



▶ Polycom® SpectraLink® 8400
Series Wireless Telephone
Deployment Guide

Trademark Information

POLYCOM®, the Polycom “Triangles” logo and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient’s personal use, without the express written permission of Polycom.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Disclaimer

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

© 2011 Polycom, Inc. All rights reserved.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording). Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

About This Guide

Who Should Read This Guide?

System administrators or network engineers should read this guide to learn how to properly set up the Polycom® SpectraLink® 8400 Series Wireless Telephone.

This guide includes administration-level tasks and is not intended for end users of the handsets. Many of the tasks involve configuring Wireless Local Area Network (WLAN) settings and affect the phone's ability to function in the network.

This guide assumes you are familiar with:

- Computer networking and driver administration for your operating system
- An XML editor
- Wireless client administration
- WLAN infrastructure parameters
- The XML-based configuration file format used by the Polycom® UC Software and its supported phones

What Will This Guide Show You?

This guide shows you how to deploy the SpectraLink 8400 Series Wireless Telephones in an 802.11 wireless environment.

Though you may be familiar with several deployment methods, Polycom recommends the method described in this guide as the most flexible and manageable.

How This Guide is Organized

This guide includes four chapters and four appendices. The chapters are structured in a sequence for reference and in a logical progression that you would follow to deploy SpectraLink 8400 Series Handsets.

Chapter 1, [Overview](#), introduces the SpectraLink 8400 Series Handsets.

Chapter 2, [Deploying SpectraLink 8400 Series Handsets](#), provides basic and advanced instructions on how to set up a wireless configuration server (WCS), and a provisioning server, create the configuration files to work in a wireless environment, deploy the SpectraLink 8400 Series Handsets from the provisioning server, and upgrade the software.

Chapter 3, [Configuring SpectraLink 8400 Series Handsets](#), provides information for configuring and using the basic and advanced features on the SpectraLink 8400 Series Handsets.

Chapter 4, [Troubleshooting SpectraLink 8400 Series Handsets](#), explains the error messages that may appear on the handsets and how to read the log files produced by the handset.

Appendix A, [Configuration Files](#), provides detailed descriptions of specific configuration parameters used by the Polycom UC Software.

Appendix B, [Miscellaneous Administrative Tasks](#), provides information about tasks like setting up an FTP server and using the Web Configuration Utility.

Appendix C, [Deployment Checklist](#), provides a checklist of all the parameters you need to change to set up your SpectraLink 8400 Series Handsets.




Appendix D, [Polycom UC Software Menu System](#), shows the menu structure of the Polycom UC Software as it displays on SpectraLink 8400 Series Handsets.

What's New in This Guide

To support worldwide deployment of the SpectraLink 8400 Series Handsets, you must select the regulatory domain appropriate to your location. See [Regulatory Domain and Radio Settings](#) on page 16.

Conventions Used in This Guide

These icons are used in the guide:

	Note	This alert points to tips that may provide additional information about a concept or procedure.
	Warning	This alert highlights information that you need to know to keep the phone running correctly.
	Caution	This alert warns you of instances where an instruction or procedure not followed exactly could result in significant issues with your phone.

These typographic conventions are used in this guide:

Bold	Interface items like menus, soft keys, filenames, and directories.
<i>Italics</i>	Guide names that are available from the Polycom Support Web site.
Blue	URLs.
Fixed-width font	Code fragments and parameter names.

These writing conventions are used in this guide:

<code><installed-dir></code>	A directory path where you must enter a value from your organization.
<code>></code>	Indicating selecting an item from a menu. For example, Settings > Basic > Preferences .

Recommended Software Tools

Polycom recommends that you use an XML editor to create/edit the configuration files. In this way, all configuration files that you create will be valid XML files.

If the configuration files are not valid XML, they will not load on the handset. In this case, an error message will be logged to the provisioning server.

Getting Help and Support

The following documents are available as supplementary information to assist you with your wireless handset deployment:

- **Quick Start Guide** Describes the physical parts of the handset, available accessories, and basic call functions
- **User Guide** Describes the basic and advanced features available on the handset
- **Administrator's Guide** Shows you how to configure, customize, manage, and troubleshoot Polycom SoundPoint® IP, SoundStation® IP, VVX® phone systems, and SpectraLink 8400 Series Wireless Handsets
- **Developer's Guide** Assists with the development of applications that run on the Microbrowser or Browser on the SoundPoint IP, SoundStation IP, VVX phones, and SpectraLink 8400 Series Wireless Handsets
- **Quick Barcode Connector Installation Guide** Shows you how to install and configure the Quick Barcode Connector application
- **AP Configuration Guides** Shows you how to correctly configure access points and WLAN controllers (if applicable) and identify the optimal settings that support SpectraLink 8400 Series Handsets. The guides can be found at http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/view_certified.html.
- **Technical Bulletins and Feature Descriptions** Show you workarounds to existing issues and provides expanded descriptions and examples
- **Release Notes** Describe the new and changed features, and resolved issues in the latest version of the software

For support or service, please contact your Polycom® reseller or go to Polycom Technical Support at

<http://support.polycom.com/PolycomService/home/home.htm>.

Polycom recommends that you record the handset model numbers, MAC address, software version, and partner platform for future reference.

SpectraLink 8400 Series Handset's MAC Address: _____

UC Software version: _____

Partner Platform: _____

We are constantly working to improve the quality of our documentation, and we would appreciate your feedback. Please send email to VoiceDocumentationFeedback@polycom.com.

Contents

About This Guide	iii
Who Should Read This Guide?	iii
What Will This Guide Show You?	iii
How This Guide is Organized	iv
What's New in This Guide	iv
Conventions Used in This Guide	v
Recommended Software Tools	v
Getting Help and Support	vi
1 Overview	1
WLAN Layout Considerations, Quality of Service, and Security	1
Where SpectraLink 8400 Series Wireless Telephones Fit	2
System Components	2
Polycom UC Software Architecture	3
Updater	4
Polycom UC Software	4
Configuration Files	4
Resource Files	6
2 Deploying SpectraLink 8400 Series Handsets	7
Overview	8
Understanding the Complete Process	10
Before You Begin	10
Part I: Working From Your Wireless Configuration Station	11
Set Up the FTP Server	11
Enable the Handset's Network Capabilities	12
Set Up the Handset's Network Parameters	14
Wireless Parameters	14
WLAN Security Configuration Parameters	14
SSID and WMM-AC	16
Regulatory Domain and Radio Settings	16
Provisioning Server Parameters	19

Network Parameter Procedure	20
Part II: Initial Provisioning of the Handsets	30
Part III: Setting Up the Provisioning Server	30
Part IV: Deploying the Handsets From the Provisioning Server	32
Creating a Phone Configuration File	32
Creating a Master Configuration File	34
Downloading the New Configuration	36
Upgrading Software on Your Handsets	37
Locating the Latest Software	37
Downloading New Software	37

3 Configuring SpectraLink 8400 Series Handsets39

Setting Up Basic Features	40
Time and Date Display	40
Notification Profiles	41
Bluetooth Headset Support	41
Keypad Lock	41
Push-to-Talk	41
Multi-Key Answer	42
User Profile Portability	42
Creating a Phone Configuration File	44
Creating a User Configuration File	44
Setting Up Advanced Features	45
Barcode Scanner Support	45
Browser and Applications	46
Open Application Interface	46
Instant Messaging and Presence	46
Location Service	47
Calendaring	47

4 Troubleshooting SpectraLink 8400 Series Handsets49

Calling	50
Display	50
Upgrading	50
Wi-Fi Diagnostics	51
Mnemonic Reason Codes	54
Run Site Survey	55
Setting Up Syslog	58
User Accessible Network Diagnostics	58
Access Point Issues	58

In Range/Out-of-Range 59
 Capacity 59
 Transmission Obstructions 59

A Configuration Files61

Master Configuration File 61
 Configuration Parameters 62
 <apps/> 64
 <bluetooth/> 64
 <device/> 64
 <exchange/> 71
 <feature/> 71
 <keypadLock/> 72
 <log/> 72
 <mb/> 73
 <messaging/> 73
 <np/> 73
 <oai/> 96
 <prov/> 97
 <ptt/> 98
 <qbc/> 99
 <reg/> 100
 <roaming_buddies/> 102
 <roaming_privacy/> 102
 <up/> 103
 <voIpProt/> 103
 <wifi/> 104

B Miscellaneous Administrative Tasks105

Setting Up an FTP Server 105
 Using the Web Configuration Utility 106
 Modifying the SpectraLink 8400 Series Handsets
 Configuration 107
 Exporting Configuration Files 110

C Deployment Checklist113

D Polycom UC Software Menu System119

Overview

This guide shows system administrators how to deploy the Polycom® SpectraLink® 8400 Series Wireless Telephone in an 802.11 wireless environment. It also shows you how to upgrade the handset's software when it is connected in a wireless environment and how to manage and modify the configuration of the deployed handsets. The handset must be running UC Software 4.0.0 or later to place and receive calls.

For the package parts list and basic instructions on how to use the handset, see the *SpectraLink 8400 Series Wireless Telephone Quick Start Guide* in the handset package.

The topics in this chapter include:

- [WLAN Layout Considerations, Quality of Service, and Security](#)
- [Where SpectraLink 8400 Series Wireless Telephones Fit](#)
- [Polycom UC Software Architecture](#)



Polycom strongly recommends that you make use of a provisioning server as well as a time server.

A provisioning server facilitates central management of software upgrades, language support, configuration management, and diagnostic logging. The SpectraLink 8400 Series Handsets support using TFTP, FTP, HTTP or HTTPS servers for provisioning.

Access to a time server enables display of the current date and time on the handset's display and verification of the time components in the handset's certificates.

WLAN Layout Considerations, Quality of Service, and Security

Careful planning of the Wireless Local Area Network (WLAN) layout, attention to Quality of Service (QoS), and proper security provisions are necessary to ensure good voice quality. For detailed guidance, see the *Best*

Practices Guide to Network Design Considerations for SpectraLink 8400 and 8000 Series Wireless Telephones, which is available at <http://support.polycom.com/support/spectralink8400>.

Where SpectraLink 8400 Series Wireless Telephones Fit

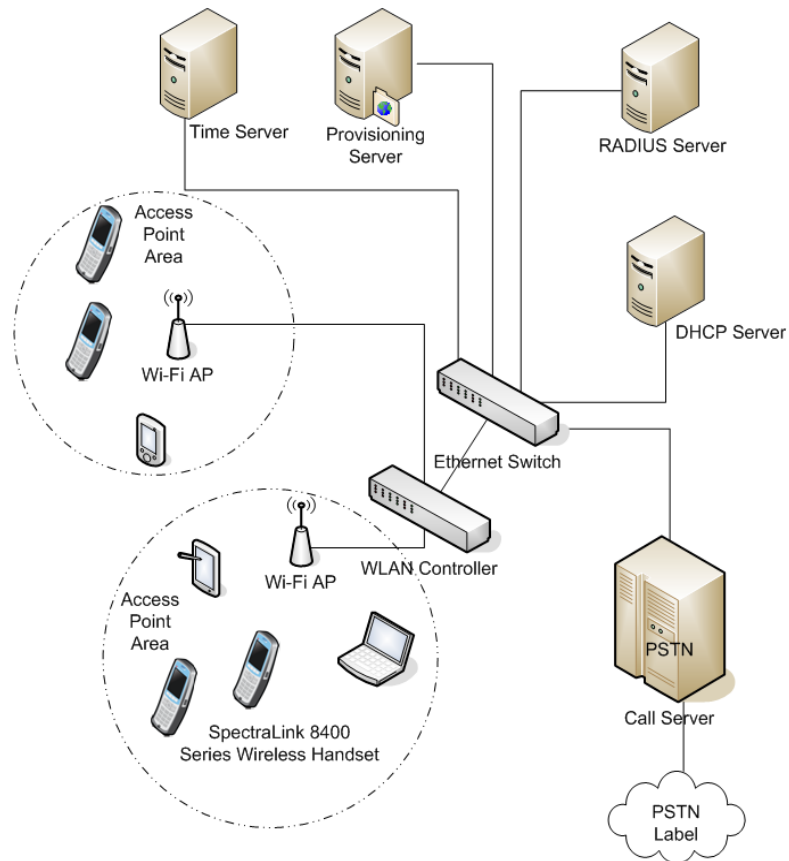
An overview of the system components can help you see how the wireless handsets fit in the wireless network environment.

System Components

The typical system components required to manage SpectraLink 8400 Series Handsets are:

- Access Points (APs) and Controller
- Ethernet Switch
- Call Server
- Provisioning Server
- Simple Network Time Protocol Server
- Authentication Server
- DHCP Server

The following figure shows how the SpectraLink 8400 Series Handsets fit in the network with APs and the wireless LAN Ethernet Switch.



For a list of supported APs, see the VIEW Certified Product Guides, which are available at http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/view_certified.html.

Polycom UC Software Architecture

To ensure a successful deployment, it is important that you understand the Polycom UC Software architecture and how the software behaves on the SpectraLink 8400 Series Handsets. Understanding this architecture will help insure that your deployment goes smoothly.

The Polycom phone software is comprised of four basic components:

- **Updater**—The application that loads first when the phone is powered on and launches the Polycom UC Software

- **Polycom UC Software** – The software that provides the telephony features and applications to the handset
- **Configuration Files** – A file or files that contain the configuration parameters used by the UC Software
- **Resource Files** – Optional files needed for some of the advanced features

The four basic components are described in more detail below.

Updater

The Updater is a small application that resides in the flash memory on the handset. All phones have the Updater installed at the factory. The Updater downloads the master configuration file, then extracts the Polycom UC Software from the flash memory.

For more information, see the Updater section of the latest *Polycom UC Software Administrator's Guide* available at

<http://support.polycom.com/support/spectralink8400> .

Polycom UC Software

After the Updater has performed its tasks, the Polycom UC Software loads on the handset. The UC Software manages the protocol stack, the digital signal processor (DSP), the user interface, and the network interaction. The UC Software manages everything to do with the handset's operation. The UC Software downloads the system, per-phone configuration, and resource files.

For more information, see the Polycom UC Software section of the latest *Polycom UC Software Administrator's Guide* available at

<http://support.polycom.com/support/spectralink8400> .

Configuration Files

The SpectraLink 8400 Series Handsets can be configured automatically through files stored on a central provisioning server, manually through the phone's local user interface or Web Configuration Utility, or by using a combination of the automatic and manual methods. This guide focuses only on Polycom's recommended provisioning method: configuring the phones through the central provisioning server.

The configuration files use an XML format. Use an XML editor to modify and validate the configuration files.



Once you have downloaded the UC Software ZIP files, Polycom recommends that you make copies of the configuration templates (from the Config folder) that you want to use, and rename and make changes to the copies. The example shown next has been modified.

<pre> xml #comment #comment #comment #comment #comment APPLICATION APP_FILE_PATH CONFIG_FILES MISC_FILES LOG_FILE_DIRECTORY OVERRIDES_DIRECTORY CONTACTS_DIRECTORY LICENSE_DIRECTORY USER_PROFILES_DIRECTORY CALL_LISTS_DIRECTORY APPLICATION_SPIP300 APPLICATION_SPIP500 APPLICATION_SPIP301 APPLICATION_SPIP300 </pre>	<pre> version="1.0" standalone="yes" Default Master SIP Configuration File For information on configuring Polycom VoIP phones please refer to the Configuration File Management white paper available from: http://www.polycom.com/common/documents/whitepapers/configuration_fi \$RCSfile: 000000000000.cfg,v \$ \$Revision: 1.30 \$ sip.ld phone[PHONE_MAC_ADDRESS].cfg </pre>
--	---

A number of sample template files are included with the Polycom UC Software 4.0.0 release.

You will create or change at least three configuration files:

- A network configuration that tells the handset how to connect to the wireless network
- A phone configuration that tells the handset what features will be available. Use the sample templates to create handset-specific files, for example, **phone00907abe80a6.cfg** and **phone00907abe80b3.cfg**.
- A master configuration file (shown above) that tells the phone the software and configuration files to load onto the handset. Use the default **000000000000.cfg** or create a handset-specific file based on the MAC address of the handset for each handset you want to deploy, for example, **00907abe80a6.cfg**.

For more information on creating configuration files, see the *UC Software Provisioning Best Practices* at

<http://www.polycom.com/global/documents/whitepapers/uc-software-provisioning-best-practices-whitepaper.pdf>.

For more information on sample template files, configuration files format, and other configuration file examples, see the latest *Polycom UC Software Administrator's Guide* at

<http://support.polycom.com/support/spectralink8400>.

Resource Files

In addition to the software and the configuration files, the handsets may require resource files that are used by some of the advanced features. These files are optional, but if the particular feature is being employed, these files are required.

For more information, see the Resource Files section of the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Deploying SpectraLink 8400 Series Handsets

This chapter is perhaps the most important section of this guide. In this chapter, you will learn Polycom's recommended method for configuring and deploying SpectraLink® 8400 Series Handsets. Since this deployment method involves multiple stages, each of which is comprised of multiple steps, ensure that you follow this guide carefully in order to deploy the phones successfully. Before you begin, review each section to familiarize yourself with each of the stages and steps.

This chapter is organized into four learning components designed to provide a complete understanding of the deployment method:

- A high-level overview of the two-stage process
- A list of all stages and steps of the process
- The information you need to gather before you begin
- The steps you need to perform to configure and deploy the SpectraLink 8400 Series Handsets

If you are new to wireless configuration and deployment, Polycom recommends that you review all four learning components of this chapter before you begin. If you are already familiar with setting up wireless environments, you may wish to skip the introductory information and go directly to what you specifically need to complete the deployment (see [Before You Begin](#) on page 10).

This chapter covers the following topics in detail:

- [Overview](#)
- [Understanding the Complete Process](#)
- [Before You Begin](#)
- [Part I: Working From Your Wireless Configuration Station](#)
- [Part II: Initial Provisioning of the Handsets](#)
- [Part III: Setting Up the Provisioning Server](#)

- [Part IV: Deploying the Handsets From the Provisioning Server](#)





Before you start provisioning the handsets, Polycom recommends that you fully charge the Battery Packs to ensure prolonged battery life.

There are three charging options available for the SpectraLink 8400 Series Handsets: dual charger, quad charger, and USB charger. The charge time will vary for each charging methods, but the charging process typically takes two to four hours.

After the Battery Packs are fully charged, install them into the back of the handsets.

The handset will automatically boot up once power is supplied. Under normal conditions, this process will take approximately 30 seconds.

Note:

- To turn on the SpectraLink 8400 Series handset, press and hold the  (End) key for roughly 3 seconds.
- To turn off the handset, press and hold the  (End) key for roughly 3 seconds.

Overview

Although there are a number of possible installation and configuration methods you can use, Polycom recommends a specific two-stage method that requires you to use a wireless configuration station and a provisioning server. This two-stage method involves a setup phase and a configuration phase as follows:

On the wireless configuration station:

- Set up the wireless configuration station
- Configure the wireless parameters

On the provisioning server:

- Set up the provisioning server
- Configure and deploy the handsets

Wireless Configuration Station

The wireless configuration station (WCS) is a computer that you will configure to provide the Wireless network configuration settings to the handset via the USB cable. You will be setting up this computer as an FTP server and loading the following credentials onto the handsets through their USB connection: the DHCP, SSID, security configuration parameters (mode, certificates, user names, and passwords), and the radio settings (2.4 GHz and 5.0 GHz). Once the initial credentials are finished loading, your handsets will be able to connect wirelessly to your network and provision itself from the provisioning server (described in the next section).

Provisioning Server

In addition to the computer you set up as a WCS, you will need to set up a second computer as a provisioning server. The handsets connect to the provisioning server over the wireless connection. The provisioning server provides the handsets with the remaining configuration parameters required to operate, such as the call server address, the line registrations, and the features that you want to enable on the handsets. The provisioning server also enables you to upgrade the handsets over their lifetime.

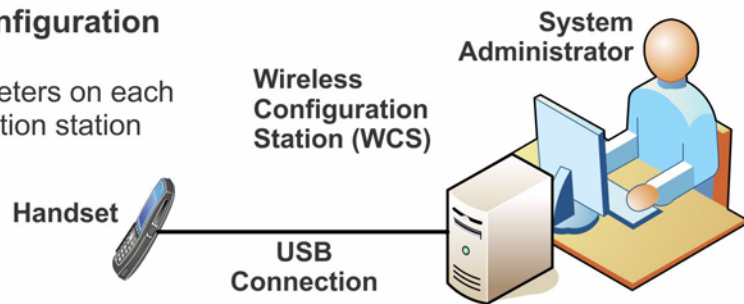
The following figure gives an overview of the deployment process.

SpectraLink 8400 Series Handset Deployment: The Two-Part Process

Part 1: Using Your Wireless Configuration Server...

Update the following wireless parameters on each handset using the wireless configuration station through the USB connection:

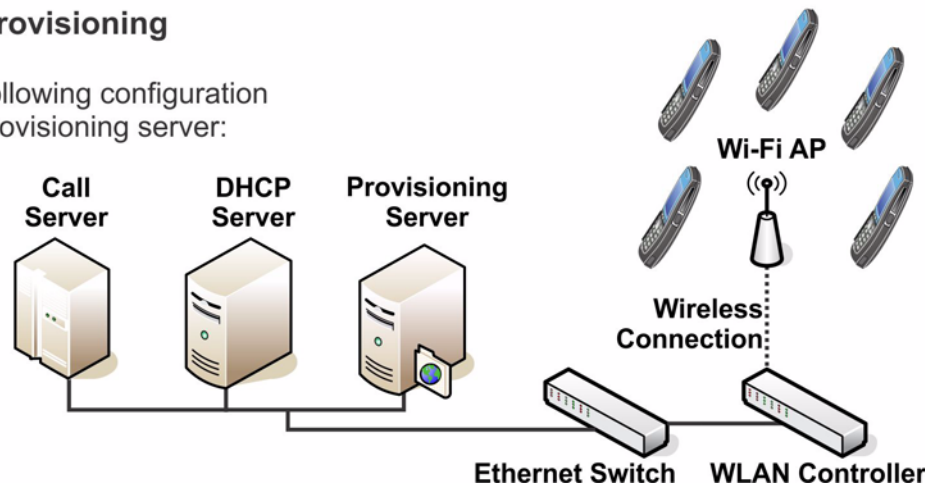
- DHCP
- SSID
- Security credentials
- 5 GHz and 2.4 GHz band



Part 2: Using Your Provisioning Server...

