

Spectralink 84-Series Wireless Telephone

Deployment Guide

Spectralink Software Versions

4.3.x to 4.13.x

Copyright Notice

© 2012-2016 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are 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 Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at <http://support.spectralink.com>.

Contact Information

US Location

800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301

info@spectralink.com

European Location

+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens, Denmark

infodk@spectralink.com

Contents

Introduction.....	8
Where is the Software?	8
Recommended Software Tools.....	9
XML editor.....	9
FTP Server.....	9
Release Notes	9
Product Support	9
Spectralink References	10
Specific Documents	11
Conventions Used in This Guide	12
Icons	12
Typography.....	13
 Part I: Getting Started	 15
 Chapter 1: Quick Start with SLIC.....	 16
 Chapter 2: Handset Usage Scenarios	 17
The Three Scenarios.....	17
Flat Deployment.....	18
Group Deployment	18
User Profiles Deployment.....	19
Listing Handsets/Users to be Deployed.....	20
Sample File for Listing Users and Parameters	22
 Chapter 3: Infrastructure.....	 23
Network Components.....	23
Recommended Reading	23
Quality of Service.....	24
WLAN Security	24
Security Methods	24
System Diagram.....	26
System Requirements	27
System Components	27
Spectralink 84-Series handsets.....	27
Servers	28
Access points.....	30
Ethernet switch	30

Chapter 4: Understanding Wireless Telephony Provisioning..... 31

What is Provisioning?	31
The Provisioning Process	32
Managing Configuration Files	33
Viewing the .cfg File Templates	33
<i>Where are the Templates?</i>	34
<i>Configuration Folder Contents</i>	34
Viewing and Editing .cfg Files	35
Creating New .cfg Files	37
Types of .cfg Files	38
<i>Top Level .cfg Files</i>	38
<i>General-to-Specific Criteria</i>	40
Flat Deployment	41
Group_Deployment	44
User_Profiles_Deployment	46
Features Deployment	48

Part II: Configuration 49**Chapter 5: Determining What Parameters You Will Need to Configure..... 50**

Using the Template Spreadsheet	50
Wireless Settings	51
System and Telephony Settings	52
Per-Phone (User) Settings	53
Feature(s) and Group(s) Settings	54

Chapter 6: Telephony Server Variations 55

Lync Telephony Server	55
<i>Microsoft Lync compatibility</i>	55
<i>Lync Interoperability Overview</i>	57
OpenSIP Telephony Server	57

Chapter 7: Configuring Central Provisioning Server .cfg files..... 58

Finalize your Deployment Scenario Structure	58
Organize the Files	58
Configure site.cfg	59
<i>System Parameters</i>	60
<i>Telephony Parameters</i>	62
<i>Feature Parameters</i>	65

<i>User Profiles</i>	69
Configure the Per-phone .cfg File	70
<i>Filenames for per-phone or per-user .cfg files</i>	70
<i>Per-Phone .cfg Files</i>	71
<i>Per-User .cfg Files</i>	73
Configure the <MACaddress>.cfg file	76
Deploying Features	78
<i>Barcode</i>	78
<i>Corporate Directory</i>	78
<i>OAI</i>	79
<i>Personal Alarms</i>	79
<i>Push-to-talk (PTT)</i>	80
<i>RTLS</i>	82
Save the Central Provisioning Server .cfg Files	83
 Chapter 8: Configuring Wireless Parameters (without SLIC)	 84
Prepare to Configure the Wireless Settings	85
The USB_Setup folder	85
Configure wireless.cfg	85
<i>USBnet</i>	86
<i>PhoneAdminPassword</i>	86
<i>Provisioning Server</i>	87
<i>WirelessSettings</i>	89
<i>Wi-Fi Radio Settings</i>	90
<i>Wi-Fi Security</i>	95
<i>DHCP</i>	103
<i>DNS</i>	103
<i>SNTP</i>	103
 Part III: Deployment	 106
 Chapter 9: Set up the Central Provisioning Server	 107
Central Provisioning Server Requirements	107
Set up Directories	108
<i>File Permissions</i>	108
Downloading Spectralink 84-Series Software Files to the Central Provisioning Server	109
View the 84-Series Software Files	110
<i>Copy your custom .cfg files to the appropriate folders</i>	110
Ensure the Provisioning Server is available on the LAN	111

Chapter 10: Wireless Deployment	112
Identify a Suitable Initial Provisioning Computer	112
<i>Enable the Handset's Network Capabilities</i>	<i>113</i>
Download the Wireless Configuration to the Handsets	114
Optimization Pointers for Quantity Deployment.....	116
Which Phone Goes to Which User?	116
Storing Wireless Configuration Files	116
Chapter 11: Testing the Handsets	118
Wireless LAN Association.....	118
Test Configured Features.....	118
Chapter 12: Deploying Additional Phones or Features.....	119
Adding New Phones	119
<i>Configuration.....</i>	<i>119</i>
<i>Deployment.....</i>	<i>119</i>
<i>Test.....</i>	<i>119</i>
Decommissioning for RMA	120
Receiving Phones from RMA	120
Changing Phone Configuration	120
Adding New or Advanced Features	120
Part IV: Troubleshooting.....	121
Chapter 13: Basic Troubleshooting	122
Config Files.....	122
Provisioning Methods and Override Files.....	122
<i>Clearing overrides on a single phone</i>	<i>123</i>
Software Version	123
Wireless Connection	123
Connection to SIP Server and Calling	124
Display	125
Upgrading.....	125
Setting Up Syslog.....	126
User Accessible Network Diagnostics.....	126
Parameter values	126
Chapter 14: Wi-Fi Diagnostics	127
Screen 1 (Packet Count).....	128
Screen 2 (General Information).....	128

