperable Medical Devices are not available in all countries. To find out if the Interoperable Medical Devices are available in your country, contact the manufacturer or the seller of the Interoperable Medical Device. For information on how to use any Interoperable Medical Device see the instructions for use provided with that device. Cisco makes no representations or warranties regarding the features, functionality or intended use of the Interoperable Medical Devices.



- If it is a wired stethoscope, verify that the physical connections to the stethoscope
- If it is a wireless stethoscope, verify that there is line of sight between the USB blue tooth and the stethoscope.

## No ECG Data?

If your site uses an Interoperable Medical Device that supports ECGs and if the Attendant has clicked the Start button, and the ECG images are not displayed:

- Have the Provider verify that the leads are properly placed.

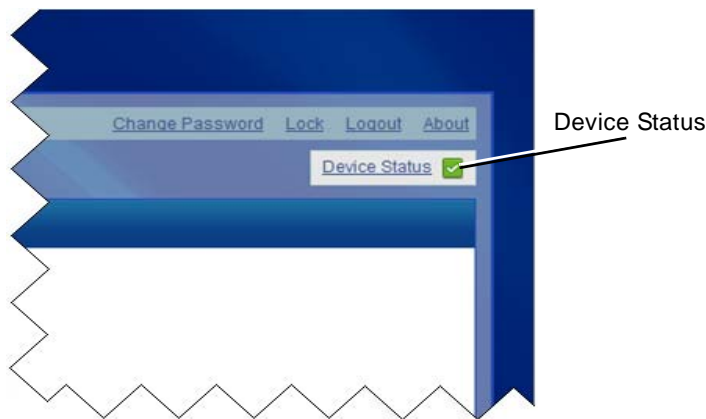
## Problem with Medical Devices?

As part of the maintenance plan, someone at your site tests the medical devices every morning to make sure that all of the devices are in working order, and can communicate with the Cisco HealthPresence system. In addition, before each appointment the Attendant checks the status of the devices using the status codes on the window. These codes are shown here so that you can double-check the device status if necessary.




### Double-Checking the Vital Signs Monitor Status

The Device Status link in the upper right-hand corner of the window (see [Figure 4-1](#)) provides an overall status of the Vital Signs Monitor. The codes are explained in [Table 4-2](#).

**Figure 4-1** Checking Overall Device Status



**Table 4-2** Overall Device Status Codes

Code	Color	Meaning
	Green	All devices are available.
	Yellow	Some devices are available. Click the <i>Device Status</i> link for more information.
	Red	No devices are available. Check the equipment.



**Note**

Depending on the Interoperable Medical Devices installed, some installations will see only green or red status codes.




## Checking the Individual Device Status

To see a detailed status report, click the *Device Status* link (see [Figure 4-1 on page 4-6](#)). The window shows individual status for the Oximeter, the Blood Pressure Monitor, and the Thermometer (see [Figure 4-2](#)). The codes are explained in [Table 4-3](#).


**Note**

Some Interoperable Medical Devices do not support this second-level status capability.

**Figure 4-2**      **Checking Individual Device Status**

Device Status		
Device Name	Device	Status
Oximeter	Welch Allyn	 Powered Off
Blood Pressure Monitor	Welch Allyn	 Powered Off
Thermometer	Welch Allyn	 Powered Off
<a href="#">Close</a>		

**Table 4-3**      **Individual Device Status Codes**

Code	Meaning	Action
Red circle with X	The system is reporting an error or an unknown status for the device.	Try turning off the device and turning it back on. Close this window and re-open it to see the updated device status.
Red box with dash	The device is powered off.	Check the device and either turn on the power or make sure the power cord is correctly attached to both the device and the wall outlet.
Green box with checkmark	The device is powered on and available.	No action necessary.

## Contact Support?

If you are unable to resolve problems on your own, contact support. When your Cisco HealthPresence system was installed, your site was provided with the appropriate numbers to call.





# APPENDIX A

## Worksheets

---

Revised: January 9, 2013, OL-28683-01

Before you configure the users of the system, it is a good idea to create a worksheet so you can track the user names and passwords you specified and can determine in advance the appropriate specialty and Provider Groups.

## Adding Providers

[Table A-1](#) is one possible approach to creating the worksheet for Providers you will **Add**. The last two columns should be replaced with a column for every Provider Group you have configured in this system with the column header naming the specific group. You can optionally add columns for Display Name and Role(s). Remember, Providers you **Add** should be Providers who have a User Name and password that is authenticated against a dedicated Cisco HealthPresence directory. For more information about authentication, see [About Authentication, page 2-2](#). For information about user naming conventions, see “Cisco HealthPresence User Names” on [page 2-4](#).

**Table A-1**      **Providers to Add**

Name	User Name	Password	Specialty	Provider Group 1	Provider Group 2

## Enabling Providers

[Table A-2](#) represents a possible worksheet for a Provider you will **Enable**. Since these users are authenticated against an external directory, the user name specified in Cisco HealthPresence **MUST** match the user name specified in the external directory. The password column does not apply, as this is controlled by the external directory. You can optionally add columns for Role(s).