Wirelessly update the following configuration parameters using the provisioning server:

- Notification profiles
- Bluetooth headset
- Keypad lock
- Push-to-talk
- User profiles



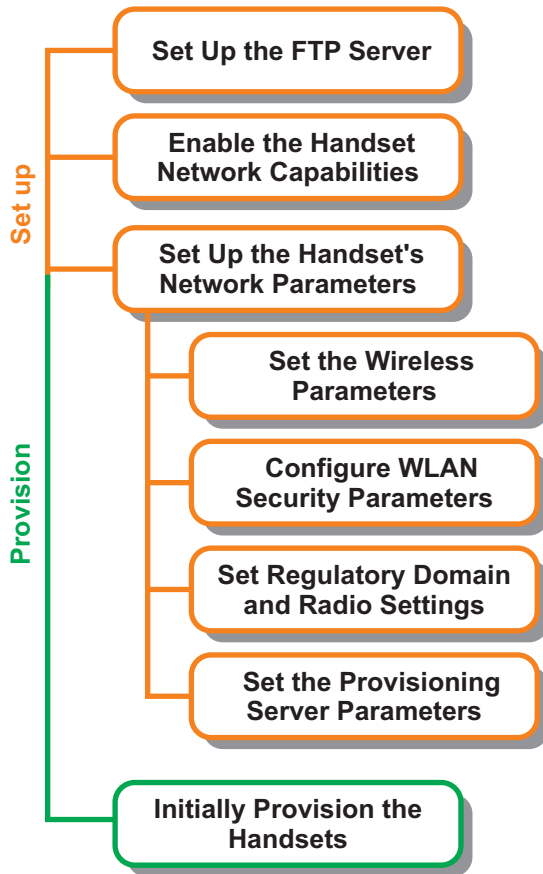
Most subsequent wireless network configuration changes can be made via the provisioning server.

Understanding the Complete Process

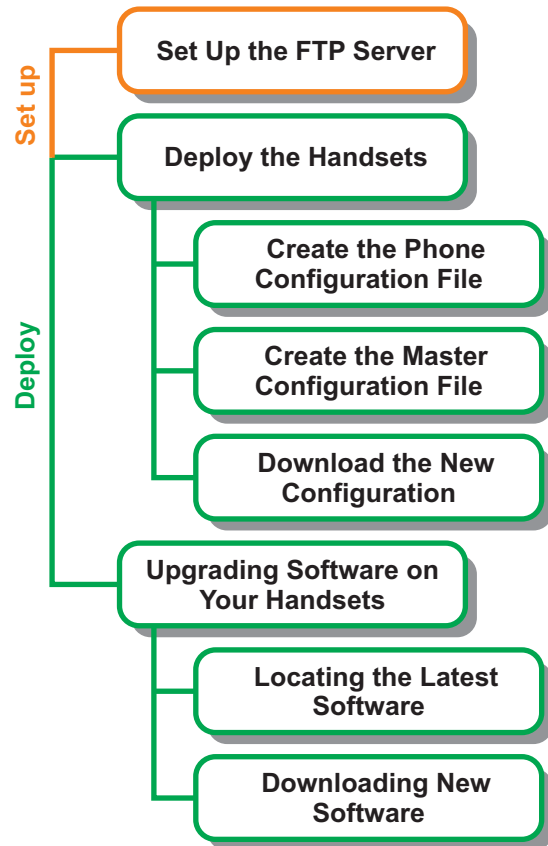
Polycom recommends a specific two-stage method for deploying and provisioning the wireless handsets.

The figure shown next summarizes the steps that complete the two stages:

From Your Wireless Configuration Station...



From Your Provisioning Server...



Before You Begin

Before you set up your WCS and Provisioning servers, Polycom recommends that you gather the information required to create the configuration files and to configure the WCS and Provisioning servers. A sample deployment checklist for SpectraLink 8400 Series Handsets can be found in [Deployment Checklist](#) on page 113.

Part I: Working From Your Wireless Configuration Station

To set up a WCS, you must complete the steps described in each of the following procedures:

- 1 Set up an FTP server on the WCS and download the Polycom UC Software from the Polycom Support Web site. See [Set Up the FTP Server](#) on page 11.
- 2 Install the **84xx.inf** file or the **84xx-64.inf** file on the WCS to allow it to recognize the handset's USB networking capabilities. This step is not needed if the WCS computer is running Microsoft® Windows® 7. See [Enable the Handset's Network Capabilities](#) on page 12.
- 3 Set up the handset's network connection parameters in the configuration file. See [Set Up the Handset's Network Parameters](#) on page 14.

To view a detailed reference for all configuration parameters, see the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Set Up the FTP Server

The first step in setting up the WCS is to set up your FTP server to provision the handsets so they can connect to the wireless network.

For directions on setting up an FTP server, see [Setting Up an FTP Server](#) on page 105.



By default, Polycom sets FTP as the provisioning protocol on all SpectraLink 8400 Series handsets. The WCS can configure the handset to use any of the other supported provisioning protocols when connecting to the Provisioning server.

To set up the wireless configuration station:

- 1 On your computer, create a folder to store the UC Software executable and the configuration files that come with the UC Software.

For example, create a folder with the path and name:

C:\FTP_root\SpectraLink8400

- 2 Download the latest UC Software from <http://support.polycom.com/support/spectralink8400> to the WCS.

The UC Software is a ZIP file.

- 3 Extract the following file from the UC Software ZIP file to the newly created folder:

000000000000.cfg

For a detailed description of each file contained in the UC Software ZIP file, see the *Release Notes* found at <http://support.polycom.com/support/spectralink8400>.

- 4 Start the FTP server software and configure it to accept requests from the handset.

In the FTP server software on a computer, create a user with a name and password identical to the phone's default user name and password: user name **PlcmSpIp** with password **PlcmSpIp**.

For more information on how to set up the server, see your FTP server documentation.

Enable the Handset's Network Capabilities

If the WCS computer is not running Microsoft Windows 7, you must copy **84xx.inf** to the WCS so that the computer can detect your SpectraLink 8400 Series Handsets as a USB network device. You will add the handset as a network device with Windows **Add New Hardware** wizard.

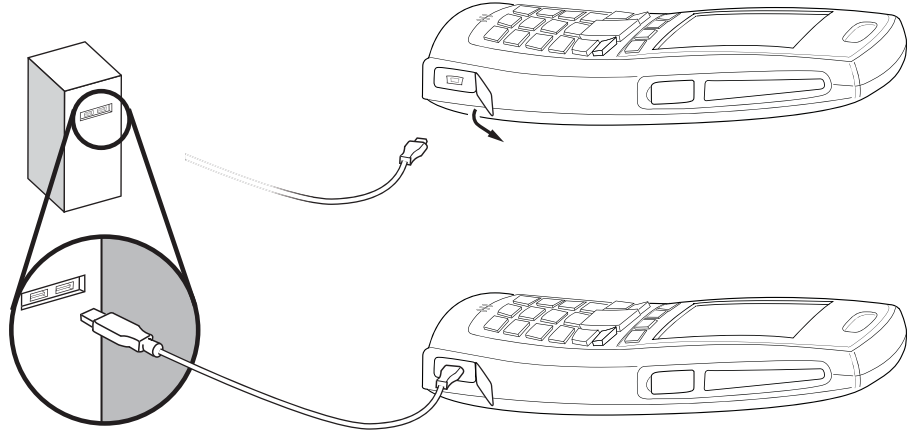


The **84xx.inf** file applies to 32-bit computers running Microsoft Windows® XP SP3 and Microsoft Vista® SP1. If you are using a 64-bit computer running Microsoft Windows Vista operating system, you must use the **84xx-64.inf** file. Computers running Linux do not require **84xx.inf** or **84xx-64.inf**.

To enable the handset's networking capabilities:

- 1 Log into the computer as the administrator.
- 2 (Optional) Download and copy **84xx.inf** onto your 32-bit computer or copy **84xx-64.inf** onto your 64-bit computer from <http://support.polycom.com/support/spectralink8400>.

- 3 Connect the handset to the computer designated as the WCS using the micro USB cable, as shown next.



The Found New Hardware wizard opens.

Connecting the handset to the WCS launches the Found New Hardware wizard automatically. Be sure to leave the handset connected to the WCS for as long as it takes to fully change the phone's wireless configuration parameters.

The Found New Hardware wizard only displays the first time you use each USB slot on your computer.

- 4 In the wizard:
- Select **No, not this time**, and click **Next**.
 - Select **Install from a list or specific location (Advanced)** and click **Next**.
 - Select **Search for the best driver in these locations**.
 - Select the check box for **Include this location in the search**:
 - Browse to your **84xx.inf** or **84xx-64.inf** and click **Next**.

The Linux USB Ethernet/RNDIS Gadget is installed.

A warning will be displayed indicating this driver **has not passed Windows Logo testing**.

- Select **Continue Anyway**.
- Click **Finish**.



Depending on the USB port you choose on the WCS, you may also encounter a Windows alert advising you of a higher speed connection available with a different USB port. You can safely ignore this message or, if you want, you can choose another USB port on your computer that provides high-speed USB 2.0 support.

Set Up the Handset's Network Parameters

Before the handset can communicate with the wireless network, you will need to set the following wireless, WLAN, and provisioning configuration parameters:

- Wireless parameters
- WLAN security parameters
- SSID and WMM-AC parameters
- Regulatory Domain and Radio settings
- Provisioning server parameters

These parameters are defined in the **8400-initial-setup.cfg** template file, which is part of the UC Software 4.0.0 (and attached to this guide).

After you update the **8400-initial-setup.cfg** file, change the master configuration file to use this updated **cfg** file.

To view a detailed reference for all configuration parameters, see the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Wireless Parameters

Next you will enable the wireless interface, and set up the DHCP and Domain Name System (DNS) parameters.

The detailed steps can be found in step 3 in [Network Parameter Procedure](#).

WLAN Security Configuration Parameters

SpectraLink 8400 Series Handsets support the following security policies:

- By default, security is not enabled.
- **Wired Equivalent Privacy (WEP)**. WEP makes use of up to 4 pre-shared encryption keys. These keys can be either 40 or 104 bits in length and must consist of only hexadecimal characters. The SpectraLink 8400 Series Handsets do not support key rotation. During operation, only one key can be used by the phone.
- **Wi-Fi Protected Access Personal (WPA-Personal) and WPA2-Personal**. WPA-Personal and WPA2-Personal use Pre-Shared Key (PSK) for authentication. WPA-Personal uses TKIP for encryption. WPA2-Personal uses AES for encryption.



The SpectraLink 8400 Series Handsets can use one encryption policy or the other but not both at the same time. SpectraLink 8400 Series Handsets run on an SSID that must not be set for both AES and TKIP; otherwise, the handset will not associate to the AP.

In both cases, a PSK is used for the authentication. The PSK is a 64-character hexadecimal key. To make the key easier to configure, a password (sometimes called a passphrase) and the SSID are used to create the PSK. The SpectraLink 8400 Series Handsets can use either the PSK or passphrase form in the configuration.

- **WPA2-Enterprise.** WPA2-Enterprise uses the authentication methods defined by 802.1X, which are also used to authenticate clients. After successful authentication, the AP and the client can negotiate a very secure AES encryption.

There are several Extensible Authentication Protocol (EAP) types supported by WPA2-Enterprise. The SpectraLink 8400 Series Handsets support two common methods: PEAPv0/-MSCHAP/-v2 and EAP-FAST. Both of these require that a certificate be installed on the handset so the phone can authenticate to the RADIUS server (and prevent a man-in-the-middle attack).

- **PEAPv0/-MSCHAP/-v2.** The server certificate is issued by a Certificate Authority (CA). The certificate downloaded to the phone will either be the public certificate of the RADIUS server or the public certificate of the CA. The CA can be publicly available like Verisign or a private CA that your organization has set up.

The handset is preloaded with many of the publicly available CA certificates. You can also store two CA certificates for RADIUS server authentication with the handset.

- **EAP-FAST.** The certificate is called a PAC file and is issued by the RADIUS server. This file can be loaded via the configuration file using a method called 'out of band provisioning'. The certificate can also be loaded directly with the authentication server via 'in band provisioning' or over the air directly in a process referred to as 'Phase Zero Provisioning'.

Full WPA2-Enterprise authentication can take several seconds. If the phone re-authenticates every time it changes APs, a significant audio gap will be created at each roam. Instead, the handsets support fast roaming techniques that allow them to derive keys for the new AP without having to re-authenticate.

There are two fast roaming methods: Opportunistic Key Caching (OKC), which is from the standards body, and Cisco Client Key Management (CCKM). CCKM is only available on Cisco wireless infrastructure. The SpectraLink 8400 Series Handsets support both methods of fast roaming for WPA2-Enterprise.



Only one security mode can be selected at any time.

The detailed steps can be found in step 8 in [Network Parameter Procedure](#).

SSID and WMM-AC

Service Set Identifier (SSID)

The Service Set Identifier (SSID) is an identifier that specifies a particular 802.11 wireless LAN. The SSID can be up to 32 characters long.

Wi-Fi Multimedia Admission Control (WMM-AC)

WMM-Admission Control allows the AP to prevent the wireless medium from being oversubscribed. When WMM-AC is used and if a phone in an active call roams to an AP that does not have sufficient capacity available, the AP will deny the handset's request for bandwidth and the handset will find another AP with adequate bandwidth to ensure good call quality.

The detailed steps can be found in step 12 in [Network Parameter Procedure](#).

Regulatory Domain and Radio Settings

Regulatory Domain

In order to conform to frequency settings regulated by different countries, you must identify a domain and select either the 2.4 GHz or 5 GHz band. If you select the 5 GHz band, you must also select the sub-band(s) used by the APs in your facility.



You must set the regulatory domain before the handsets can be used. There is no default setting for this option and the handsets will not associate with an AP until this option is set.

Setting the correct regulatory domain ensures that the phone complies with local regulatory requirements for your location.

If you are in North America, only regulatory domain 1 is permitted. If any other domain is selected, the error message 'Invalid Regulatory Domain' appears once the handset is restarted and the handset will not associate with an AP. If this should occur, check the label on the handset for the FCC certificate to verify that the handset is for North America only, change the regulatory domain to 1 and update the handset's configuration.

Select the regulatory domain according to your country of operation. If you are in North America, only regulatory domain 1 is permitted although other regulatory domains may be available. Not all regulatory domains may be available on your SpectraLink 8400 Series Handsets.

Domain	Regulatory Body	Country
1	FCC	United States Canada
2	ETSI	Europe (ETSI) New Zealand
10	Australia	Australia

Radio Settings

The Band/Frequency (2.4 GHz or 5 GHz) parameters can be configured for the desired 802.11 band on your WLAN network. If both bands are configured as active, the SpectraLink 8400 Series Handsets' band roaming capabilities will choose the best signal available from both the 2.4 GHz and 5 GHz options. To disable the band roaming mechanism, configure only the band that the SpectraLink 8400 Series Handsets are to use (either 2.4 GHz or 5 GHz, not both).

For maximum performance, you should enable only the same bands and sub-bands as are configured on your wireless infrastructure, otherwise SpectraLink 8400 Series Handsets will waste time looking for a signal on the unused sub-bands, which will impact roaming performance.

Regulatory authorities throughout the world subdivide the 5 GHz band into multiple sub-bands according to the channel assignments in the country of use. After you select the regulatory domain for your country, choose the channels used in your facility, if any. The following tables identify which channels are available in your domain.



The SpectraLink 8400 Series handset menus will display all four sub-bands but only those with channels shown in the following tables are available in your domain. Sub-bands that are not available are marked in the tables as not applicable. If a band is not available and you select it anyway and that is the only selected sub-band, the handset will not be able to associate with an AP and the error message 'Invalid Regulatory Domain Setting' displays on the handset. If this message displays, check that the correct regulatory domain is selected, and then compare the sub-bands that are enabled with the table for that regulatory domain shown next. Enable only those sub-bands that are permitted for your regulatory domain.

For Regulatory Domain 1:

Sub-band of 5 GHz Band	Channel	DFS (Yes/No)
1	36, 40, 44, 48	No
2	52, 56, 60, 64	Yes
3	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Yes
4	149, 153, 157, 161, 165	No

For Regulatory Domain 2:

Sub-band of 5 GHz Band	Channel	DFS (Yes/No)
1	36, 40, 44, 48	No
2	52, 56, 60, 64	Yes
3	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Yes
4	Not applicable	Not applicable

For Regulatory Domain 10:

Sub-band of 5 GHz Band	Channel	DFS (Yes/No)
1	36, 40, 44, 48	No
2	52, 56, 60, 64	Yes
3	100, 104, 108, 112, 116, 136, 140	Yes
4	Not applicable	Not applicable

Transmit Power

For 2.4 GHz and each sub-band of 5 GHz, you will need to set the maximum transmit power level on the handset will use. If no maximum is set, the handset uses the P5 settings for each channel activated.

The handset listens to transmit power control (TPC) and will reduce or increase its power to match what the AP advertises.

The maximum power used by the handsets to transmit in supported 5 GHz sub-bands are defined as follows.

Maximum Power of 5 GHz Band	Definition
P1	1mW RMS power 0dBm (6mW peak OFDM)
P2	5 mW RMS power 7dBm (32mW peak OFDM)
P3	10 mW RMS power 10dBm (63mW peak OFDM)
P4	16 mW RMS power 12dBm (100mW peak OFDM)
P5	25 mW RMS power 14dBm (158mW peak OFDM) (default)

Maximum Power of 5 GHz Band	Definition
P6	40 mW RMS power 16dBm (250mW peak OFDM)
P7	MAX (maximum allowable power for that channel and data rate)

The maximum power used by that the handsets to transmit in supported 2.4 GHz bands are defined as follows.

Maximum Power of 2.4 GHz Band	Definition
P1	1mW RMS power 0dBm (6mW peak OFDM, 1.8mW peak CCK)
P2	5 mW RMS power 7dBm (32mW peak OFDM, 9mW peak CCK)
P3	10 mW RMS power 10dBm (63mW peak OFDM, 18mW peak CCK)
P4	16 mW RMS power 12dBm (100mW peak OFDM, 28mW peak CCK)
P5	25 mW RMS power 14dBm (158mW peak OFDM, 45mW peak CCK) (default)
P6	40 mW RMS power 16dBm (250mW peak OFDM, 71mW peak CCK)
P7	MAX (maximum allowable power for that channel and data rate)



OFDM stands for Orthogonal Frequency Division Multiplexing found in 802.11a and 802.11g , while CCK stands for Complementary Code Keying found in 802.11b .

The detailed steps can be found in step 14 in [Network Parameter Procedure](#).

Provisioning Server Parameters

You may set the provisioning server type, address, user name, and password or obtain these parameters from DHCP. You may want to change the syslog parameters.

The detailed steps can be found in step 21 in [Network Parameter Procedure](#).



For detailed guidance on what to set these parameters to, see *Best Practices Guide to Network Design Considerations for SpectraLink 8400 and 8000 Series Wireless Telephones* at <http://support.polycom.com/support/spectralink8400>.

Network Parameter Procedure

In the following procedure, you will change parameter values in the **8400-initial-setup.cfg** configuration template.



A sample **8400-initial-setup.cfg** file is attached to this guide to assist with configuration of the SpectraLink 8400 Series Handsets.

Polycom recommends that you use the latest version of Adobe Reader to view the contents of this guide and for access to the attached configuration template. Click the paperclip icon on the left-hand side to locate the attachment.

To modify the network configuration file:

- 1 Copy **8400-initial-setup.cfg** from the UC Software 4.0.0 build into the FTP directory you created in [Set Up the FTP Server](#) on page 11.

For example, `C:\FTP_root\SpectraLink8400\8400-initial-setup.cfg`

- 2 Open **8400-initial-setup.cfg** in an XML editor.



Polycom recommends that you use an XML editor to create/edit the configuration files. This will enable you to save all configuration files that you create as valid XML files.

If the configuration files are not valid, they will not load on the handset. In this case, an error message will be logged to the provisioning server.

- 3 Enable the use of device parameters (`device.set="1"`).



You must enable the global `device.set` parameter when the initial installation is done, and it must remain enabled.

Two device parameters exist for every configuration parameter—`device.xxx.set` and `device.xxx`—and both must be modified in the configuration file.

For example, if you want to change `device.wifi.enabled`, you must set `device.wifi.enabled.set` in the configuration file you modify on the WCS.

For more information, see [<device/>](#) on page 64.

4 Enable the wireless interface (`device.wifi.enabled="1"`).

device.wifi	
device.wifi.enabled	1
device.wifi.enabled.set	1
device.wifi.ssid	

5 If you want to use DHCP addressing, enable the DHCP flag on the wireless interface if not using static IP addressing (`device.wifi.dhcpEnabled="1"`).

device.wifi.ipNetwork	
device.wifi.dhcpEnabled	1
device.wifi.dhcpEnabled.set	1
device.wifi.ipAddress	
device.wifi.ipAddress.set	0

If you want to use static IP addressing, do the following:

- Disable the DHCP flag if you are using static IP addressing (`device.wifi.dhcpEnabled="0"`).
- Set the network address of the wireless interface if not using DHCP (`device.wifi.ipAddress="192.168.0.100"`).
- Set the network mask address of the wireless interface if not using DHCP (`device.wifi.subnetMask="255.0.0.0"`).
- Set the IP gateway address for the wireless interface if not using DHCP (`device.wifi.IPgateway="192.168.0.1"`).

device.wifi.ipNetwork	
device.wifi.dhcpEnabled	0
device.wifi.dhcpEnabled.set	1
device.wifi.ipAddress	192.168.0.100
device.wifi.ipAddress.set	1
device.wifi.subnetMask	255.0.0.0
device.wifi.subnetMask.set	1
device.wifi.ipGateway	192.168.0.1
device.wifi.ipGateway.set	1
device.wifi.dhcpBootServer	
device.wifi.dhcpBootServer.set	0

6 Set the DNS parameters to appropriate values for your organization.

For example, DNS domain name (`device.dns.domain`), DNS server name (`device.dns.serverAddress`), and DNS alternate server name (`device.dns.altSrvAddress`).

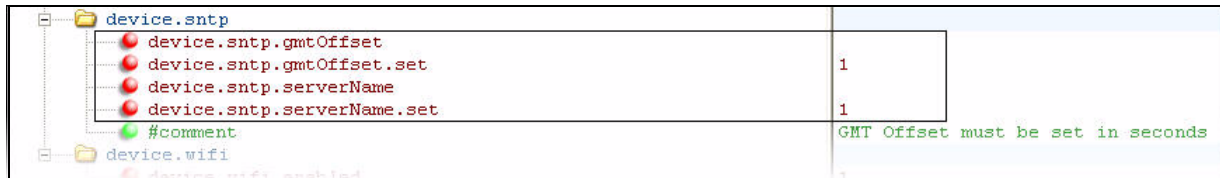
device.dns	
device.hostname	
device.hostname.set	0
device.dns.domain	
device.dns.domain.set	1
device.dns.serverAddress	
device.dns.serverAddress.set	1
device.dns.altSrvAddress	
device.dns.altSrvAddress.set	1
device PROV	
device PROV.serverType	



This step is optional. The DNS parameters can be supplied by DHCP.

7 Set SNTP parameters to appropriate values for your organization.

For example, SNTP server name (`device.snntp.serverName`) and SNTP GMT offset (`device.snntp.gmtOffset`).

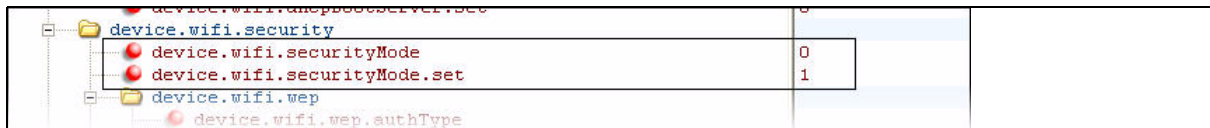


This step is optional. The SNTP parameters can be supplied by DHCP.

8 Set the wireless security mode (`device.wifi.securityMode`).

The possible values are:

- **None** = No security (default). If you select this value, there is no over-the-air encryption. Go to step 12.
- **WEP** = WEP. Go to step 9.
- **WPA-PSK** = WPA-Personal. Go to step 10.
- **WPA2-PSK** = WPA2-Personal. Go to step 10.
- **WPA2-Enterprise** = WPA2-Enterprise. Go to step 11.



9 Set the WEP configuration parameters as follows:

a Select the authentication method (`device.wifi.wep.authType`).

The possible values are:

- » **0** = open system (default)
- » **1** = shared key authentication

b Select the default key (`device.wifi.wep.defaultKey`).

The possible values are:

- » **1** = Key 1 (default)

- » 2 = Key 2
 - » 3 = Key 3
 - » 4 = Key 4
- c** Enable WEP encryption of the wireless data (device.wifi.wep.encryptionEnabled).
- d** Set one or more of the four keys (device.wifi.wep.keyx, where x=1 to 4).
- The values must be hexadecimal, 10 characters for 40 bits or 26 characters for 104 bits.
- e** Select the key length (device.wifi.wep.keyLength).
- The possible values are:
- » 0 = 40 bits (default)
 - » 1 = 104 bits

device.wifi.security	
device.wifi.securityMode	1
device.wifi.securityMode.set	1
device.wifi.wep	
device.wifi.wep.authType	0
device.wifi.wep.authType.set	1
device.wifi.wep.defaultKey	1
device.wifi.wep.defaultKey.set	1
device.wifi.wep.encryptionEnabled	1
device.wifi.wep.encryptionEnabled.set	1
device.wifi.wep.key1	1
device.wifi.wep.key1.set	1
device.wifi.wep.key2	0
device.wifi.wep.key2.set	0
device.wifi.wep.key3	0
device.wifi.wep.key3.set	0
device.wifi.wep.key4	0
device.wifi.wep.key4.set	0
device.wifi.wep.keyLength	1
device.wifi.wep.keyLength.set	1
device.wifi.wpa2psk-wpa2psk	
device.wifi.wpa2psk.wpa2psk.keyType	0
device.wifi.wpa2psk.wpa2psk.keyType.set	0

10 Set the WPA-Personal or WPA2-Personal Security configuration parameters as follows:

- a** Set the Pre-Shared Key (PSK) type (device.wifi.wpa2psk.wpa2psk.keyType).
- The possible values are:
- » 0 = Hexadecimal key. Go to step **b**.
 - » 1 = Passphrase (default). Go to step **c**.
- b** Set the hexadecimal key (device.wifi.wpa2psk.wpa2psk.key).
- The value must be a 64-character key.

- c Set the passphrase (`device.wifi.psk.key`).
The value must be 8 to 63 ASCII characters in length.

device.wifi.security	
device.wifi.securityMode	2
device.wifi.securityMode.set	1
device.wifi.wep	
device.wifi.wpa2psk	
device.wifi.psk.keyType	1
device.wifi.psk.keyType.set	1
device.wifi.psk.key	
device.wifi.psk.key.set	1
#comment	Key Types: 0-preshe
device.wifi.wpa2Ent	
device.wifi.wpa2Ent.method	
device.wifi.wpa2Ent.method.set	0

11 Set WPA2- Enterprise Security configuration parameters as follows:

- a Set the fast roaming method to one of the methods supported on your wireless infrastructure. (`device.wifi.wpa2Ent.roaming`)

The possible values are:

- » OKC (default)
- » CCKM

- b Set the WPA2- Enterprise Security user name (`device.wifi.wpa2Ent.user`).

By default, the value is **PlcmSpIp**.

- c Set the WPA2- Enterprise Security password (`device.wifi.wpa2Ent.password`). By default, the value is **PlcmSpIp**.

- d Set the EAP type used for authentication (`device.wifi.wpa2Ent.method`).

The possible values are:

- » EAP-PEAPv0-MSCHAPv2. (default) See step e.
- » EAP-FAST. See step f or g.



Only the values EAP-PEAPv0-MSCHAPv2 and EAP-FAST are supported. Using any other value may cause connectivity issues.

- e If you selected PEAPv0/MSCHAP/-v2 for the EAP type:
 - » Select the security profile (`device.sec.TLS.profileSelection.dot1x`). The possible values are **PlatformProfile1** and **PlatformProfile2**.



Polycorn recommends that you select the value 0, which is the default value.

- » Select the provisioning profile (device.sec.TLS.profileSelection.provisioning). The possible values are 0 and 1.
- » Set the parts of the certificate store that are valid for this security profile and which can be used to verify the server (device.sec.TLS.profile.caCertListx, where x= 1 or 2). The possible values are:
 - » 0 = Use only built-in default certificates.
 - » 1 = Use default and custom certificate #1.
 - » 2 = Use default and custom certificate #2.
 - » 3 = Use any certificate (built-in or either custom certificate).
 - » 4 = Use only custom certificate #1.
 - » 5 = Use only custom certificate #2.
 - » 6 = Use either custom certificate #1 or custom certificate #2.
- » If you are using a private CA, load the private CA certificate to use for PEAP authentication into one of the custom slots.

Depending on the value you select in the step above, use device.sec.SSL.customCaCert1 or device.sec.SSL.customCaCert2. For example, if you set device.sec.TLS.profile.caCertList1 to 5, use device.sec.SSL.customCaCert2 for your certificate.

You must start with a certificate in PEM/base64 format. This is an ASCII format that can be stored in an XML file. Copy only the contents between the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" without hard returns.

Store the certificate in the configuration file using (device.sec.TLS.customCaCert1) for slot 1 and (device.sec.TLS.customCaCert2) for slot 2.

For example (without hard returns):

```
device.sec.TLS.customCaCert1="MIIDhzCCAvCgAwIBAgIJALY
gwM545734tgYIWSn4A1UECBMOQW5kaHJhIFByYWRlc2gxZjAQBgNV
BACtCUh5ZGVyYWJhZDEhMB8GA1UEChMYSGVsYm99Zb2Z044f59WEeg
WF4F8fe2FVQQLew1XaXJlbGVzcyBUZWFtMRMwEQYDVQDFApoc193
bGFuX2NhMB4XDTA2MDQxNzEwMjUyMFoXDTE2MDQxNDEwMjUyMFow
YoxCzAJBgNVBAYTAklOMRcwFQYDVQQLIEw5BmRocmEgUHQhZGVzaD
ESMBAGA1UEBxMjSHlkZXJhYmFkMSEwHwYDVQKEXhIZWxsY3NvZnQ
gSW5kaWEgUHZ0LiBMDGQxYjAUBgNVBAsTDVdpcmVsZXNzIFRlYW0x
```

```
EzARBgNVBAMUCmhzX3dsYW5fY2EwgZ8wDQYJKoZIhvcNAQEBBQADg
Y0AMIGJAoGBAJzESpj3Rshcw7cR9dSpQDu0TtN1CnfVJTTCIdehkLD
X4Msns4Zv1IfhoBhAQpd47ec"
```



When using an XML editor, leave out the quotation marks at the beginning and end of the certificate and remove the line feeds/hard returns.

f If you selected EAP-FAST for the EAP type and want to perform out-of-band provisioning—the PAC file can be loaded into the handset during configuration:

- » Disable in-band provisioning (device.wifi.wpa2Ent.eapFast.inBandProv="0").
- » Set the PAC file password (device.pacfile.password).
- » Set the PAC file (device.pacfile.data).

Since the PAC file is, by default, a binary file, it cannot be stored in the configuration file in this form. You must convert the PAC file to a base64 encoded file. Copy only the contents between the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" without hard returns.



Use openssl command to convert the file to base64 encoded file:

```
$ openssl enc -base64 -in eapuser.pac -out eapuser.pac.b64
```

For example (without hard returns):

```
device.pacfile.data="AQApBAUAAAGG+81pXXvXy01Uy250kTnp
yAuqb+23455Kfnfg4WFkffwergr72ef57g/1lGghe04xH3Ne9I/ky
qmolQN0eis6B7YoLHh3N9G9kIltg98flDNgiPmh+dUm9GxCsSvsyI
BjxKceqzkyPgpDaxhV/vZesD7Q6XI3464SGkighEFJD+m00+Hewex
jXFyY0WJNE0TXyNQhOwr27KQRqZYrUq9BqyDE9FFZoweA3Jtog9ze
h0QZEe4TkGeKQotlaT0we6chh8+DPLaafCdCwXGd7aDQfC8eMEtX2
gMpPoDIhv9RXVunca3T4JXVWrumQxd7rm1Dl/MKjsi/4jjIHg3+BF
qpABSetXVCZA9HUo+c="
```



When using an XML editor, leave out the quotation marks at the beginning and end of the certificate.

device.wifi.security	
device.wifi.securityMode	3
device.wifi.securityMode.set	1
device.wifi.wep	
device.wifi.wpa2psk	
device.wifi.wpa2Ent	
device.wifi.wpa2Ent.method	6
device.wifi.wpa2Ent.method.set	1
device.wifi.wpa2Ent.roaming	0
device.wifi.wpa2Ent.roaming.set	1
device.wifi.wpa2Ent.user	PlcmSpIp
device.wifi.wpa2Ent.user.set	1
device.wifi.wpa2Ent.password	PlcmSpIp
device.wifi.wpa2Ent.password.set	1
device.wifi.wpa2Ent.peap	
device.wifi.wpa2Ent.eapFast	
device.wifi.wpa2Ent.eapFast.inBandProv	0
device.wifi.wpa2Ent.eapFast.inBandProv.set	1
#comment	Valid WPA2 Enterprise Meth
#comment	Valid WPA2 Enterprise roa
#comment	Valid Security modes: 0-No

- g** If you selected EAP-FAST for the EAP type and want to perform in-band provisioning – the PAC file can be automatically loaded from the network:
- » Enable in-band provisioning
(device.wifi.wpa2Ent.eapFast.inBandProv="1").
 - » Remove any existing PAC file by selecting **Settings > Advanced Settings > Network Configuration > Network Interfaces > WiFi Menu > WPA2-Enterprise > PAC File Menu > Remove PAC File > Remove** on the handset, and pressing the OK soft key.
- When prompted, enter the administrative password. The default value is **456**.

- 12** Set the Service Set Identifier (SSID) of the wireless network (device.wifi.ssid="SSID1").
- 13** Determine whether or not the handset will connect only to APs that enforce admission control (Wi-Fi Multimedia Admission Control (WMM-AC)) and set the parameters accordingly (device.wifi.acMandatory).
- Use the default (the value **0**) to set the Admission control to optional or to **1** if it is required.
- 14** Set the regulatory domain to the appropriate value for your location (device.wifi.radio.regulatoryDomain="1").

For a list of supported regulatory domains, see [Regulatory Domain and Radio Settings](#) on page 16.



You must set the regulatory domain before the handsets can be used.

device.wifi	
device.wifi.enabled	1
device.wifi.enabled.set	1
device.wifi.ssid	SSID1
device.wifi.ssid.set	1
device.wifi.QoS	
device.wifi.acMandatory	
device.wifi.acMandatory.set	1
device.wifi.ipNetwork	
device.wifi.security	
device.wifi.radio	
device.wifi.radio.regulatoryDomain	1
device.wifi.radio.regulatoryDomain.set	1

- 15 Enable the 5 GHz wireless band
(`device.wifi.radio.band5GHz.enable="1"`).
- 16 For each 5 GHz sub-band 1 through 4, enable/disable that specific 5 GHz subband (`device.wifi.radio.band5GHz.subBandx.enable="1"`, where $x=1$ to 4).
- 17 For each 5 GHz sub-band 1 through 4, set the maximum power that the handset uses to transmit in that band.
(`device.wifi.radio.band5GHz.subBandx.txPower`, where $x=1$ to 4)

The supported values are P1 to P7 (although not all may be available). The default value is P5 (if no settings is selected). For power definitions, see [Regulatory Domain and Radio Settings](#) on page 16.

device.wifi.radio	
device.wifi.radio.regulatoryDomain	1
device.wifi.radio.regulatoryDomain.set	1
device.wifi.radio.band2_4GHz	
device.wifi.radio.band2_4GHz.enable	
device.wifi.radio.band2_4GHz.enable.set	0
device.wifi.radio.band2_4GHz.txPower	
device.wifi.radio.band2_4GHz.txPower.set	0
device.wifi.radio.band5GHz	
device.wifi.radio.band5GHz.enable	1
device.wifi.radio.band5GHz.enable.set	1
device.wifi.radio.band5GHz.subBand1.enable	1
device.wifi.radio.band5GHz.subBand1.enable.set	1
device.wifi.radio.band5GHz.subBand1.txPower	6
device.wifi.radio.band5GHz.subBand1.txPower.set	1
device.wifi.radio.band5GHz.subBand2.enable	1
device.wifi.radio.band5GHz.subBand2.enable.set	1
device.wifi.radio.band5GHz.subBand2.txPower	6
device.wifi.radio.band5GHz.subBand2.txPower.set	1
device.wifi.radio.band5GHz.subBand3.enable	1
device.wifi.radio.band5GHz.subBand3.enable.set	1
device.wifi.radio.band5GHz.subBand3.txPower	6
device.wifi.radio.band5GHz.subBand3.txPower.set	1
device.wifi.radio.band5GHz.subBand4.enable	1

- 18 Enable the 2.4 GHz wireless band
(`device.wifi.radio.band2_4GHz.enable="1"`).
- 19 Set the maximum power that the handset uses to transmit in that band
(`device.wifi.radio.band2_4GHz.txPower`).

The supported values are P1 to P7 (although not all may be available). The default value is P5 (if no settings is selected). For power definitions, see [Regulatory Domain and Radio Settings](#) on page 16.



The handset will choose the best channel for its current position, regardless of band.

- 20 Set the syslog parameters to appropriate values for your organization.
- 21 Set provisioning parameters to appropriate values for your organization.

For example:

- The provisioning server type (`device.prov.serverType="FTP"`)
- The provisioning server name (`device.prov.serverName="<server host name>"`)
- The provisioning server user name (`device.prov.user="<login Id"`, the default is **PlcmSpIp**)
- Provisioning server password
(`device.prov.password="<password>"`, the default is **PlcmSpIp**)

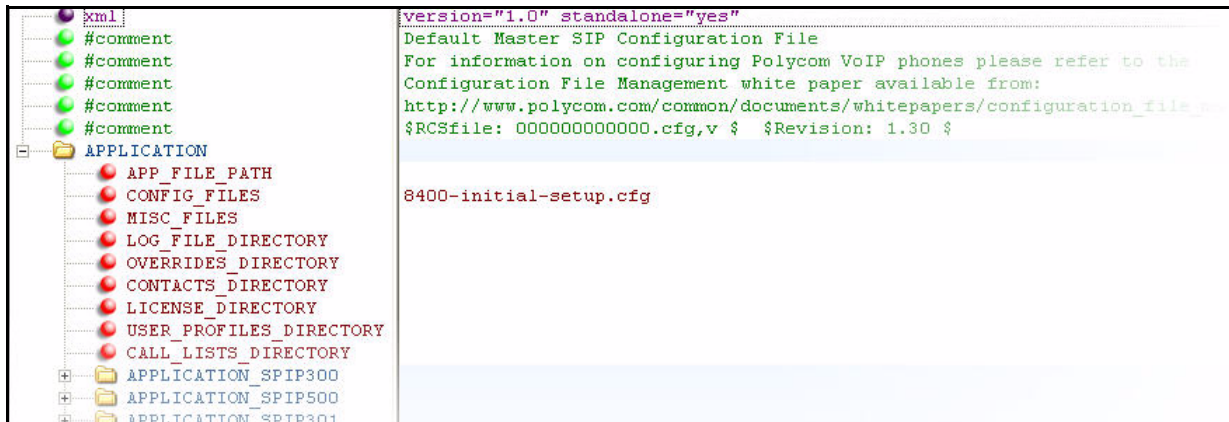
Property	Value
<code>device.prov.serverType</code>	FTP
<code>device.prov.serverType.set</code>	1
<code>device.prov.serverName</code>	hostname@polycom.com
<code>device.prov.serverName.set</code>	1
<code>device.prov.user</code>	PlcmSpIp
<code>device.prov.user.set</code>	1
<code>device.prov.password</code>	PlcmSpIp
<code>device.prov.password.set</code>	1
<code>#comment</code>	Valid Server types: 0-FTP,

- 22 Save the XML file to accept your changes.

To change the master configuration file:

- 1 Open `000000000000.cfg` in an XML editor.

2 Edit the file to use the network configuration file you created above.



Part II: Initial Provisioning of the Handsets

Initial provisioning of each SpectraLink 8400 Series handset requires:

- A physical USB connection between the handset and the WCS as shown in [Enable the Handset's Network Capabilities](#) on page 12.
- Setup of the handset's network connection parameters. See [Set Up the Handset's Network Parameters](#) on page 14.

To perform the initial provisioning of the handset:

- 1 Plug the USB cable between the phone (micro USB plug) and the WCS.
- 2 Reboot the handset to change the network configuration.

After the handset reboots and picks up the information from the network configuration file, it should be connected to the wireless network and be ready for the next provisioning step.

Part III: Setting Up the Provisioning Server

Next, you must set up the provisioning server to update the remainder of the configuration parameters.

For organizational purposes, Polycom recommends configuring a separate log file directory, an override directory, a contact directory, and a license directory, though this is not required. The different directories can have different access permissions. For example, you can allow LOG, CONTACTS, and OVERRIDES to have full read and write access, and LICENSE to have read-only access.



By default, Polycom sets FTP as the provisioning protocol on all SpectraLink 8400 Series handsets.

The default provisioning server protocol is FTP and is the focus of this deployment guide. Other supported protocols include TFTP, HTTP, and HTTPS.

For more information, see [Setting Up an FTP Server](#) on page 105.

To set up the provisioning server:

- 1 On your computer, create a folder to store the UC Software executable and the configuration files that come with the UC Software.

For example, **C:\SpectraLink8400**

- 2 Copy the latest UC Software from the WCS to the provisioning server.

See step 2 in [Set Up the FTP Server](#) on page 11.

- 3 Extract all files from the UC Software ZIP file to the newly created folder maintaining the same folder hierarchy.

Although the ZIP file contains many files, the following files are the only ones you need:

- **3111-36150-001.sip.ld** (for SpectraLink 8440)
- **3111-36152-001.sip.ld** (for SpectraLink 8450)
- **000000000000.cfg**
- **SoundPointIPWelcome.wav** (welcome tone)

For a detailed description of each file contained in the UC Software ZIP file, see the *Release Notes* found at

<http://support.polycom.com/support/spectralink8400> .

- 4 Start the FTP server software and configure it to accept requests from the handset.

In the FTP server software on a computer, create a unique user with names and passwords.

For more information on how to set up the server, see your server documentation.

You will use this provisioning server to maintain the handset's configuration and, periodically, update the software in the future.

Part IV: Deploying the Handsets From the Provisioning Server

You can create specific configuration files for each handset, one company-wide configuration file for all handsets in your organization, or you can put all configuration parameters into one file. The example discussed next describes the scenario using two configuration files.

For details on the features available on the SpectraLink 8400 Series Handsets, see [Configuring SpectraLink 8400 Series Handsets](#) on page 39.

For more information on the reasons for creating company-specific configuration files, see the *Polycom UC Software Provisioning Best Practices* white paper at <http://www.polycom.com/global/documents/whitepapers/uc-software-provisioning-best-practices-whitepaper.pdf>.