**Table A-2**      **Providers to Enable**

Name	User Name	Specialty	Provider Group 1	Provider Group 2

## Adding Attendants

[Table A-3](#) is one possible approach to creating the worksheet for Attendants you will **Add**. Remember, Attendants you **Add** should be Attendants who have a User Name and password that is authenticated against a dedicated Cisco HealthPresence directory. You can optionally add columns for Display Name and Role(s). For more information about authentication, see [About Authentication, page 2-2](#). For information about naming conventions, see “Cisco HealthPresence User Names” on [page 2-4](#).

**Table A-3**      **Attendant's to Add**

Name	User Name	Password

## Enabling Attendants

[Table A-4](#) represents a possible worksheet for Attendants you will **Enable**. Since these users are authenticated against an external directory, the user name specified in Cisco HealthPresence **MUST** match the user name specified in the external directory. The password column does not apply, as this is controlled by the external directory. You can optionally add columns Role(s).

**Table A-4**      **Attendants to Enable**

Name	User Name

# Adding Provider Groups

It is a good idea to consider how you want to name Provider groups and how you want to assign Providers to Provider Groups. A Provider can belong to Multiple Provider Groups and you may want one group that includes all the Providers. [Table A-5](#) represents a possible worksheet for Provider Groups you will *Add*.

**Table A-5**      **Provider Groups**

Name	Description	Providers







# APPENDIX B

## Types of Audio Equipment




Revised: January 9, 2013, OL-28683-01





**Some video systems use an integrated IP phone to connect video conference calls and to control the volume of conference calls. Depending on how your system was configured, if you have one of these IP phones, outside calls may or may not be supported.**

The phone that you use with your Cisco HealthPresence system will be one of the ones listed in the table below. This table tells you whether or not the phone you are using is one of the IP phones, and how to control the volume.

**Table B-1** *Phones Compatible with the Cisco HealthPresence System*

Telephone	IP Phone?	Description	Volume Control	Illustration
Cisco TelePresence System 500 (CTS 500)	Yes	Consists of an integrated 37" display, camera, microphone, speakers, a Cisco Unified 7975G IP phone, and the Cisco TelePresence codec.	Use the volume control on the phone. Use the mute button to toggle mute on and off.	
Cisco Unified Video Advantage	Yes	Adds video to your communications by adding video telephony functionality to the Cisco IP Communicator.	Use the volume button on the IP Communicator screen, or use the up and down arrows on your keyboard. Use the mute button on the IP Communicator screen to toggle mute on and off.	
Cisco Unified IP phone 7985G	Yes	A desktop video phone, which includes a camera, LCD screen, speaker, keypad, an integrated codec, and a handset.	Use the volume control on the phone to adjust volume. Use the microphone mute button to mute volume on the microphone.	

Telephone	IP Phone?	Description	Volume Control	Illustration
Cisco TelePresence System EX90	No	Video conferencing systems with fully integrated units including a codec, display, camera, microphone, and loudspeakers.	Use the volume control on the right side of the touch pad to adjust volume. Use the microphone mute button on the top right of the touch pad to mute the volume on the microphone.	
Cisco TelePresence System EX60	No			
Cisco TelePresence C20	No	Fully interoperable with standards-based video conferencing or telepresence systems' (might require MCU in some combinations).	Use the remote control (shown) or the touch pad to raise or lower volume. Use the microphone mute button to mute the volume on the microphone.	
Cisco TelePresence System C40	No			



## GLOSSARY

Revised: January 9, 2013, OL-28683-01

---

### A

- 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 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).
- Browser** A computer application that connects your computer with the Internet. The Cisco HealthPresence solution uses *Internet Explorer* as its browser.
- Business Entity** The Attendant and Provider stations managed by a single Cisco HealthPresence Application Server.

---

### C

- Cisco HealthPresence Solution** The system that combines audio, video, telemetry, computer networking, and a graphical user interface to enable physicians to offer services to patients in locations throughout the world.
- 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).

---

### E

- E- Pen** Electronic Pen. Allows physicians to write online prescriptions.
- 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.

---

## 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).

---

## 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 Group** A collection of Providers who can be requested to accept a Cisco HealthPresence appointment with a single click. A facility can configure any number of Provider Groups. The Provider Groups appear in a drop down menu on the Attendant Start Appointment window.

**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.

---

## 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.

---

## U

<b>URL</b>	Uniform Resource Locator. An address on the World Wide Web. When you click a URL, your web page is redirected to that location
<b>User Role</b>	Your User Role determines which windows you see, and which functions you can perform. User Accounts are configured so that users with a particular role (or roles) see only the windows 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. See <a href="#">“Understanding User Roles” on page 1-5</a> .

---

## V

<b>Vitals</b>	Patient data that includes temperature, blood pressure, and pulse. Collected using the Welch Allyn VSM, and transmitted to the Cisco HealthPresence system.
---------------	---

---

## W

<b>Windows</b>	The operating system used by your Cisco HealthPresence system. If your system has been powered off, either deliberately or accidentally, you will need to enter the Windows password for your installation. See <a href="#">“Gaining Access to the System (If Necessary)” on page 2-5</a> .
----------------	---