Deploy SpectraLink 8400 Series Handsets by performing the following steps on the provisioning server:

- 1 Create a phone configuration file. See [Creating a Phone Configuration File](#) on page 32.
- 2 Create a master configuration file for each handset. See [Creating a Master Configuration File](#) on page 34.
- 3 Download the new configuration to the handset. See [Downloading the New Configuration](#) on page 36.

By default, the SpectraLink 8400 Series Handsets run Polycom UC Software 4.0.0. When you want to upgrade the software on the handsets in the future, follow the directions in [Upgrading Software on Your Handsets](#) on page 37 to get the latest software. You must verify that the configuration files you created for [Creating a Phone Configuration File](#) on page 32 will work with the new UC Software. New and changed configuration parameters are described in the *Release Notes*. You do not need to change the master configuration files unless you change the names of the phone configuration file or add new files.

Creating a Phone Configuration File

This section provides instructions on how to create a phone configuration file.



Polycom recommends that you use an XML editor to create and edit valid configuration files.

If the configuration files are not valid, they will not load on the handset. In this case, an error message will be logged to the provisioning server.

To create a phone configuration file:

- 1 Obtain the handset’s MAC address from the barcoded label on the handset’s battery pack well or on the outside of the shipping box.
- 2 Copy **wireless.cfg** from the UC Software 4.0.0 build into the FTP directory you created in [Part III: Setting Up the Provisioning Server](#) on page 30.

For example, C:\SpectraLink8400\wireless.cfg

- 3 Rename the file to **phone[PHONE_MAC_ADDRESS].cfg**.
- 4 Change the phone configuration file as required.

For more information on configuring features on the SpectraLink 8400 Series Handsets, see [Configuring SpectraLink 8400 Series Handsets](#) on page 39.

For example:

phone	
apps	
bcma	
bluetooth	
call	
dialplan	
dialplan.digitmap	[2346789]11 [0-1][2-9]11 0[#T] 00 01[2-9]xx.[#T] *xx 011x.[#T]
exchange	
device	
feature	
feature.messaging.enabled	1
feature.presence.enabled	1
feature.exchangeCalendar.enabled	1
keypadLock	
keypadLock.enabled	1
keypadLock.idleTimeout	0
messaging	
messaging.quicknotes.1	Hello
messaging.quicknotes.2	Bye
messaging.quicknotes.3	Thx
messaging.quicknotes.4	R U available
messaging.quicknotes.5	Cannot talk. In a meeting.
messaging.quicknotes.6	Call back later.
messaging.quicknotes.7	See U at lunch.
log	
mb	
np	
oai	
oai.gateway.address	172.29.75.195
oai.userId	12345678
prov	
ptt	
reg	
roaming_buddies	
roaming_privacy	
saf	
up	
up.multiKeyAnswerEnabled	1
up.headsetOnlyAlerting	1
voIpProt	
wifi	



If you are using an HTTPS server using Transport Layer Security (TLS), you may also need to install the appropriate certificates on the handset and select those certificates in the TLS Profiles where they are selected for provisioning. See TLS Profiles in the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

- 5 Save the XML file to accept your changes.
- 6 Make a copy of **phone[MACADDRESS].cfg** for each handset you want to deploy, replacing '[MACADDRESS]' in the filename with the MAC address of each handset.

For example:

For handset MAC address	Create configuration file
00907abe80a6	phone00907abe80a6.cfg
00907abe80b3	phone00907abe80b3.cfg
00907abe8222	phone00907abe8222.cfg

Creating a Master Configuration File

This section provides instructions on how to modify the master configuration file.

To modify the master configuration file:

- 1 Modify the **000000000000.cfg** file that is part of the UC Software 4.0.0 software.



Creating a handset-specific configuration file provides a convenient means of overriding the behavior of one or more handsets without changing the baseline configuration files for an entire system.

2 Add contents to the master configuration file.

For example:

<pre> xml #comment #comment #comment #comment #comment APPLICATION APP_FILE_PATH CONFIG_FILES MISC_FILES LOG_FILE_DIRECTORY OVERRIDES_DIRECTORY CONTACTS_DIRECTORY LICENSE_DIRECTORY USER_PROFILES_DIRECTORY CALL_LISTS_DIRECTORY APPLICATION_SPIP300 APPLICATION_SPIP500 APPLICATION_SPIP301 APPLICATION_SPIP302 APPLICATION_SPIP303 </pre>	<pre> version="1.0" standalone="yes" Default Master SIP Configuration File For information on configuring Polycom VoIP phones please refer to the Configuration File Management white paper available from: http://www.polycom.com/common/documents/whitepapers/configuration_file \$RCSfile: 000000000000.cfg,v \$ \$Revision: 1.30 \$ sip.ld phone[PHONE_MAC_ADDRESS].cfg </pre>
--	---



The order of the configuration files listed in CONFIG_FILES is significant:

- The files are processed in the order listed (left to right).
- If the same parameter is included in more than one file, the parameter in the file read first will be used.

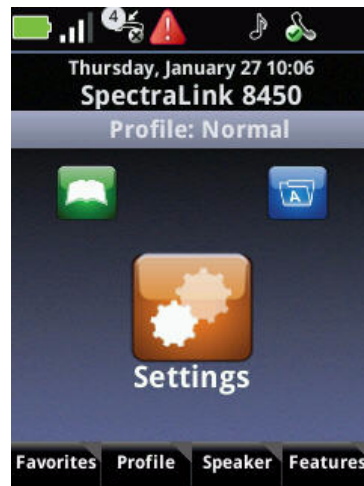


For more information on using substitution in the master configuration file, see the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Downloading the New Configuration

To download the new configuration to the handsets:

- 1 Select **Settings** on the Home screen, and then do one of the following:
 - Select **Basic Settings > Update Configuration**.
 - Select **Basic Settings > Restart Phone**.



- 2 Wait for the phone to restart.

In a standard deployment, the following messages will display on the screen:

- Please wait
- Reboot initiated
- Starting application
- Application started

The update process will take some time.

- 3 Ensure that the configuration process is completed correctly by doing the following:
 - Monitor the provisioning server event log and the uploaded event log files (if permitted). All configuration files used by the provisioning server are logged. To make changes to the information that is logged, see [<log/>](#) on page 72.
 - To determine the UC software version running on the handset, select **Settings** on the Home screen, and select **Status > Platform > Application > Main**.
 - Check for configuration file errors. Select **Settings** on the Home screen, and select **Status > Platform > Configuration**.

You can now instruct your users to start making calls.

Upgrading Software on Your Handsets

To upgrade the handset's software, you need to:

- Download the latest Polycom UC Software to the provisioning server from the SpectraLink 8400 Series Handsets support page – the same place you found this deployment guide. See the next section, [Locating the Latest Software](#).
- Download the new Polycom UC Software to the handset. See [Downloading New Software](#) on page 37.

For more information on upgrading the UC Software, see 'Upgrading the SIP Application' in the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Locating the Latest Software

To determine the latest software version, go to the VoIP SIP Software Release matrix on the Polycom Customer Support web site at http://downloads.polycom.com/voice/voip/sip_sw_releases_matrix.html.

Download the latest UC Software and *Release Notes* from <http://support.polycom.com/support/spectralink8400> to the provisioning server.

Downloading New Software

To download and install the new UC Software to the handset, you need to:

- Extract the appropriate files from the UC Software ZIP file as you did in [Part III: Setting Up the Provisioning Server](#) on page 30.
- Review the *Release Notes* to determine if there are any new and changed configuration parameters.
- Reboot the handset to download the new software.

To update the software on the handset:

- 1 Reboot the handsets by selecting **Settings** on the Home screen, and select **Advanced Settings > Reboot Phone**. Select the **Yes** soft key.

When prompted, enter the administrative password and press the **Enter** soft key. The default administrative password is **456**.

In a standard deployment, the following messages will display on the screen:

- Please wait
- Reboot initiated
- Waiting for network to initialize
- Downloading new application
- Saving new application
- Checking new application
- Extracting application
- Starting application
- Application started

The reboot process will take some time.

- 2 Ensure that the configuration process completed correctly.

On the handset, select **Settings** on the Home screen, and select **Status > Platform > Application > Main** to see the UC Software version and **Status > Platform > Configuration** to see the configuration files downloaded to the handset.

Configuring SpectraLink 8400 Series Handsets

Now that your Polycom® SpectraLink® 8400 Series Handsets are working, they are ready for your users. However, you may want to make some basic optimization changes to fine-tune your system for your users or add additional features or functionality.

This chapter provides information on how to configure the following SpectraLink 8400 Series Handsets features:

- [Time and Date Display](#)
- [Notification Profiles](#)
- [Bluetooth Headset Support](#)
- [Keypad Lock](#)
- [Push-to-Talk](#)
- [Multi-Key Answer](#)
- [User Profile Portability](#)
- [Barcode Scanner Support](#)
- [Browser and Applications](#)
- [Open Application Interface](#)
- [Instant Messaging and Presence](#)
- [Location Service](#)
- [Calendaring](#)

For information on all of the other configuration parameters that you can change—for example, setting up registrations on the handsets and connecting to voicemail—and the sample templates that are included in the software package, see the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

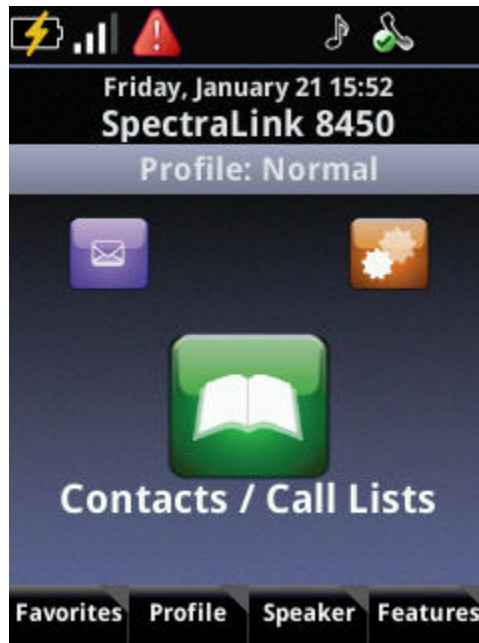
Setting Up Basic Features

This section shows you how to make configuration changes to enable the following basic features:

- [Time and Date Display](#)
- [Notification Profiles](#)
- [Bluetooth Headset Support](#)
- [Keypad Lock](#)
- [Push-to-Talk](#)
- [Multi-Key Answer](#)
- [User Profile Portability](#)

Time and Date Display

The handset maintains a local clock. You can display the time and date during an active call and when the handset is idle. The clock and calendar must be synchronized to a remote Simple Network Time Protocol (SNTP) time server. The time and date are not displayed on the handset until a successful SNTP response is received. The time and date display can display in one of several formats or can be turned off.



For instructions on turning off the time and date display, see [Display](#) on page 50.

Notification Profiles

The SpectraLink 8400 Series Handsets support four notification profiles: **Normal**, **Silent**, **Meeting**, and **Custom 1**.

With each profile, you can assign special alerts and ringtones and vibrations for certain events, for example, when the user sends a barcode scan to the Quick Barcode Connector application, when the user places the handset in the Speakerphone Dock, and when the user receives an instant message on their handset.

By default, the ringing and alert volumes are at the same level. If configured in this way, the ringer volume is used for ringing only and the alert volume is different for each alert type.

For detailed information on configuration parameters, see [<np/>](#) on page 73.

Bluetooth Headset Support

You can use Bluetooth v2.1 headsets with your handsets.



Using a Bluetooth headset while the 2.4 GHz band is enabled is not recommended for the highest voice quality due to inherent limitations with Bluetooth technology.

Using a Bluetooth headset in highly loaded Bluetooth environments is not recommended for the highest voice quality due to inherent limitations with Bluetooth technology.

For detailed information on configuration parameters, see [<bluetooth/>](#) on page 64.

Keypad Lock

You can configure the SpectraLink 8400 Series Handsets to support a keypad lock feature.

For detailed information on configuration parameters, see [<keypadLock/>](#) on page 72.

Push-to-Talk

The Push-to-Talk (PTT) feature is disabled by default. When enabled, SpectraLink 8400 Series Handsets use channels 1 to 25 for incoming and outgoing PTT calls. The use of channels 24 (Priority) and 25 (Emergency) cannot be disabled.

The PTT button is on the left side of the handset. When enabled, subscribed channels are available for transmission and reception. You can configure the SpectraLink 8400 Series Handsets to be compatible with existing SpectraLink 8020/8030 Handsets.

The handset can also receive regular calls while PTT calls are in session. Once the call is answered, the PTT call ends.



The Push-to-Talk feature uses a multicast address. Multicasting is a technique developed to send packets from one location in the Internet to many other locations, without any unnecessary packet duplication. In multicasting, one packet is sent from a source and is replicated as needed in the network to reach as many end users as necessary.

You do not need to use the default multicast address. If you want to use a different multicast address, check if the address already has an official purpose.

For the list of current multicast addresses, go to <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>.

The following table summarizes the supported audio codecs for PTT:

Algorithm	Ref.	Raw Bit Rate	IP Bit Rate	Sample Rate	Default Payload Size	Effective audio bandwidth
G.711 μ -law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	20ms	3.5 KHz
G.722	RFC 1890	64 Kbps	80 Kbps	16 Ksps	20ms	7 KHz
G.726QI	RFC 3951	24Kbps	N/A	N/A	30ms	3.5 KHz

For detailed information on configuration parameters, see [<ptt/>](#) on page 98.

Multi-Key Answer

If configured, users can answer an incoming call by pressing any hard or soft keys on the front of the SpectraLink 8400 Series handset. The keys on the sides of the handsets and the **End** key are excluded.

For detailed information on configuration parameters, see [<up/>](#) on page 103.

User Profile Portability

The User Profile Portability feature enables users to access their personal phone settings from any phone in the organization. This means that users can access their contact directory and speed dials, as well as other phone settings, even as they temporarily change work areas. This feature is particularly useful for remote and mobile workers who do not have a dedicated work space and conduct their business in more than one location. The User Profile feature is also beneficial if an office has a common conference phone. In this case, multiple users can use the phone and access their own settings.

If a user changes any settings while logged in to a phone, the settings will be saved and displayed the next time the user logs in to a phone. When a user logs out, the user's personal phone settings no longer display.

If you set up the User Profile feature, a user can log in to a phone by entering their user ID and password. Default passwords are preset in the configuration to the numerals **123**.



If a phone is in the logged out state and requires a user login, you may be able to use the phone to place emergency calls to standard emergency numbers such as 911 and other pre-configured phone numbers. These numbers are configured by your administrator (see the `<dialplan/>` parameter definition in the latest *Polycom UC Software Administrator's Guide*).

If the User Profile feature is set up on your company's phones, users can:

- Log in to a phone to access their personal phone settings.
- Log out of a phone after they finish using it.
- Place a call to an authorized number from a phone that is in the logged out state and requires a user login.
- Change their user password.

When you set up the User Profile feature, you will have to plan in advance whether you want to require users to always log in to a phone. If the User Profile feature is enabled, but not required, users can choose to use the phone as is (that is, without access to their personal settings), or they can log in to display their personal settings.

You can also choose to define default credentials for the phone (see the next section, [Creating a Phone Configuration File](#)). If you specify a default user ID and password, the phone automatically logs itself in each time an actual user logs out or the phone restarts or reboots. When the phone logs itself in using the default login credentials, a default phone profile is displayed (as defined in the phone's master configuration file on the provisioning server). In this scenario, users will still have the option to log in and view their personal settings.

To set up the User Profile feature, you will need to perform the following procedures on the provisioning server:

- Create a phone configuration file, or update an existing file, to enable the feature's settings.
- Create a user configuration file—called `<user>.cfg`—that specifies the user's password and registration, and other user-specific settings that you want to define for the user.



You can quickly reset the user's password by removing the password parameter from the override file. This will cause the phone to use the default password in the `<user>.cfg` file.

After you complete these steps, update the phone's configuration to effect your changes. The User Profile feature will be ready to use.

For detailed information on configuration parameters, see [<prov/>](#) on page 97.

Creating a Phone Configuration File

You can create a phone configuration file for the User Login feature, and then add and set the attributes for the feature. Or, if you already have a phone configuration file, you can update the file to include the User Login parameters you want to change.



Polycom recommends that you create a single default user password for all users. This password is encrypted in the configuration file.

To define the feature's settings:

- 1 Create a **site.cfg** file for the phone and place it on the provisioning server.
You can base this file on the sample configuration template that is in your software package. To find the file, navigate to **<provisioning server location>/config templates/site.cfg**.
- 2 In **site.cfg**, open the **<prov.login/>** attribute, and then add and set values for the user login attributes.

Creating a User Configuration File

Create a configuration file for each user that you want to be able to log in to the phone. The name of the file will specify the user's login ID. In the file, specify any user-specific settings that you want to define for the user.



To convert a phone-based deployment to a user-based deployment, copy the **phone[PHONE_MAC_ADDRESS].cfg** file to **<user>.cfg** and **[MACADDRESS]-phone.cfg** to **<user>-phone.cfg**.

To create a user configuration file:

- 1 On the provisioning server, create a user configuration file for each user that will be able to log in to the phone. The name of the file will be the user's ID to log in to the phone. For example, if the user's login ID is **user100**, the name of the user's configuration file is **user100.cfg**.
- 2 In each **<user>.cfg** file, add and set values for the user's login password.
- 3 Add and set values for any user-specific parameters, such as:
 - Registration details (for example, number of lines the profile will display and line labels).
 - Feature settings (for example, Browser settings).



If you add optional user-specific parameters to **<user>.cfg**, add only those parameters that will not cause the phone to restart or reboot when the parameter is updated. For information on which parameters cause the phone to restart or reboot, see [Configuration Parameters](#) on page 62.



If a user updates their password or other user-specific settings using the Main Menu on the phone, the updates will be stored in **<user>-phone.cfg**, not **<MACaddress>-phone.cfg**.

If a user updates their Contact Directory while logged in to a phone, the updates will be stored in **<user>-directory.xml**. Directory updates will be displayed each time the user logs in to a phone.

For certain phones (for example, the VVX 1500 phone), an up-to-date call lists history will be defined in **<user>-calls.xml**. This list will be retained each time the user logs in to a certain phone.

Configuration parameter precedence (from first to last) for a phone that has the User Profile feature enabled is:

- **<user>-phone.cfg**
- **<user>.cfg**
- Web Configuration Utility (through a browser)
- Polycom CMA system
- Configuration files listed in the master configuration file
- Default values

Setting Up Advanced Features

This section shows you how to make configuration changes for the following advanced features:

- [Barcode Scanner Support](#)
- [Browser and Applications](#)
- [Open Application Interface](#)
- [Instant Messaging and Presence](#)
- [Location Service](#)
- [Calendaring](#)

Barcode Scanner Support

SpectraLink 8450 handsets have a built-in barcode scanner. The user can send barcode scans to a computer running the Polycom Quick Barcode Connector application. Two Quick Barcode Connector modes are available:

- Single endpoint mode

- Multiple endpoint mode

In single endpoint mode, the computer's IP address is stored in the handset's configuration parameters. When the handset is not connected to the computer, it will attempt to connect. Failure to connect will result in a re-attempt after a configurable timeout period (default is 60 seconds).

In multiple endpoint mode, the handset connects to a computer by identifying a barcode generated by the Quick Barcode Connector program. The barcode data must contain a host name or an IP address. Failure to connect will result in a re-attempt after a configurable timeout period (default is 10 seconds).

By default, all data passed to the computer is encrypted using AES-128.

For instructions on how to install and configure the Quick Barcode Connector application, see the *Quick Barcode Connector Installation Guide* at <http://support.polycom.com/support/spectralink8400>.

For detailed information on configuration parameters, see <qbc/> on page 99.

Browser and Applications

You can configure SpectraLink 8400 Series Handsets so that users can access custom browser applications by selecting **Applications** on the Home screen.

By using the Polycom XML API Application, you can control the handset's telephone notification events, state polling events, and push server controls. For more information on the application integration capabilities of the SpectraLink 8400 Series Handsets, see the *Web Application Developer's Guide Polycom Phones Running Polycom UC Software* at <http://support.polycom.com/support/spectralink8400>.

For detailed information on configuration parameters, see <mb/> on page 73 and <apps/> on page 64.

Open Application Interface

SpectraLink 8400 Series Handsets support the Open Application Interface (OAI) 2.2. For more information, see the SpectraLink 8000 Open Applications Interface (OAI) Gateway Administration Guide, which is available at http://support.polycom.com/support/spectralink8000_oai.

For detailed information on configuration parameters, see <oai/> on page 96.

Instant Messaging and Presence

You can use SpectraLink 8400 Series Handsets with Microsoft® Office Communication Server 2007 R2 to help improve efficiency, increase productivity, and to share ideas and information immediately with business contacts.

SpectraLink 8400 Series Handsets support sending and receiving instant text messages when integrated with Microsoft Office Communication Server 2007 R2. The user is alerted to incoming messages visually and audibly. The user can view the messages immediately or when it is convenient. To send messages, the user can either select a message from a preset list of short messages or type custom messages using an alphanumeric text entry mode on the dial pad. Users can initiate message sending by replying to an incoming message or by initiating a new dialog. The destination address for new dialog messages can be entered manually or selected from the contact directory, which is the preferred method.



Any contacts added through the handset's buddy list will appear as a contact in Microsoft Office Communication Server 2007 R2.

For detailed information on configuration parameters, see [<feature/>](#) on page 71, [<messaging/>](#) on page 73, [<reg/>](#) on page 100, [<roaming_buddies/>](#) on page 102, and [<roaming_privacy/>](#) on page 102.

Location Service

You can set up location services to give users the option of sending reports for Ekahau Real-Time Location Systems (RTLS), selecting a transmit interval, or entering a static IP address for the Ekahau Positioning Engine (EPE). Location services capability is provided by the EPE 4.0 using Ekahau Location Protocol (ELP). See Ekahau's user documentation for more information (<http://www.ekahau.com/products/real-time-location-system/overview.html>).

For detailed information on configuration parameters, see [<wifi/>](#) on page 104.

Calendaring

The Calendaring feature enables users to view their Microsoft Exchange calendar on their handset in order to access meeting information and dial into a conference call with just one key press.

For detailed information on configuration parameters, see [<exchange/>](#) on page 71 and [<feature/>](#) on page 71.

Troubleshooting SpectraLink 8400 Series Handsets

This chapter contains general troubleshooting and diagnosis information to help you solve common issues you might encounter when using the Polycom® SpectraLink® 8400 Series Wireless Handsets in a wireless environment. The handset can provide feedback in the form of on-screen error messages, status indicators, and log files for troubleshooting issues.

For detailed information on error messages, log files, handset testing hardware, and handset issues – along with likely causes and corrective actions – see the Troubleshooting chapter of the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

This chapter explains handset issues, likely causes, and corrective actions for the SpectraLink 8400 Series Handsets in a wireless environment. Issues are grouped as follows:

- [Calling](#)
- [Display](#)
- [Upgrading](#)
- [Wi-Fi Diagnostics](#)
- [Run Site Survey](#)
- [Setting Up Syslog](#)
- [User Accessible Network Diagnostics](#)
- [Access Point Issues](#)

Review the latest *Release Notes* for the Polycom UC Software 4.0.0 for known issues and available workarounds.

Calling

Symptom	Problem	Corrective Action
The line icon shows an unregistered line icon.	The line is unregistered.	<ul style="list-style-type: none"> Verify that the appropriate configuration parameters are set correctly. Verify that the call server is functioning correctly.

Display

Symptom	Problem	Corrective Action
The time and date are not displayed.	You have disconnected the handset from the WLAN or there is no SNTP server configured.	<p>Do one of the following:</p> <ul style="list-style-type: none"> Reconnect the handset to the WLAN. Disable the time and date display on the handset: <ol style="list-style-type: none"> Select Settings > Basic Settings > Preferences > Time & Date. The Time & Date screen displays. Scroll to Disable, and then press the Ok key. Press the Home key. The Home Screen no longer displays the time and date.

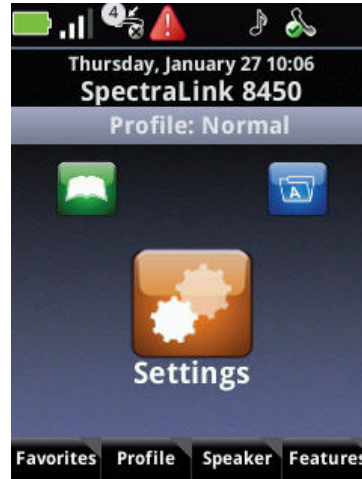
Upgrading

Symptom	Problem	Corrective Action
The handset does not upgrade from the provisioning server.	The provisioning server is offline or the handset is disconnected from the WLAN.	<ul style="list-style-type: none"> Verify that the provisioning server address is correct on the handset and in the configuration files. Verify that the Polycom UC Software is available on the provisioning server. Verify that the configuration files are available from the provisioning server. Verify that WLAN parameters in the configuration files are correct.

Wi-Fi Diagnostics

The Wi-Fi diagnostics feature enables you to gauge the overall health of the SpectraLink 8400 Series Handsets in relation to the rest of the system, particularly the Access Points (APs).

Select the **Settings** icon on the Home Screen. Select **Status > Diagnostics > Wi-Fi Stats**.



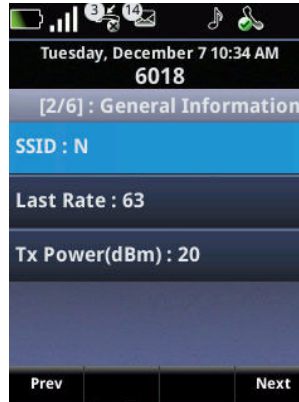
You can scroll forward or backward through these screens using the **Prev** and **Next** soft keys.

The six Wi-Fi Diagnostic screen selections are as follows:

- Screen 1 (Packet Count):
 - Line 1: Missed receive packet count since power on
 - Line 2: Missed transmit packet count since power on
 - Line 3: Receive retry count since power on
 - Line 4: Transmit retry count since power on



- Screen 2 (General Information)
 - Line 1: Service set identifier (SSID) of the current AP
 - Line 2: Last successful transmit data rate
 - Line 3: Transmit power (in dBm)



- Screen 3 (AP List)
 - Line 1: Currently associated AP

The format of this line is as follows: mmmmch-ssaid
where:

 - mmmm – Last 2 bytes of the AP's MAC address
 - ch – Channel number
 - ss – Signal Strength

- Other lines: Other local APs

The format of each line is as follows: mmmmch-ssmnm

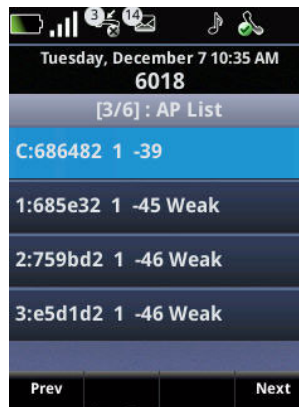
where:

mmmm – Last 2 bytes of the AP’s MAC address

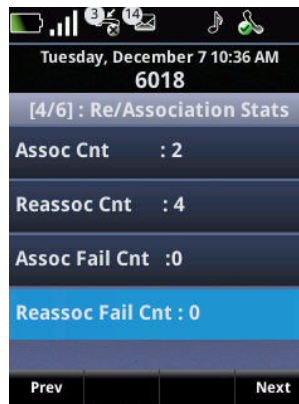
ch – Channel number

ss – Signal Strength

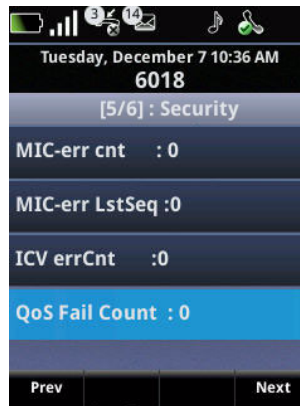
mnm – Mnemonic for the reason code as to why the handset did not hand off to this AP (For the list of mnemonic reason codes, see [Mnemonic Reason Codes](#) on page 4-54.)



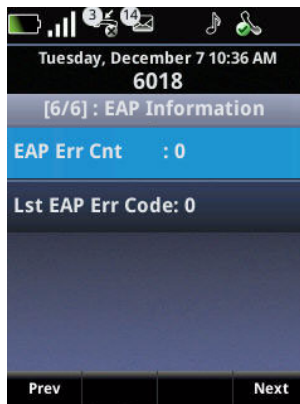
- Screen 4 (Association Count/Failure)
 - Line 1: Association count since power on
 - Line 2: Reassociation count since power on
 - Line 3: Association failures since power on
 - Line 4: Reassociation failures since power on



- Screen 5 (Security)
 - Line 1: Count of Message Authentication Code (MIC) Failures since power on
 - Line 2: MAC sequence number of packet causing last MIC error/failure
 - Line 3: Count of Integrity Check Value (ICV) errors since power on
 - Line 4: Count of Traffic Specification (TSPEC) rejections since power on



- Screen 6 (Extensible Authentication Protocol (EAP) Information)
 - Line 1: EAP error count since power on
 - Line 2: Last generated EAP error code



Mnemonic Reason Codes

The following mnemonic reason codes display on the **AP Lists** (third screen) of the **Wi-Fi Diagnostics**:

- **Unkn**: Reason unknown
- **Weak**: Signal strength too weak or weaker than better candidates

- **Rate:** One or more basic rates are not supported
- **Full:** The AP cannot handle the bandwidth requirements
- **AthT:** Authentication timeout
- **AscT:** Association timeout
- **AthF:** Authentication failure
- **AscF:** Association failure
- **SecT:** Security handshake timeout
- **SecF:** Security handshake failure
- **Cnfg:** The AP is not configured correctly for security, QOS, or infrastructure network

Run Site Survey

Run Site Survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area for all APs regardless of the Service Set Identifier (SSID). The AP information available through the site survey includes:

- SSID
- Beacon Interval
- AP information regarding support of 802.11d, 802.11h, and other 802.11 amendment standards as required
- Current security configuration

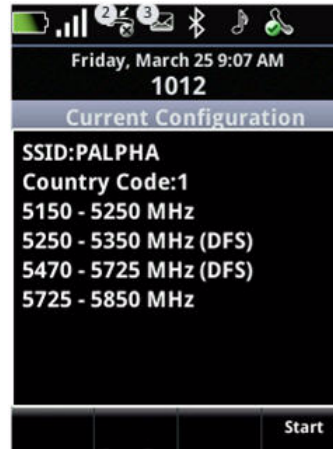
From the Home Screen, select **Settings**, and then select **Advanced Settings > Administration Settings > Diagnostics > Run Site Survey**.

The Site Survey uses the user-configured bands/sub-bands for its scanning. If the site survey is not able to understand which bands are allowed for the scanning, it will not proceed and the error message **Cannot run site survey with current configuration** displays.

The Site Survey will not start if:

- The Wi-Fi is disabled.
- The regulatory domain is not set.
- The 5z GHz and 2.4 GHz bands are both disabled.

A summary of the current Wireless Local Area Network (WLAN) configuration displays.



On this screen:

- Line 1: SSID set by user
- Line 2: Regulatory domain
- Line 3: 2.4-GHz band channels, if enabled. Channel range is displayed in parentheses ().
- Lines 4 to 7: 5-GHz band channels, if enabled. If a particular band is a Dynamic Frequency Selection (DFS) channel, **(DFS)** is displayed.



- 1 Lines 3 to 7 display the channels that are scanned for the site survey. The channels/band(s) not displayed here will not be scanned.
- 2 If 2.4 GHz is not enabled and 5 GHz band is enabled, 5 GHz occupies lines 3 to 6.

To start the site survey, press the **Start** soft key.

There are two modes of display: Summary and Detail. These modes can be selected using selecting either the **Summary** or **Detail** soft key.

- Summary Mode displays the list of APs as discussed next:

Each AP entry is displayed in the format:

line 1: [AP index]: BSSID:SNR:RSSI

line 2: channel:SSID

where:

AP index: The index of the AP in the list, sorted on the basis of signal strength

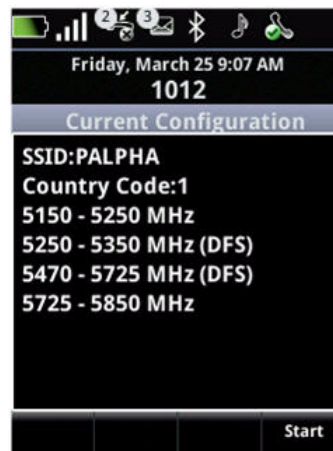
BSSID: bssid of the AP

SNR: Signal to noise ratio of the AP (not considered for selection of an AP and is shown as 0)

RSSI: Signal strength in dBm

Channel: Channel of operation for the AP

SSID: ssid being advertised by the AP



- Detail Mode shows details of each AP:

line 1: [AP index]: BSSID:SNR:RSSI

line 2: Channel:SSID

line 3: Security_type:CCX-info

line 4: WMM-info

line 5: Rates-info // "+" indicating there is more which cannot be displayed

line 6: Beacon-DTIM:ieee802.11-standard-supported// "+" indicating there is more which cannot be displayed



DTIM is the abbreviation for Delivery Traffic Indication Message. This parameter value indicates the time interval in terms of no beacons at which the AP releases multicast and broadcast packets to associated clients and associated clients have to be awoken to receive all of these multicast and broadcast packets.

line 7: Capability_info: special capability like spectrum management (SM*)

* SM=spectrum management enabled, SP=short preamble, ST=short timeslot, PR=privacy bit enabled, CA=channel agility

Site survey display is updated (typically every one second) with the refreshed AP List. It can become difficult to read the details of the scanned APs, if the update appears too frequently (especially in All mode). You have the option of freezing the display by pressing the **Freeze** soft key. When enabled, the **Freeze** soft key will not update the AP list until the Update is again activated. To activate the Update, press the **Update** soft key.

Setting Up Syslog

For more information on setting up syslog, see *Quick Tip 17124: Using Syslog for Logging of Complete SIP Messaging on Polycom® Phones* at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html.

User Accessible Network Diagnostics

You can access the Ping and TraceRoute network diagnostic features through the handset's menu.

From the Home Screen, select **Settings**, and then select **Status > Diagnostics > Network**.

Access Point Issues

Most, but not all, handset audio issues are associated with AP range, positioning, and capacity. Performing a site survey as described in [Run Site Survey](#) on page 4-55 can isolate the AP causing these types of issues. If the handset itself is suspected, conduct a parallel site survey with a handset that is known to be properly functioning.

In Range/Out-of-Range

Service will be disrupted if a user moves outside the area covered by the WLAN APs. Service is restored if the user moves back within range. If a call drops because a user moves out of range, the handset will recover the call if the user moves back into range within a few seconds.

Capacity

In areas of heavy use, the call capacity of a particular AP may be full. If this happens, the user will hear three chirps from the handset. The user can wait until another user terminates a call, or the user can move within range of another AP and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another AP. Due to range limitations, this may be the same as moving out of range.

Transmission Obstructions

Prior to system installation, you should determine locations for optimal AP transmission coverage. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after system installation. This loss of service can be restored by moving out of the obstructed area or by adding/rearranging APs.

Configuration Files

This appendix provides detailed descriptions of certain configuration files used by the Polycom® UC Software running on the Polycom® SpectraLink® 8400 Series Wireless Handsets.

This appendix contains information on:

- [Master Configuration File \(MACaddress.cfg or 000000000000.cfg\)](#)
- [Configuration Parameters](#)

The configuration parameters dictate the behavior of the handset once it is running the executable file specified in the master configuration file.

For detailed information—including permitted values, default values, and a brief description—on the complete set of configuration parameters available to you in the configuration files, see the ‘Configuration Files’ appendix of the latest *Polycom UC Software Administrator’s Guide* available at <http://support.polycom.com/support/spectralink8400>.



You can also make changes to the configuration files through the web interface of the phone. Using a Web browser, enter the phone’s IP address into the browser’s address bar. For more information, refer to [Using the Web Configuration Utility](#) on page B-106.

Changes made through the Web interface are written to the override file. These changes remain active until you reset to the default configuration files. To reset to the default configuration files, go to **Settings > Advanced Settings > Administrative Settings > Reset to Defaults > Reset Web Configuration**.

Master Configuration File

Master configuration files contain the following XML parameters:

- APP_FILE_PATH
- CONFIG_FILES
- MISC_FILES
- LOG_FILE_DIRECTORY

- CONTACTS_DIRECTORY
- OVERRIDES_DIRECTORY
- LICENSE_DIRECTORY
- USER_PROFILES_DIRECTORY
- CALL_LISTS_DIRECTORY

For example:

```

xml
#comment
#comment
#comment
#comment
#comment
APPLICATION
  APP_FILE_PATH
  CONFIG_FILES
  MISC_FILES
  LOG_FILE_DIRECTORY
  OVERRIDES_DIRECTORY
  CONTACTS_DIRECTORY
  LICENSE_DIRECTORY
  USER_PROFILES_DIRECTORY
  CALL_LISTS_DIRECTORY
  APPLICATION_SPIP300
  APPLICATION_SPIP500
  APPLICATION_SPIP301
  APPLICATION_SPIP302

version="1.0" standalone="yes"
Default Master SIP Configuration File
For information on configuring Polycom VoIP phones please refer to the
Configuration File Management white paper available from:
http://www.polycom.com/common/documents/whitepapers/configuration_file
$RCSfile: 000000000000.cfg,v $ $Revision: 1.30 $

sip.ld
phone[PHONE_MAC_ADDRESS].cfg
    
```

Configuration Parameters



A number of sample template files are included with the UC Software 4.0.0 release. The following templates may assist you in creating your own configuration files:

- **reg-basic.cfg**
- **reg-advanced.cfg**
- **sip-basic.cfg**
- **sip-interop.cfg**
- **wireless.cfg**
- **device.cfg**
- **features.cfg**
- **applications.cfg**
- **site.cfg**

For more information, refer to 'Sample Template Files' in the 'Configuration Files' appendix of the latest *Polycom UC Software Administrator's Guide* at <http://support.polycom.com/support/spectralink8400>.

The important parameters for the SpectraLink 8400 Series Handsets include:

- `<apps/>` – Define the list of applications that display when **Applications** is selected on the Home screen.
- `<bluetooth/>` – Set the parameters that support the use of Bluetooth headsets.
- `<device/>` – Set the following parameters:
 - Power Settings
 - USB Net
 - WLAN Configuration Parameters
- `<exchange/>` – Set the connection parameters for the Microsoft Exchange application.
- `<feature/>` – Enable the following features at run time:
 - Calendaring
 - Instant messaging
 - Presence
- `<keypadLock/>` – Enable the keypad lock feature.
- `<log/>` – Set basic logging levels.
- `<mb/>` – Set the Application browser home page, a proxy to use, and size limits.
- `<messaging/>` – Set quick notes for instant messaging and inactivity timeout period.
- `<np/>` – Set notifications for different events like incoming calls or placing the handset in the Speakerphone Dock.
- `<oai/>` – Set the connection parameters for the Open Application Interface.
- `<prov/>` – Set user profiles.
- `<ptt/>` – Set Push-to-Talk parameters.
- `<qbc/>` – Set the connection parameters for the Quick Barcode Connector application.
- `<reg/>` – Set the registration protocol for calls and instant messaging.
- `<roaming_buddies/>` – Set the registration that enables roaming buddy support.
- `<roaming_privacy/>` – Set the registration that enables roaming privacy support.
- `<up/>` – Set user preferences.
- `<voIpProt/>` – Set call server and DTMF signaling parameters.
- `<wifi/>` – Set miscellaneous wireless parameters.

<apps/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
apps.x.label	String	Null	The descriptive text that appears in the Applications menu. x=1 to 12.
apps.x.url	URL	Null	The URL of an application. x=1 to 12.

For more information, see the **applications.cfg** template.

<bluetooth/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
bluetooth.radioOn	0 or 1	0	A flag to determine whether or not Bluetooth radio is enabled by default.

For more information, see the **features.cfg** template.

<device/>

The <device/> parameters – also known as flash parameters – can be used to initialize multiple phones and remove the need for manual interaction with the handsets to configure basic settings.

The global `device.set` parameter must be enabled to use any <device/> parameters. Two device parameters exist for every configuration parameter – `device.xxx` and `device.xxx.set`. For example, you must include both `device.wifi.dhcpEnabled` and `device.wifi.dhcpEnabled.set`.

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.pacfile.data	String	Null	The PAC file (base64 encoded).
device.pacfile.password	String	Null	The password protecting the PAC file.
device.sec.TLS.profile. caCertList1	Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2	Null	The supported values are: <ul style="list-style-type: none"> • Use only built-in default certificates • Use default and Custom Certificate #1 • Use default and Custom Certificate #2 • Use any certificate (built-in or either custom cert) • Use only Custom Certificate #1 • Use only Custom Certificate #2 • Use either Custom Certificate #1 or Custom Certificate #2
device.sec.TLS.profile. caCertList2	Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2	Null	Same as device.sec.TLS.profile.caCertList1.
device.sec.TLS.profile .cipherSuite1	string	Null	The cipher suite for platform profile 1.
device.sec.TLS.profile .cipherSuite2	string	Null	The cipher suite for platform profile 2.
device.sec.TLS.profile .cipherSuiteDefault1	0 or 1	Null	A flag to determine whether or not to use the default cipher suite for the platform profile 1. If set to 1, use the default cipher suite. If set to 0, use the custom cipher suite.
device.sec.TLS.profile .cipherSuiteDefault2	0 or 1	Null	A flag to determine whether or not to use the default cipher suite for the platform profile 2. If set to 1, use the default cipher suite. If set to 0, use the custom cipher suite.
device.sec.TLS .customCaCert1	String	Null	The custom certificate that depends on the value of device.sec.TLS.profile.caCertList1.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.sec.TLS. customCaCert2	String	Null	The custom certificate that depends on the value of device.sec.TLS.profile.caCertificate2.
device.sec.TLS.profile. deviceCert1	Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2	Null	The supported values are: <ul style="list-style-type: none"> • Use only built-in default certificates • Use default and Custom Certificate #1 • Use default and Custom Certificate #2 • Use any certificate (built-in or either custom cert) • Use only Custom Certificate #1 • Use only Custom Certificate #2 • Use either Custom Certificate #1 or Custom Certificate #2
device.sec.TLS.profile. deviceCert2	Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2	Null	Same as device.sec.TLS.profile.deviceCertificate1.
device.sec.TLS. profileSelection.dot1x	PlatformProfile1, PlatformProfile2	Null	The profile to use for 802.1X authentication.
device.sec.TLS. profileSelection. provisioning	PlatformProfile1, PlatformProfile2	Null	The profile to use for provisioning.
device.sec.TLS. profileSelection.syslog	PlatformProfile1, PlatformProfile2	Null	The profile to use for syslog.
device.usbnet. IPgateway	String	169.254.1 .1	The provisioning server IP address.
device.usbnet. subnetMask	String	255.255.0 .0	The handset's subnet mask.
device.usbnet. dhcpServerEnabled	0 or 1	Null	A flag to determine whether or not DHCP servers enabled on the USBNet interface.
device.usbnet.enabled	0 or 1	1	A flag to determine whether or not USBNet is supported.
device.usbnet. ipAddress	String	169.254.1 .2	The handset's IP address on the USBNet interface.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.wifi. ccxMandatory	0 or 1	0	If set to 0, the SpectraLink handsets will connect to access points (APs) that do not advertise Cisco Compatible Extensions (CCX v4) or higher. If set to 1, the handsets will not connect to APs that do not advertise CCX v4 or higher (CCX is mandatory).
device.wifi.dhcpEnabled	0 or 1	1	Enables DHCP on the wireless interface.
device.wifi.dot11n. enabled	0 or 1	0	A flag to determine whether or not 802.11n support is enabled.
device.wifi.enabled	0 or 1	0	Enables the wireless interface.
device.wifi.ipAddress	String	0.0.0.0	The IP address of the wireless interface (if not using DHCP).
device.wifi.ipGateway	String	0.0.0.0	The IP gateway address for the wireless interface (if not using DHCP).
device.wifi.psk.key	String	0xFF	Depending on the value of <code>device.wifi.psk.keyType</code> , the value is: <ul style="list-style-type: none"> • A string of 8 to 63 ASCII characters • A 256-bit hexadecimal key
device.wifi.psk.keyType	Key or Passphrase	Key	A flag to determine whether or not the information stored in <code>device.wifi.psk.key</code> is a passphrase or a key.
device.wifi.qos. acMandatory	String	Null	A flag to determine whether or not the handset will connect only to APs that enforce access control.
device.wifi.radio. regulatoryDomain	1, 2, 10	Null	The regulatory domain. The supported values are: <ul style="list-style-type: none"> • 1 = North America • 2 = Europe • 10 = Australia

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.wifi.radio.band. band5GHz.subBand1 .enable	0 or 1	0	A flag to determine whether or not the 5 GHz wireless sub-band 1 is enabled. Note: <i>The regulatory authorities (FCC North America) further subdivide the 5 GHz band into multiple sub-bands (not all of which are available in all countries). You can enable and disable individual sub-bands and set the maximum transmit power for each. For maximum performance, you should enable only the same bands and sub-bands as configured on your wireless infrastructure, otherwise SpectraLink 8400 Series Handsets will waste time looking for a signal on the unused sub-bands.</i>
device.wifi.radio.band. band5GHz.subBand1. txPower	1 to 7	5	The maximum power that the handset will use to transmit in that band. In general, this power should match the power setting at the access point so that the coverage radius of the phone matches that of the access point. For detailed guidance, see the <i>Best Practices Guide to Network Design Considerations for SpectraLink 8400 and 8000 Series Wireless Telephones</i> at http://support.polycom.com/support/spectrallink8400 .
device.wifi.radio.band. band5GHz.subBand2 .enable	0 or 1	0	A flag to determine whether or not the 5 GHz wireless sub-band 2 is enabled.
device.wifi.radio.band. band5GHz.subBand2. txPower	1 to 7	5	The maximum power that the handset will use to transmit in that band. In general, this power should match the power setting at the access point so that the coverage radius of the phone matches that of the access point.
device.wifi.radio.band. band5GHz.subBand3 .enable	0 or 1	0	A flag to determine whether or not the 5 GHz wireless sub-band 3 is enabled.
device.wifi.radio.band. band5GHz.subBand3. txPower	1 to 7	5	The maximum power that the handset will use to transmit in that band. In general, this power should match the power setting at the access point so that the coverage radius of the phone matches that of the access point.
device.wifi.radio.band. band5GHz.subBand4 .enable	0 or 1	0	A flag to determine whether or not the 5 GHz wireless sub-band 4 is enabled.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.wifi.radio.band. band5GHz.subBand4. txPower	1 to 7	5	The maximum power that the handset will use to transmit in that band. In general, this power should match the power setting at the access point so that the coverage radius of the phone matches that of the access point.
device.wifi.radio.band. band5GHzEnable	0 or 1	0	A flag to determine whether or not the 5 GHz wireless band is enabled. Note: Enable the individual sub-band and transmit power for those sub-bands below.
device.wifi.radio.band.b and2_4GHzEnable	0 or 1	0	A flag to determine whether or not the 2.4 GHz wireless band is enabled.
device.wifi.radio.band2_ 4GHz.txPower	1 to 7	5	The maximum power that the handset will use to transmit in that band. In general, this power should match the power setting at the access point so that the coverage radius of the phone matches that of the access point. For detailed guidance, see the <i>Best Practices Guide for Deploying SpectraLink 8400 Series Wireless Telephones</i> at http://support.polycom.com/support/spectralink8400 .
device.wifi.securityMode	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise	0	The wireless security mode.
device.wifi.ssid	String	SSID1	The Service Set Identifier (SSID) of the wireless network.
device.wifi.subnetMask	String	255.0.0.0	The network mask address of the wireless interface (if not using DHCP).
device.wifi.wep. authType	0 or 1	0	The supported authentication methods are: <ul style="list-style-type: none"> The value 0 = Open. The values 1 = Shared.
device.wifi.wep. defaultKey	1 to 4	1	Specifies which key from device.wifi.wep.key1 to device.wifi.wep.key4 is used.
device.wifi.wep. encryptionEnable	0 or 1	1	A flag to determine whether or not WEP encryption is enabled.
device.wifi.wep. keyLength	0 or 1	0	The supported values are: <ul style="list-style-type: none"> 0 = 40 bits (default) 1 = 104 bits

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.wifi.wep.key1	String	0xFF	The hexadecimal key where the length is determined by <code>device.wifi.wep.keyLength..</code>
device.wifi.wep.key2	String	0xFF	The hexadecimal key where the length is determined by <code>device.wifi.wep.keyLength..</code>
device.wifi.wep.key3	String	0xFF	The hexadecimal key where the length is determined by <code>device.wifi.wep.keyLength..</code>
device.wifi.wep.key4	String	0xFF	The hexadecimal key where the length is determined by <code>device.wifi.wep.keyLength..</code>
device.wifi.wpa2Ent. eapFast.inBandProv	0 or 1	0	The PAC file can be loaded into the handset during configuration (called 'out-of-band') or automatically loaded from the network (called 'in-band').
device.wifi.wpa2Ent. method	EAP-PEAPv0-MSCHA Pv2, EAP-FAST	Null	The EAP type to use for authentication.
device.wifi.wpa2Ent. password	String	PlcmSplp	The WPA2-Enterprise password.
device.wifi.wpa2Ent. roaming	OKC, CCKM	0	The fast roaming method.
device.wifi.wpa2Ent. user	String	PlcmSplp	The WPA2-Enterprise user name.

For more information, see the **device.cfg** and **wireless.cfg** templates.

<exchange/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
exchange.meeting. phonePattern	String	Null	The pattern used to identify phone numbers in meeting descriptions, where "x" denotes any digit and " " separates alternative patterns (for example, "xxx-xxx-xxxx 604.xxx.xxxx").
exchange.meeting. reminderEnabled	0 or 1	1	A flag to determine whether or not to enable the meeting reminders.
exchange.server.url	String	Null	The Microsoft Exchange server IP address.

For more information, see the **features.cfg** template.

<feature/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
feature.bluetooth. enabled	0 or 1	1	The Bluetooth headset feature. Note: This feature is only supported on SpectraLink 8400 Series Handsets.
feature. exchangeCalendar. enabled	0 or 1	0	The calendaring feature.
feature.messaging. enabled	0 or 1	0	The instant messaging feature.
feature.presence. enabled	0 or 1	0	The presence feature, including management of buddies and your own status.

For more information, see the **features.cfg** template.

<keypadLock/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
keypadLock.enabled	0 or 1	1	A flag to determine whether or not the keypad lock feature is enabled.
keypadLock .idleTimeout	0 to 65535	0	The maximum time the handset can be idle before the keypad locks.

For more information, see the **features.cfg** template.

<log/>

By default, the logging detail level for the individual components are set to four (Minor error - graceful recovery). The following components will be of interest:

- `log.level.change.barcd`
- `log.level.change.bluetooth`
- `log.level.change.dot1x`
- `log.level.change.nwmgr`
- `log.level.change.oaip`
- `log.level.change.ptt`
- `log.level.change.usbio`
- `log.level.change.wlan`
- `log.level.change.wmgr`

The permitted values are:

- 0—Debug only
- 1—High detail event class
- 2—Moderate detail event class
- 3—Low detail event class
- 4—Minor error-graceful recovery
- 5—Major error-will eventually stop the software
- 6—Fatal error

<mb/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
mb.main.idleTimeout	0 to 600, seconds	40	Timeout for the interactive browser. If the interactive browser remains idle for a defined period of time, the phone should return to the idle browser. If set to 0, there is no timeout and the phone will remain in the browser until the user closes the browser. If set to a value greater than 0 and less than 600, the timeout is for that number of seconds.
mb.main.toolbar. autoHide.enabled	0 or 1	0	A flag to determine whether or not to hide the browser tool bar.

For more information, see the **applications.cfg** template.

<messaging/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
messaging. maxImMessages	10 to 1000	1000	The maximum number of instant messages.
messaging.quicknotes.x	String of up to 128 characters	Null	Quick note text for use in instant messages (x=1 to 10)

For more information, see the **features.cfg** template.

<np/>

There are currently four notification profiles. Each notification profile defines alerting and ringing parameters. There are 15 alert types and three ringing types. Each alert type and ringing type has a tone pattern and a vibration flag.

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.selected	Normal, Silent, Meeting, Custom1	Normal	The initial profile selected at power on and active during operation. The selected profile can be overridden by the user and that value will be used when the handset powers on the next time.
Normal Profile Type			
np.normal.label	String	Normal	The name of the profile type.
np.normal.alert. barcodeBeep. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc2	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. barcodeBeep. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. docked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	postiveC onfirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. docked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. undocked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.normal.alert. undocked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. instantMessaging. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	instantMessage	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. instantMessaging. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. localHoldNotification. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	localHoldNotification	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. localHoldNotification. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. lossOfNetwork. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. lossOfNetwork. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.normal.alert. lowBattery.tonePattern	custom1 to custom10 , instantMessaging , localHoldNotification , messageWaiting , misc1 to misc9 , negativeConfirm , positiveConfirm , remoteHoldNotification , silent , welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i>
np.normal.alert. lowBattery.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. veryLowBattery. tonePattern	custom1 to custom10 , instantMessaging , localHoldNotification , messageWaiting , misc1 to misc9 , negativeConfirm , positiveConfirm , remoteHoldNotification , silent , welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. veryLowBattery. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. messageWaiting. tonePattern	custom1 to custom10 , instantMessaging , localHoldNotification , messageWaiting , misc1 to misc9 , negativeConfirm , positiveConfirm , remoteHoldNotification , silent , welcome	messageWaiting	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. messageWaiting. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.normal.alert. negativeConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. negativeConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. positiveConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	positive Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. positiveConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. pttTransmit.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	misc3	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. pttTransmit.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.normal.alert. pttWait.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc4	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. pttWait.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.alert. welcome.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	welcome	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.alert. welcome.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.ringing.calls. tonePattern	default, ringer1 to ringer24, 1 to 22	ringers2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.ringing. calls.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.ringing.oai1. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.normal.ringing. oai1.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.ringing.oai2. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.normal.ringing. oai2.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.normal.ringing. toneVolume.handset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Handset and Normal profile is active.
np.normal.ringing. toneVolume.headset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Headset and Normal profile is active.
np.normal.ringing. toneVolume.chassis	-1000 to 1000	0	The attribute is set (on adjusting ring volume) when ringing termination is Chassis and Normal profile is active.
np.normal.ringing. toneVolume.dock	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when phone is at the speakerphone dock and Normal profile is active.
np.normal.ringing. toneVolume. bluetoothHeadset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Bluetooth Headset and Normal profile is active.
np.normal.ringing. toneVolume.reserved	-1000 to 1000	-21	Not used.
Silent Profile Type			
np.silent.label	String	Silent	The name of the profile type.
np.silent.alert. barcodeBeep. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in <code>se.pat.misc</code> . For a definition of the <code><se/></code> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. barcodeBeep. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.alert. docked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. docked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. undocked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. undocked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. instantMessaging. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. instantMessaging. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.alert. localHoldNotification. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. localHoldNotification. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. lossOfNetwork. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. lossOfNetwork. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. lowBattery.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. lowBattery.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.alert. veryLowBattery. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. veryLowBattery. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. messageWaiting. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. messageWaiting. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. negativeConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. negativeConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.alert. positiveConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. positiveConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. pttTransmit.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. pttTransmit.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.alert. pttWait.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. pttWait.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.alert. welcome.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	silent	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.alert. welcome.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.ringing.calls. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.ringing. calls.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.ringing.oai1. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.ringing. oai1.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.ringing.oai2. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.silent.ringing. oai2.vibration	off, continuous, shortPulse, longPulse	off	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.silent.ringing. toneVolume.handset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Handset and Silent profile is active.
np.silent.ringing. toneVolume.headset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Headset and Silent profile is active.
np.silent.ringing. toneVolume.chassis	-1000 to 1000	0	The attribute is set (on adjusting ring volume) when ringing termination is Chassis and Silent profile is active.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.silent.ringing. toneVolume.dock	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when phone is at the speakerphone dock and Silent profile is active.
np.silent.ringing. toneVolume. bluetoothHeadset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Bluetooth Headset and Silent profile is active.
np.silent.ringing. toneVolume.reserved	-1000 to 1000	-21	Not used.
Meeting Profile Type			
np.meeting.label	String	Meeting	The name of the profile type.
np.meeting.alert. barcodeBeep. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc2	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. barcodeBeep. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. docked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	positive Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. docked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.meeting.alert. undocked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. undocked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. instantMessaging. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	instantM essage	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. instantMessaging. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. localHoldNotification. tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	localHol dNotifica tion	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. localHoldNotification. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.meeting.alert. lossOfNetwork. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. lossOfNetwork. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. lowBattery.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. lowBattery.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. veryLowBattery. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. veryLowBattery. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.meeting.alert. messageWaiting. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	message Waiting	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. messageWaiting. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. negativeConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. negativeConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. positiveConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	positive Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. positiveConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.meeting.alert. pttTransmit.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	misc3	A pointer to the pattern in <code>se.pat.misc</code> . For a definition of the <code><se/></code> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. pttTransmit.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. pttWait.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	misc4	A pointer to the pattern in <code>se.pat.misc</code> . For a definition of the <code><se/></code> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. pttWait.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.alert. welcome.tonePattern	custom1 to custom10, instantMessaging, localHoldNotification, messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotification, silent, welcome	welcome	A pointer to the pattern in <code>se.pat.misc</code> . For a definition of the <code><se/></code> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.alert. welcome.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.ringing.calls. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in <code>se.pat.ringer</code> . For a definition of the <code><se/></code> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.ringing.calls.vibration	off, continuous, shortPulse, longPulse	continuous	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.meeting.ringing.oai1. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in se.pat.ringer . For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.ringing. oai1.vibration	off, continuous, shortPulse, longPulse	continuo us	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.ringing.oai2. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer1	A pointer to the pattern in se.pat.ringer . For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.meeting.ringing. oai2.vibration	off, continuous, shortPulse, longPulse	continuo us	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.meeting.ringing. toneVolume.handset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Handset and Meeting profile is active.
np.meeting.ringing. toneVolume.headset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Headset and Meeting profile is active.
np.meeting.ringing. toneVolume.chassis	-1000 to 1000	0	The attribute is set (on adjusting ring volume) when ringing termination is Chassis and Meeting profile is active.
np.meeting.ringing. toneVolume.dock	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when phone is at the speakerphone dock and Meeting profile is active.
np.meeting.ringing. toneVolume. bluetoothHeadset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Bluetooth Headset and Meeting profile is active.
np.meeting.ringing. toneVolume.reserved	-1000 to 1000	-21	Not used.
Custom 1 Profile Type			
np.custom1.label	String	Custom1	The name of the profile type.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.alert. barcodeBeep. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc2	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. barcodeBeep. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. docked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	positive Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. docked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. undocked.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. undocked.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.alert. instantMessaging. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	instantM essage	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. instantMessaging. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. localHoldNotification. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	localHol dNotifica tion	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. localHoldNotification. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. lossOfNetwork. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. lossOfNetwork. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.alert. lowBattery.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. lowBattery.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. veryLowBattery. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc1	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. veryLowBattery. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. messageWaiting. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	message Waiting	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. messageWaiting. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.alert. negativeConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	negative Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. negativeConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. positiveConfirm. tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	positive Confirm	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. positiveConfirm. vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. pttTransmit.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc3	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. pttTransmit.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.alert. pttWait.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	misc4	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. pttWait.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.alert. welcome.tonePattern	custom1 to custom10, instantMessaging, localHoldNotificatio n,messageWaiting, misc1 to misc9, negativeConfirm, positiveConfirm, remoteHoldNotificat ion, silent, welcome	welcome	A pointer to the pattern in se.pat.misc. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.alert. welcome.vibration	0 or 1	0	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.ringing.calls. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.ringing. calls.vibration	off, continuous, shortPulse, longPulse	continuo us	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.ringing.oai1. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .
np.custom1.ringing. oai1.vibration	off, continuous, shortPulse, longPulse	continuo us	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.ringing.oai2. tonePattern	default, ringer1 to ringer24, 1 to 22	ringer2	A pointer to the pattern in se.pat.ringer. For a definition of the <se/> parameter, see the latest <i>Polycom UC Software Administrator's Guide</i> .

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
np.custom1.ringing. oai2.vibration	off, continuous, shortPulse, longPulse	continuo us	A flag to determine whether or not the handset should vibrate when the alert occurs.
np.custom1.ringing. toneVolume.handset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Handset and Custom1 profile is active.
np.custom1.ringing. toneVolume.headset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Headset and Custom1 profile is active.
np.custom1.ringing. toneVolume.chassis	-1000 to 1000	0	The attribute is set (on adjusting ring volume) when ringing termination is Chassis and Custom1 profile is active.
np.custom1.ringing. toneVolume.dock	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when phone is at the speakerphone dock and Custom1 profile is active.
np.custom1.ringing. toneVolume. bluetoothHeadset	-1000 to 1000	-21	The attribute is set (on adjusting ring volume) when ringing termination is Bluetooth Headset and Custom1 profile is active.
np.custom1.ringing. toneVolume.reserved	-1000 to 1000	-21	Not used.

For more information, see the **wireless.cfg** template.

<oai/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
oai.gateway.address	String	Null	The address of the OAI server.
oai.userId	String of eight hexadecimal characters	Null	The lower four bytes of the six-byte OAI handset identifier in the OAI gateway. If the value is null or invalid, the handset identifies itself to the OAI gateway using the MAC address of the handset; otherwise, the upper two bytes are zero and the lower four bytes are as specified.

For more information, see the **applications.cfg** and **wireless.cfg** templates.

<prov/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
prov.login. automaticLogout	0 to 46000	0	The time (in minutes) before a non-default user is automatically logged out of the handset. If set to 0, the user is not logged out.
prov.login. defaultPassword	String	Null	The default password associated with the default user name.
prov.login.defaultOnly	0 or 1	0	A flag to determine whether or not a default user is the only user who can be logged in.
prov.login.defaultUser	String	Null	The default user name that, if present, is automatically sent to the provisioning server during the boot sequence and after a user logout.
prov.login.enabled	0 or 1	0	A flag to determine whether or not the user login feature is enabled.
prov.login.localPassword	String	123	The password used to validate the user login. It is stored either as plain text or encrypted (an MD5 hash).
prov.login.persistent	0 or 1	0	A flag to determine whether or not a user is remains logged in when the handset is rebooted.
prov.login.required	0 or 1	0	A flag to determine whether or not the user login is required when the feature is enabled.

For more information, see the **site.cfg** templates.



The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
ptt.address	Multicast IP address	224.0.1.1 16	The multicast IP address to send audio to and receive audio from.
ptt.allowOffHookPages	0 or 1	0	A flag to determine whether or not incoming PTT pages will play out on the handset while there is an active call. Note: This flag is ignored for Priority and Emergency pages.
ptt.callWaiting.enable	0 or 1	0	A flag to determine whether or not new incoming page sessions produce standard call waiting behavior on the active audio channel.
ptt.channel.x. allowTransmit	0 or 1	1	A flag to determine whether or not a channel x is available for sending outgoing pages. x=1 to 25
ptt.channel.x.available	0 or 1	1	A flag to determine whether a channel x is available for subscription. x=1 to 25
ptt.channel.x.label	String	x=1: All x=24: Priority x=25: Emergen cy others: Null	A label to use when announcing a page or within a page appearance to identify the channel in use. x=1 to 25
ptt.channel.x.subscribed	0 or 1	x=1: 1, x=24: 1, x=25: 1, others: 0	A flag to determine whether or not a channel x can be subscribed to if available. x=1 to 25
ptt.codec	G.711mu, G.726QI, G.722	G.722	The audio codec to use for outgoing pages. Incoming pages will be decoded according to the codec specified in the incoming message.
ptt.compatibilityMode	0 or 1	1	A flag to determine whether or not the PTT protocol will be compatible with older SpectraLink handsets.
ptt.defaultChannel	1 to 25	1	The default PTT channel. Used when the user does not specify a channel.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
ptt.displayName	String	Null	The strings displayed in the caller ID field of outgoing pages. If Null, the value from <code>reg.1.displayName</code> is used. If the value is also Null, the handset's MAC address is used.
ptt.emergencyChannel	1 to 25	25	The channel assigned for emergency pages.
ptt.emergencyChannel. volume	-32768 to 32767	-10	The gain in dB relative to the maximum handsfree Rx digital gain to set the handsfree Rx digital gain to during an incoming Emergency page. Note: When decreasing the volume on the handset, press the * key first.
ptt.payloadSize	10 to 80	20	The audio payload size in milliseconds.
ptt.port	0 to 65535	5001	The port to send audio to and receive audio from.
ptt.priorityChannel	1 to 25	24	The channel assigned for priority pages.
ptt.pttMode.enable	0 or 1	0	A flag to determine whether or not Push-to-Talk (PTT) is enabled.

For more information, see the `site.cfg` template.

<qbc/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qbc.connect. ipAddress.hostname	IP address or hostname	Null	The IP address or host name of the computer where the Quick Barcode Connector application is running. Used in 'single' endpoint mode only.
qbc.connect.passphrase	String	BcmaTest Password 1	The barcode scanner connector passphrase. This is supported only if <code>bcma.encryption.enabled</code> is set to 1.
qbc.connection.port	0 to 65535	14394	The Quick Barcode Connector application port number. Note: Do not change unless directed by Polycom Customer Support.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qbc.encryption.enabled	0 or 1	0	A flag to determine whether or not scanned data is encrypted.
qbc.inactivity.timeout	30000 to 300000	60000	The barcode scanner disconnect inactivity timeout period (in milliseconds).
qbc.keepalive.timeout	30000 to 120000	60000	The barcode scanner keep-alive message timeout period (in milliseconds). <i>Note: Do not change unless directed by Polycom Customer Support.</i>
qbc.operating.mode	disabled, single, multi	multi	The Quick Barcode Connector application operating mode.

For more information, see the **wireless.cfg** template.

<reg/>

SpectraLink 8400 Series Handsets support six registrations (x= 1 to 6 in the table shown below).

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.address	string in the format userPart from userPart@domain	Null	The user part or the user and the host part of the phone's SIP URI. For example: reg.x.address="1002" from 1002@polycom.com or reg.x.address="1002@polycom.com". x=1 to 6
reg.x.auth.password	string	Null	The password to be used for authentication challenges for this registration. If non-Null, this password will override the "Reg Password x" parameter entered into the Authentication submenu on the phone's Settings menu.
reg.x.auth.userId	string	Null	The user ID to be used for authentication challenges for this registration. If non-Null, this user ID will override the "Reg User x" parameter entered into the Settings menu on the phone.
reg.x.displayName	UTF-8 encoded string	Null	The display name used in SIP signaling as the default caller ID.

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.label	UTF-8 encoded string	Null	The text label to appear on the display beside the associated line key. If omitted, the label will be derived from the user part of reg.x.address.
reg.x.server.y.address	dotted-decimal IP address or hostname	Null	The optional IP address, host name, port, transport, registration period, fail-over parameters, and line seize subscription period of a SIP server that accepts registrations. Multiple servers can be listed starting with y=1 to 4 for fault tolerance. If specified, these servers may override the servers specified in <voIpProt.server/> . Note: If the reg.x.server.y.address parameter is non-Null, all of the reg.x.server.y.xxx parameters will override the parameters specified in <voIpProt.server/> . Note: If the reg.x.server.y.address parameter is non-Null, it takes precedence even if the DHCP server is available.
reg.x.server.y. specialInterop	standard, ocs2007r2, lcs2005, lync2010	standard	Specify if this registration should support Microsoft Office Communications Server 2007 R2 (ocs2007r2), Microsoft Live Communications Server 2005 (lcs2005), or Microsoft Lync 2010 (lync2010). Note: To use instant messaging on SpectraLink handsets, set this parameter to ocs2007r2.
reg.x.server.y.transport	DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly	DNSnaptr	The transport method the phone uses to communicate with the SIP server.
reg.x.type	private OR shared	private	If set to private, use standard call signaling. If set to shared, augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.

For more information, see the **reg-basic.cfg** and **reg-advanced.cfg** templates.

<roaming_buddies/>



This parameter is used in conjunction only with Microsoft Office Communications Server 2007 R2.

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
roaming_buddies.reg	positive integer	0	Specifies the line/registration number which has roaming buddies support enabled. If Null, roaming buddies is disabled. If the value < 1, then the value is replaced with 1.

For more information, see the **features.cfg** template.

<roaming_privacy/>



This parameter is used in conjunction only with Microsoft Office Communications Server 2007 R2.

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
roaming_privacy.reg	positive integer	0	Specifies the line/registration number which has roaming privacy support enabled. If Null, roaming privacy is disabled. If the value < 1, then the value is replaced with 1.

For more information, see the **features.cfg** template.

<up/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up. multikeyAnswerEnabled	0 or 1	0	A flag to determine whether or not pressing any key on the handset will answer an incoming call.
up.headsetOnlyAlerting	0 or 1	0	A flag to determine whether or not alerts are played out in the attached headset.

For more information, see the **wireless.cfg** and **site.cfg** templates.

<volpProt/>

The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
volpProt.SIP.IM. autoAnswerDelay	0 to 40, seconds	10	The time interval from receipt of the instant message invitation to automatically accepting the invitation.
volpProt.server.x. address	dotted-decimal IP address or hostname	Null	The IP address or host name and port of a SIP server that accepts registrations. Multiple servers can be listed starting with x=1 to 4 for fault tolerance.
volpProt.server.x. specialInterop	standard, ocs2007r2, lcs2005, lync2010	standard	If a special protocol is to be used by a registration, this parameters must be set appropriately. Note: To use instant messaging on SpectraLink handsets, set this parameter to ocs2007r2.

For more information, see the **sip-basic.cfg** and **sip-interop.cfg** templates.



The relevant configuration parameters are defined as follows:

Parameter (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
wifi.rtls.ekahua.address	String	169.254. 10.10	The IP address of the Ekahau Positioning Engine.
wifi.rtls.ekahau.enable	0 or 1	0	A flag to determine whether or not to support the Ekahau Real-Time Location System (RTLS).
wifi.rtls.ekahua.port	0 to 65535	8552	The port number of the Ekahau Positioning Engine.
wifi.rtls.ekahua.txInterval	0 to 2	0	The maximum transmit intervals. If set to 0, the transmit interval is 1 minute. If set to 1, the transmit interval is 5 minutes. If set to 2, the transmit interval is 10 minutes.

For more information, see the **wireless.cfg** template.

Miscellaneous Administrative Tasks

This appendix provides information that may be required to administer the Polycom® SpectraLink® 8400 Series Wireless Handsets. This includes:

- [Setting Up an FTP Server](#)
- [Using the Web Configuration Utility](#)

For other miscellaneous tasks, see the 'Miscellaneous Administrative Tasks' chapter of the latest *Polycom UC Software Administrator's Guide* available at <http://support.polycom.com/support/spectralink8400>.

Setting Up an FTP Server

A simple provisioning configuration uses File Transfer Protocol or FTP. Although FTP servers are free, they require installation, and use logins and passwords.

A free and popular server, Filezilla Server is available for Windows at <http://filezilla-project.org>. This application has been tested with the SpectraLink 8400 Series Handsets.

To set up the server:

- 1 Download and install the latest version of Filezilla Server.
- 2 After installation, you are presented with a "Connect to Server" pop-up. Select **OK** to open the administrative user interface.
- 3 To configure a user, select **Edit > Users** in the status bar.
- 4 Select **Add**.
- 5 Enter the user name for the phone and select **OK**.

For example, **bill123** .

- 6 Select the **Password** checkbox and enter a password.
For example, **1234**.
The phone will use this password to log in.
- 7 Select **Page >Shared folders** to specify the server-side directory where the provisioning files will be located (and the log files uploaded).
- 8 Select **Add** and pick the directory.
- 9 To allow the phone to upload logs onto the provisioning server, select the **Shared Folders > Files >Select Write and Delete** checkboxes, and then select **OK**.
- 10 Copy the configuration files from the software download into the directory specified above.
- 11 Determine the IP address of the provisioning server by entering **ipconfig** at a command prompt to display the server network configuration.
The IP Address of the provisioning server is shown.
- 12 To configure the phone to point to the IP address of the server, do the following:
 - a On the Home screen, select **Settings >Advanced Settings >Network Configuration**.
When prompted for the administrative password, enter **456**.
 - b Scroll down to **Server Menu**, then press the **Edit** soft key.
 - c Using the right arrow key, select **FTP** as the **Server Type**.
 - d Enter the IP address from step 11 as the **Server Address**, and then press the **OK** soft key.
 - e Enter the user name and password from steps 5 and 6 as the **Server User** and **Server Password**.
 - f Scroll down to **Save & Reboot**, and then press the **Select** soft key.
The phone will reboot.

The phone will upload two logs files to the directory specified in step 9: <MACaddress>-app.log and <MACaddress>boot.log .

Using the Web Configuration Utility

You can make changes to the phone's configuration through the Web Configuration Utility. The utility also permits many application settings to be modified, such as SIP server address, ring type, or regional settings such as time/date format and language. Some items in the **Settings** menu are locked to prevent accidental changes. To unlock these menus, enter the user or administrator passwords. The administrator password can be used anywhere

that the user password is used. The default user password is **123** and the default administrative password is **456**. Polycom recommends that you change the administrative password from the default value.



You cannot enable / disable blind transfer, call recording, picture frame, corporate directory (LDAP integration), and phone server redundancy through the Web Configuration Utility. You must make changes for these features through the configuration files. See [Part IV: Deploying the Handsets From the Provisioning Server](#) on page 32.

Changes made through the Web Configuration Utility or the phone's user interface are stored internally as overrides. These overrides take precedence over settings contained in the configuration obtained from the provisioning server.

If the provisioning server permits uploads, these override settings will be saved in a file called **<MAC Address>-web.cfg** on the provisioning server as well as in flash memory.



Web configuration changes will continue to override the provisioning server-derived configuration until deleted through the **Reset Web Configuration** menu selection or configured using the `<device/>` parameters.

Local configuration changes—made through the phone's user interface—will continue to override the provisioning server-derived configuration until deleted through the **Reset Local Configuration** menu selection or configured using the `<device/>` parameters.

This section provides instructions on the following topics:

- [Modifying the SpectraLink 8400 Series Handsets Configuration](#)
- [Exporting Configuration Files](#)

Modifying the SpectraLink 8400 Series Handsets Configuration

You can change the SpectraLink 8400 Series Handsets configuration using the Web Configuration Utility.

To configure the phone through the Web Configuration Utility:

- 1 Get your phone's IP address.

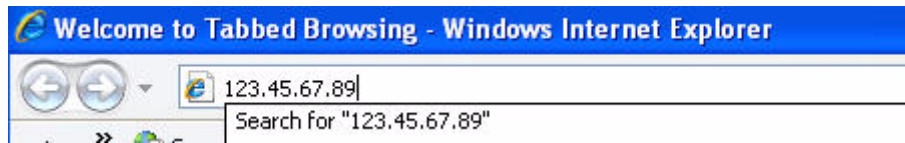
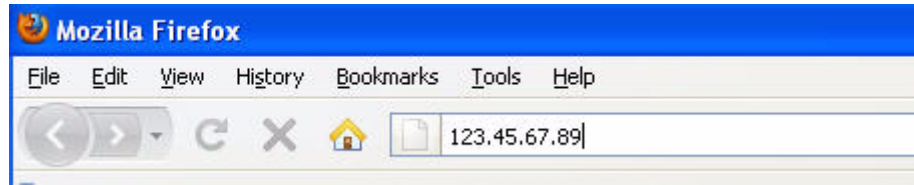
Select **Settings** on the handset's Home screen, and then select **Status > Platform > Phone**. Scroll down to see the IP address.

- 2 Select one of the supported Web browsers.

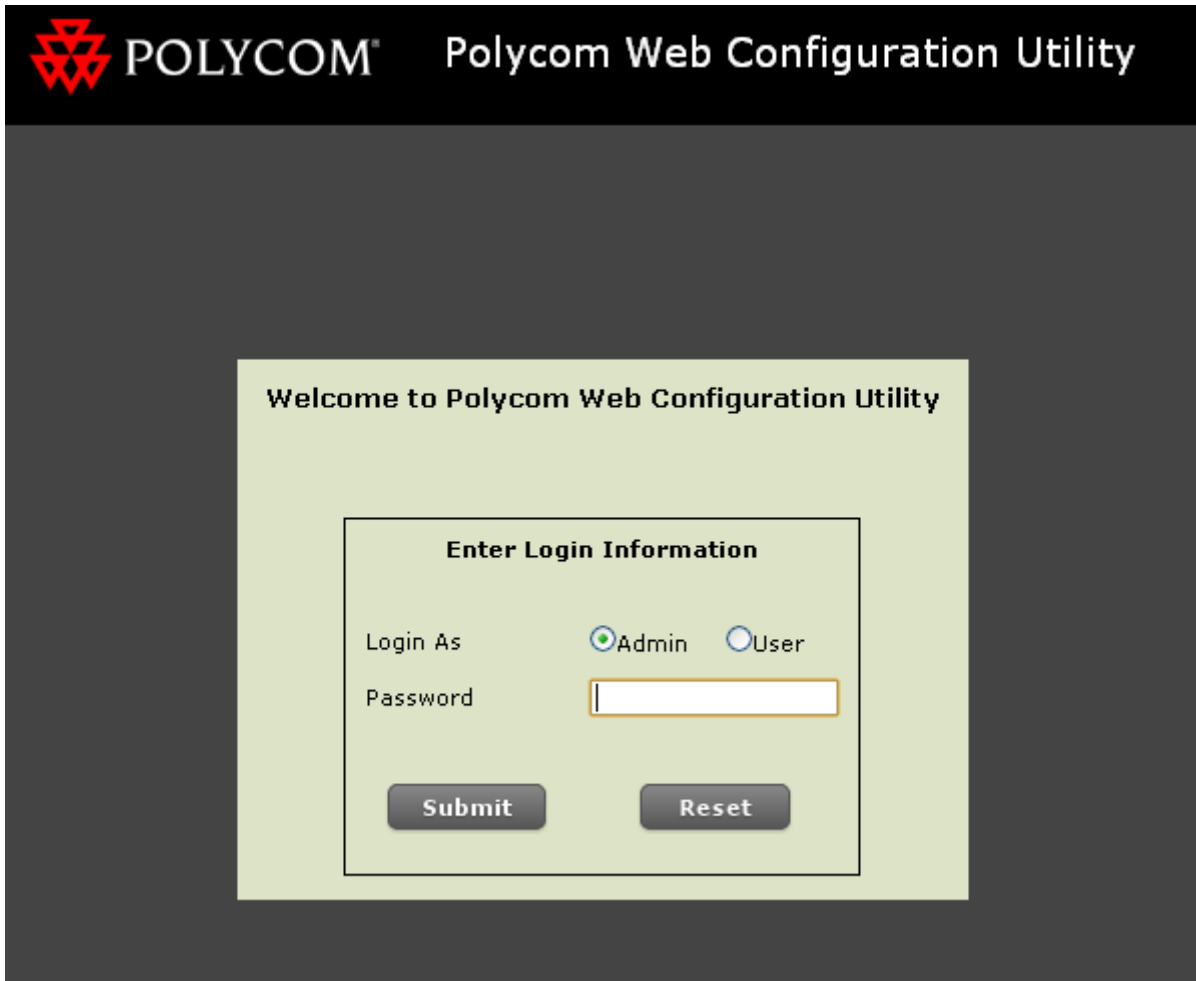
For a list of supported Web browsers, see the latest *Polycom UC Software Administrator's Guide* at

<http://support.polycom.com/support/spectralink8400> .

- 3 Enter the phone's IP address in the Web browser's address bar (as shown next).



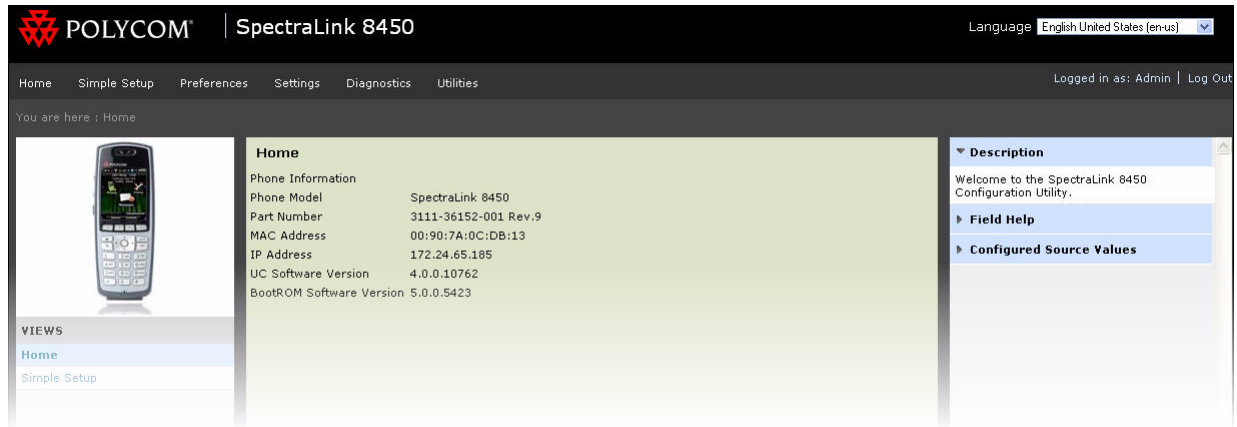
A Web page similar to the one shown next displays.



4 Log in as an Admin.

By default, the administrative password is 456.

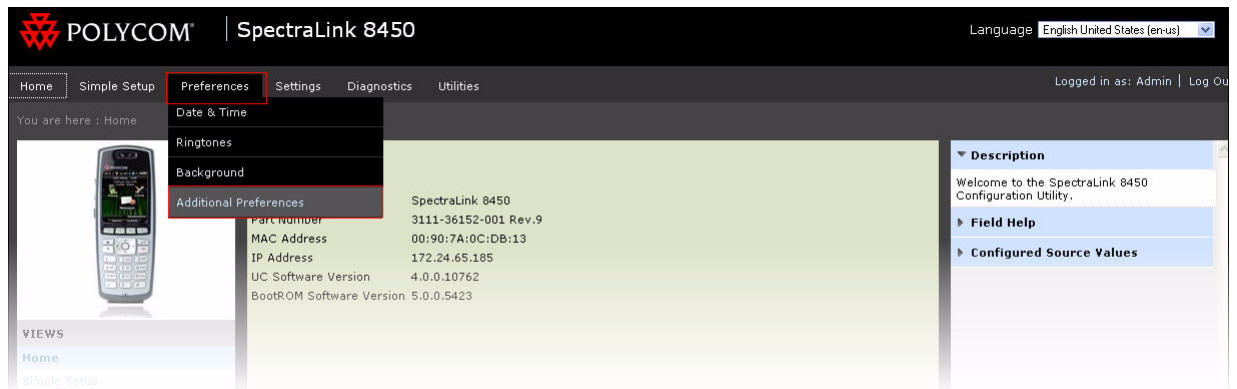
A Web page similar to the one shown below displays.



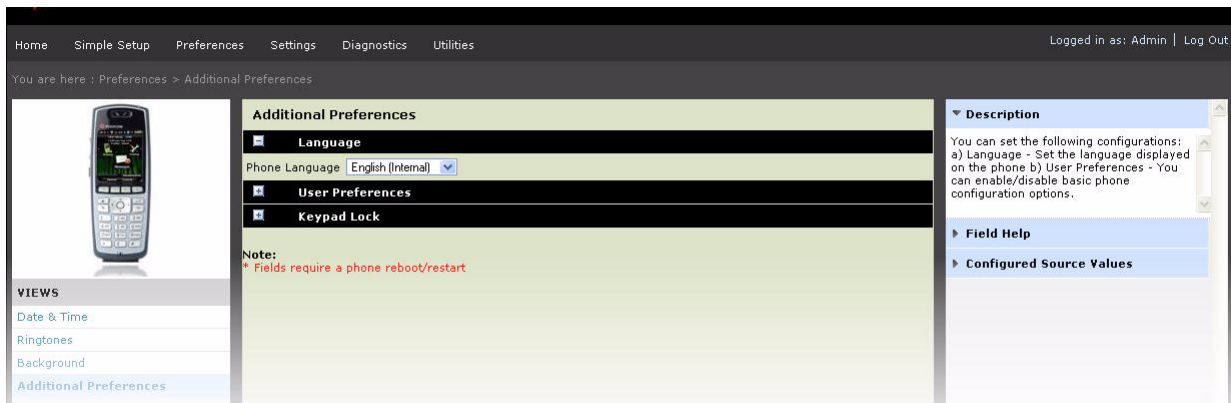
5 Make the desired configuration changes to the handset's configuration.

For example, to change the handset's displayed language to French, do the following:

- a Select **Preferences > Additional Preferences**.



A Web page similar to the one shown below displays.



b Select **French** from the Phone Language drop-down list.

c Select the **Save** button at the bottom of the page.

The language on the handset will change to French.

6 Log out of the Web Configuration Utility.

Exporting Configuration Files

You can export the SpectraLink 8400 Series Handsets configuration files using the Web Configuration Utility.



Passwords and security keys from the device settings are not exported. These parameters are listed at the top of the exported file, so they can be found quickly for editing.

To export configuration files through the Web Configuration Utility:

1 Get your phone's IP address.

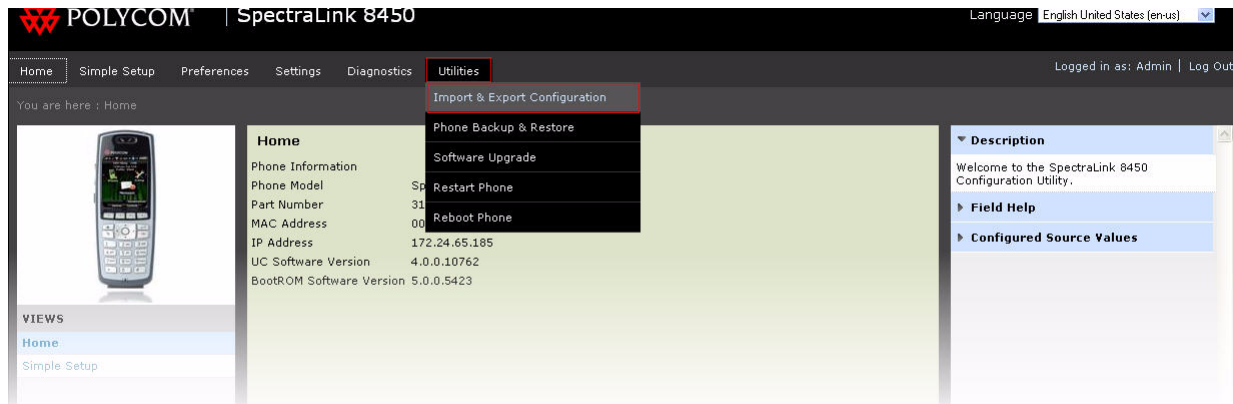
Select **Settings** on the handset's Home screen, and then select **Status > Platform > Phone**. Scroll down to see the IP address.

2 Select one of the supported Web browsers.

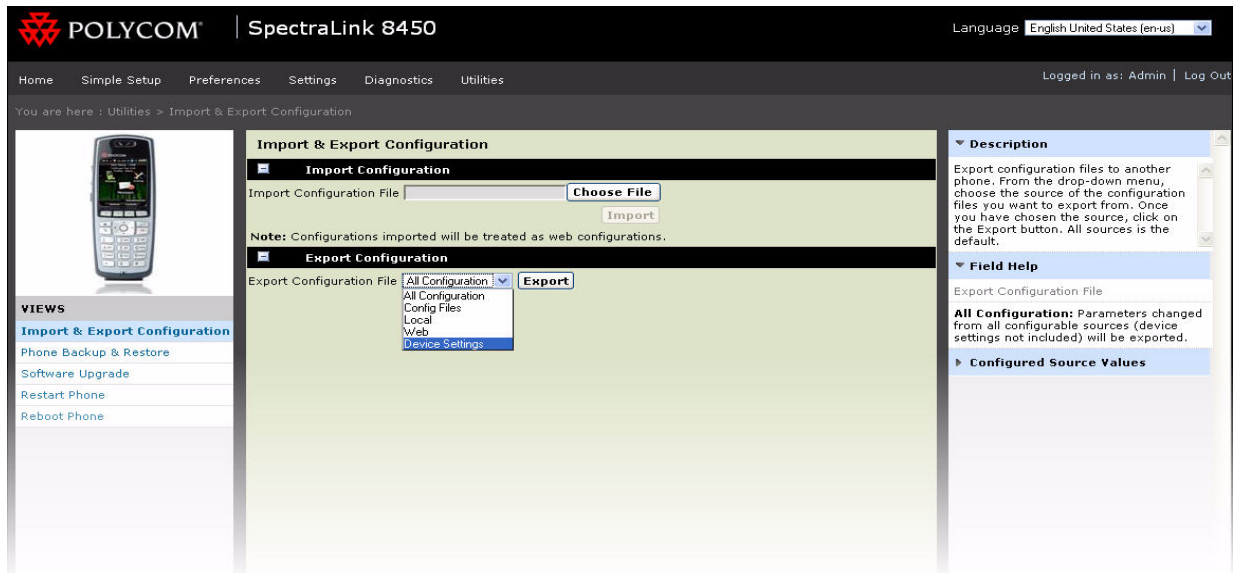
3 Enter the phone's IP address in the Web browser's address bar.

4 Enter the appropriate user name and password.

- 5 To export the configuration files, do the following:
 - a Select **Utilities > Import & Export Configuration**.



A Web page similar to the one shown below displays.



- b Select the configuration source that you want to export.
For example, if you want to export the device parameters, select **Device Settings**. Selecting **All** does not include device settings.
- c Select the **Export** button.
A pop-up displays on your computer with options to open or save the file.
- d Save the file in the desired location.

Deployment Checklist

This appendix provides a checklist of configuration parameters that you must set to provision the Polycom® SpectraLink® 8400 Series Wireless Handsets.

Before you provision your SpectraLink 8400 Series Handsets, you must gather up the following information to enter at the Wireless Configuration Station (WCS):

- Location of the latest Polycom UC Software
<http://support.polycom.com/support/spectralink8400>
- WCS folder name

- WCS user name

- WCS password

- SpectraLink 8400 Series Handsets IP Address from factory
_169.254.1.2_____
- WCS server address from factory
_169.254.1.1_____
- Wireless interface network address

- Wireless interface network mask

- Wireless interface IP gateway

- DNS domain name

- DNS server name

- DNS alternate server name

- Wi-Fi security mode

- Authentication method (if WEP is selected)

- Default key (if WEP is selected)

- WEP encryption (if WEP is selected)

- WEP keys (if WEP is selected)

- WEP key length (if WEP is selected)

- Pre-share key type (if WPA-Personal or WPA2-Personal is selected)

- Hexadecimal key (if WPA-Personal or WPA2-Personal is selected)

- Passphrase (if WPA-Personal or WPA2-Personal is selected)

- Fast roaming method (if WPA2- Enterprise is selected)

- Security name (if WPA2- Enterprise is selected)

- EAP type (if WPA2- Enterprise is selected)

- Security profile (if WPA Enterprise and PEAPv0/ are selected)

-
- CA profile (if WPA2- Enterprise and PEAPv0/ are selected)

 - CA certificate (if WPA2- Enterprise and PEAPv0 are selected)

 - In-band provisioning (if WPA2- Enterprise and EAP-FAST are selected)

 - PAC file password (if WPA2- Enterprise and EAP-FAST are selected)

 - PAC file (if WPA2- Enterprise and EAP-FAST are selected)

 - SSID

 - WMM-AC

 - Regulatory Domain

 - 5 GHz band

 - 5 GHz sub-band 1

 - 5 GHz sub-band 1 transmit power

 - 5 GHz sub-band 2

 - 5 GHz sub-band 2 transmit power

 - 5 GHz sub-band 3

 - 5 GHz sub-band 3 transmit power

 - 5 GHz sub-band 4

- 5 GHz sub-band 4 transmit power

- 2.4 GHz band

- 2.4 GHz band transmit power

- Syslog server name

- Syslog server transport

- Syslog server facility

- Syslog server render level

- Syslog server prepend MAC address

- WCS server type
__FTP__
- WCS server name

- WCS server user name
__PlcmSpIp__
- WCS server password
__PlcmSpIp__
- WCS master configuration filename
__000000000000.cfg__
- WCS network configuration filename
__8400-initial-setup.cfg__

Before you provision your SpectraLink 8400 Series Handsets, you must gather up the following information to enter at the provisioning server:

- Location of the latest Polycom UC Software
<http://support.polycom.com/support/spectralink8400>
- Provisioning server folder name

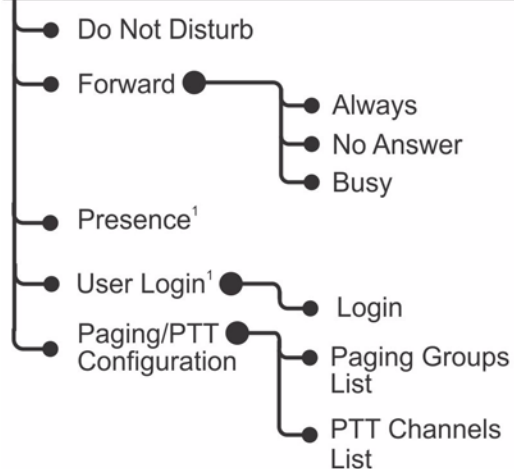
- Provisioning server type
__FTP__
- Provisioning server name

- Provisioning server user name
__PlcmSpIp__
- Provisioning server password
__PlcmSpIp__
- UC Software filename

- Per-phone configuration filename
__phone[MACAddress].cfg__
- Provisioning server master configuration filename
__000000000000.cfg__

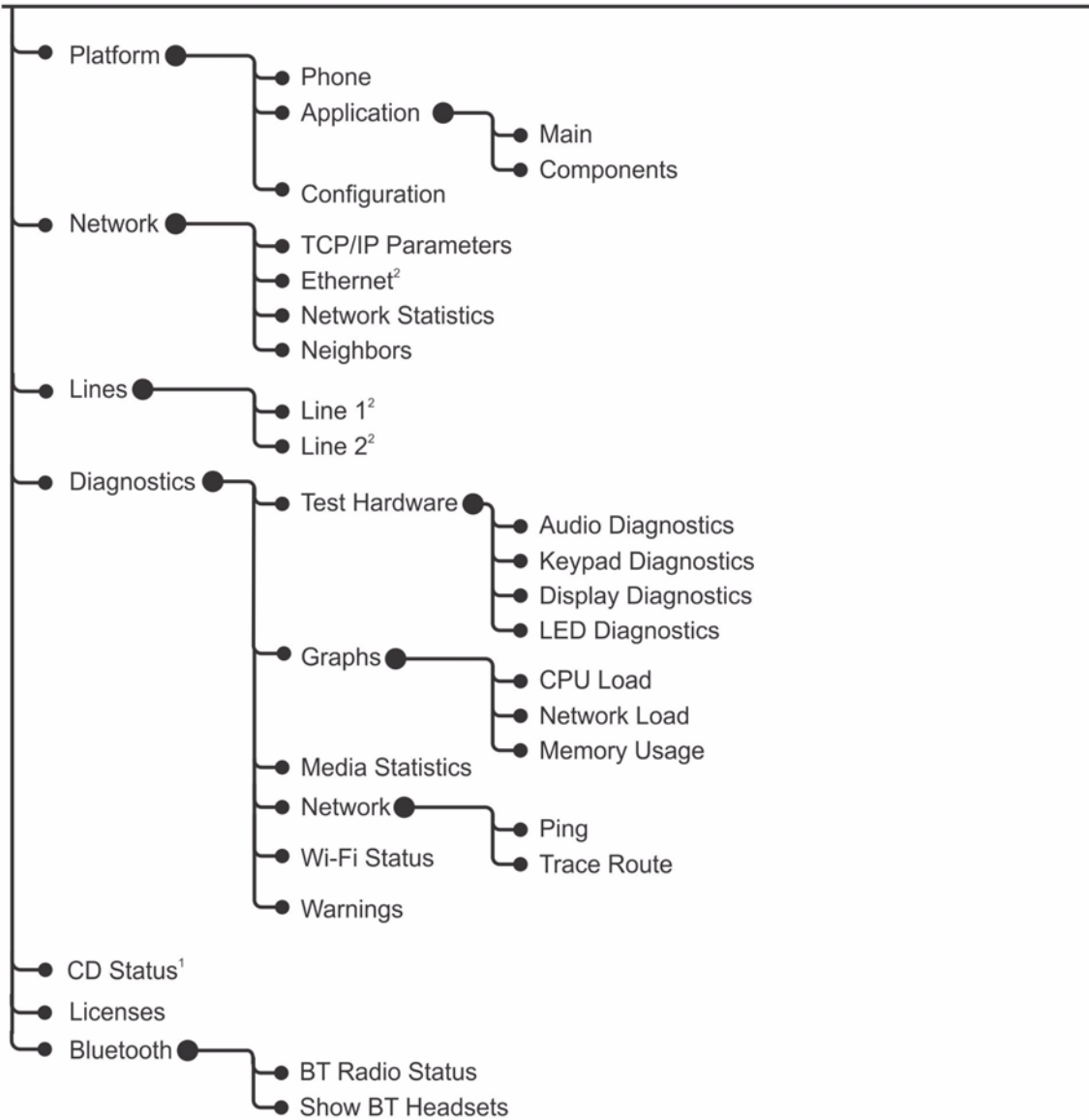
Polycom UC Software Menu System

Settings > Features Settings



¹ If enabled.

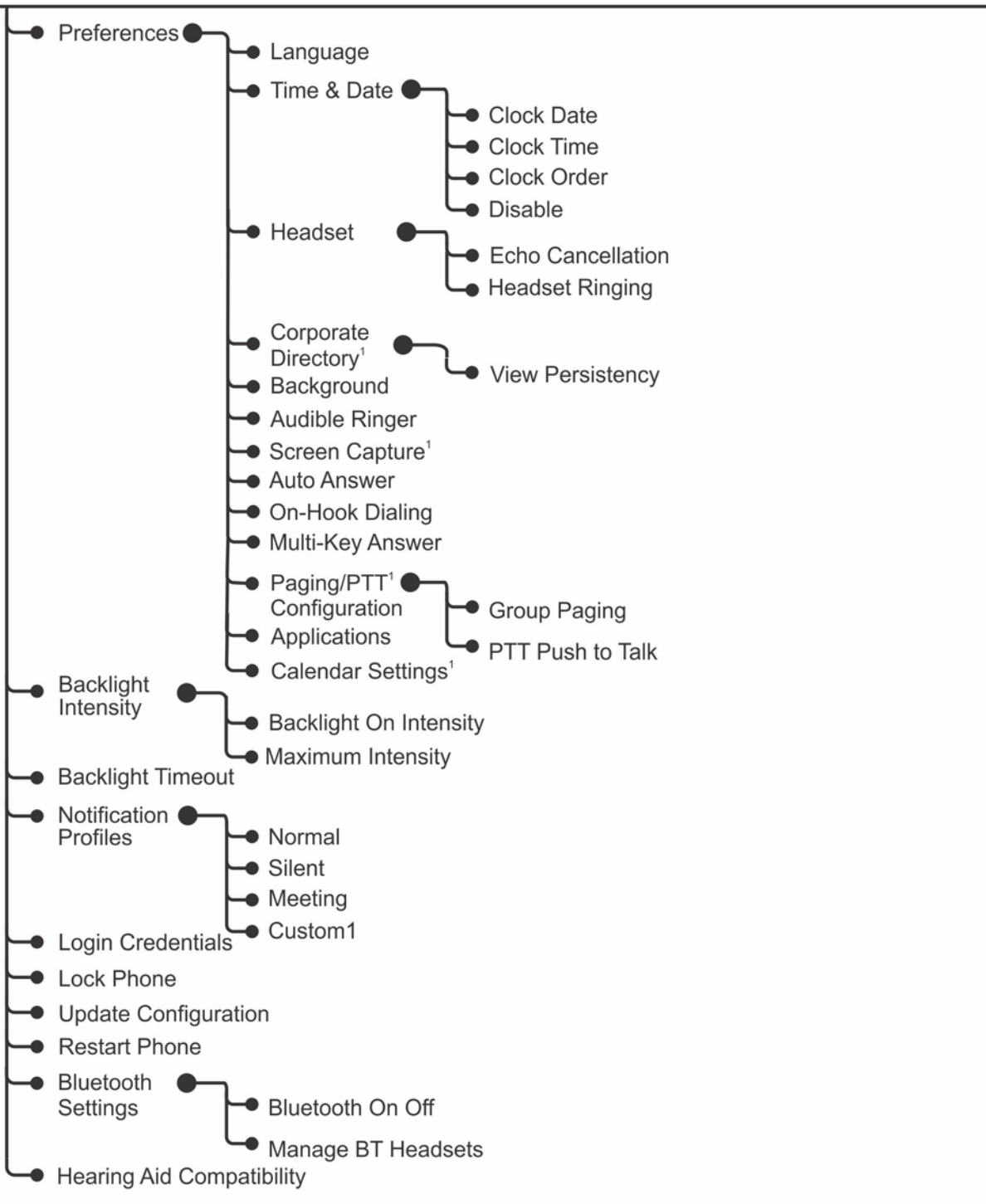
Settings > Status



¹ If enabled.

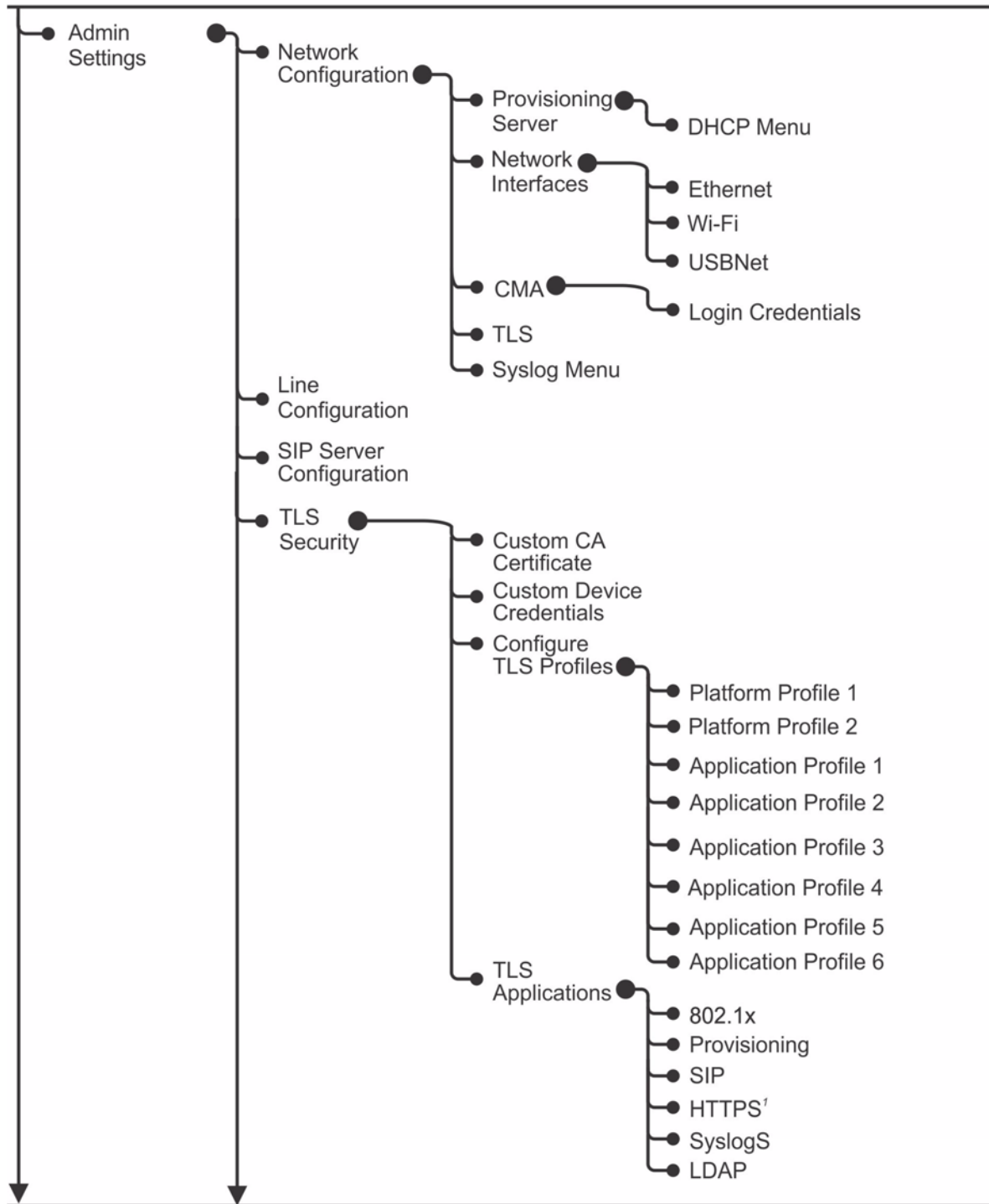
² If applicable.

Settings > Basic



¹ If enabled.

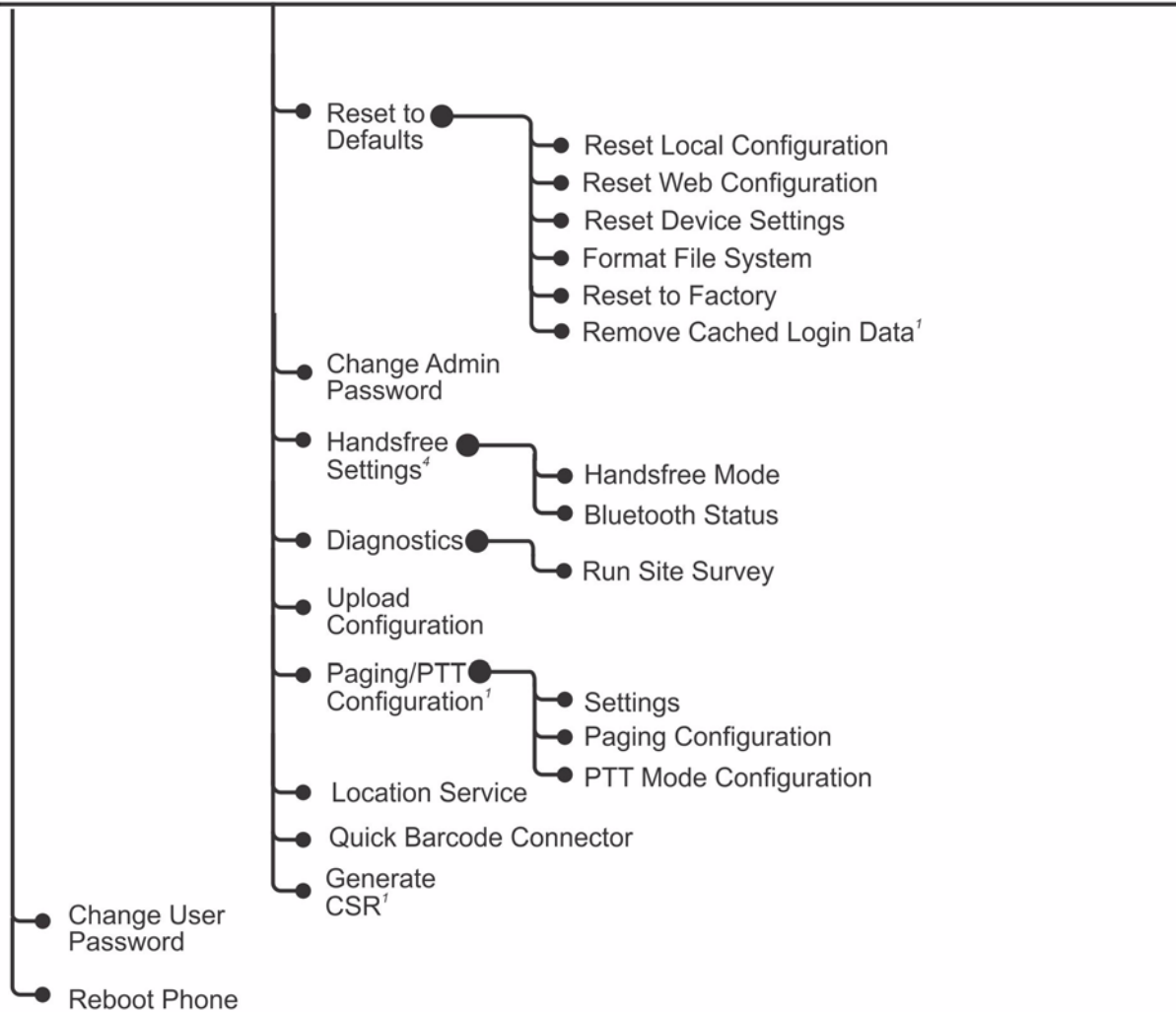
Settings > Advanced³



¹ If enabled.

³ Requires administrator password.

Settings > Advanced³ (Continued)



¹ If enabled.

³ Requires administrator password.

Contacts/Call Lists⁴

- Contact Directory
- Corporate¹ Directory
- Call Lists

Messages⁴

Applications⁴

¹ If enabled.

⁴ Organization dependent.