Screen 3 (AP List)	129
<i>Mnemonic Reason Codes</i>	129
Screen 4 (Association Count/Failure)	130
Screen 5 (Security)	131
Screen 6 (Extensible Authentication Protocol (EAP) Information)	131
 Chapter 15: Run Site Survey	 132
Update Interval	134
 Chapter 16: Access Point Issues	 136
In Range/Out-of-Range	136
Capacity	136
Transmission Obstructions	136
 Part V: Appendices	 137
 Appendix A: Setting up an FTP Server	 138
 Appendix B: Upgrading Spectralink 84-Series Software	 140
<i>Upgrading Your Phones</i>	140
 Appendix C: Using the Web Configuration Utility	 143
Configuration Using the Web Configuration Utility	143
Exporting Configuration Files	146
 Appendix D: Software Copyrights and Open Source Information	 148
Software Copyright	148
OFFER for Source for GPL and LGPL Software	148
<i>Contact Information for Requesting Source Code</i>	149
 Appendix E: Spectralink Certificates	 150

Introduction

This guide introduces the requirements of wireless telephony provisioning and how these requirements are implemented for the Spectralink 84-Series Wireless Telephones. The intention of this document is to help you set up your system so that you establish the necessary building blocks for efficient administration and easy expansion.



Spectralink recommends: Use these configuration methods

You may be familiar with several deployment methods or ready to learn. However, Spectralink recommends the methods described in this guide as the most flexible and manageable. Once you learn how to work with the configuration requirements recommended here, you will be able to use other provisioning and deployment methods with more understanding.

Although it assumes a fairly high level of familiarity with your existing system, this guide will walk you through each step that specifically pertains to wireless telephone configuration, the parameters required by the 84-Series handsets and major features that are commonly deployed.

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 and equipment
- Your phone system and how to add SIP telephones extensions to it



Admin Tip: If you are currently using Polycom UC desk phones

This guide does not provide information about how to deploy Spectralink 84-Series handsets into a system currently using Polycom UC software. Refer to the Interoperability Guide: *Spectralink 84-Series Coexistence with Polycom Desksets* and contact your Polycom representative if you are currently using Polycom wired phones.

Where is the Software?

You will need to download the software from the Spectralink website. When you unzip the file, you will find folders for the configuration file templates and other files that are referenced in this document to help you deploy the handsets. Get the software at <http://support.spectralink.com>.

Recommended Software Tools

XML editor

In order to view, edit and create the configuration files, you will need to use an XML editor. Some we have used are listed below. See [Managing Configuration Files](#) for more information.

The XML editor used in the screen shots in this document is a free editor provided by Microsoft, *XML Notepad*

XML Notepad can be downloaded from this site:

<http://www.microsoft.com/en-us/download/details.aspx?id=7973>

Notepad++ with the XML Plugin is a text editor that uses colors to emphasize the XML structure. *Notepad++* is free and available at this site:

<http://notepad-plus-plus.org/>

XML Marker is a free text editor which may prove useful for file viewing.

XML Marker is available at:

<http://symbolclick.com/>

FTP Server

Although you can use other protocols (TFTP, HTTP, HTTPS), we recommend the use of FTP as the file transfer protocol required by the system. Accordingly this document will direct you to set up the provisioning server and the wireless configuration station as FTP servers. See [Appendix A: Setting up an FTP Server](#) for exact information about how to set up an FTP server.



Settings: Using other file transfer protocols

For directions on setting up a different file transfer protocol (TFTP, HTTP, or HTTPS), please contact your Spectralink support representative.

Release Notes

Every software release is accompanied by release notes that provide the new and changed features and resolved issues in the latest version of the software. Please review these for the most current information about your software.

Product Support

Spectralink wants you to have a successful installation. If you have questions please contact the Customer Support Hotline at 1-800-775-5330.

The hotline is open Monday through Friday, 6 a.m. to 6 p.m. Mountain time.

For Technical Support: <mailto:technicalsupport@spectralink.com>

For Knowledge Base: <http://support.spectralink.com>

For Return Material Authorization: <mailto:nalarma@spectralink.com>

Spectralink References

All Spectralink documents are available at <http://support.spectralink.com>.

The screenshot shows the Spectralink Support website. At the top, there is a navigation bar with links for Partner Access, Spectralink.com, Contact Support, and a search bar. Below this is the Spectralink logo with the tagline 'solving every day' and the word 'support'. The main navigation menu includes Product Resources, RMAs, Service Requests, and Customer Management. The main content area is titled 'Welcome to Spectralink Support' and includes a search bar for product documents and downloads. The search bar has dropdown menus for Product Category (set to 'Wi-Fi') and Product Type (set to '- Any -'), and a 'FIND' button. To the right of the search bar, there is a list of links for finding all product resources: All Documents & Downloads, Feature Requests, Product Alerts, Service Policies, FAQs, and Contact Support. Below the search bar, there are two main sections: 'RMAs AND SERVICE REQUESTS' and 'CUSTOMER MANAGEMENT'. The 'RMAs AND SERVICE REQUESTS' section includes links for RMA Status, RMA Forms, RMA Requests, My Company's RMAs, My Service Requests, My Company's Service Requests, and Repair Pricing. The 'CUSTOMER MANAGEMENT' section includes links for Warranty and Entitlement Lookup, My Company's Entitlements, and Batch Warranty and Entitlement Lookup. At the bottom of the page, there is a copyright notice: © 2013 Spectralink Corporation, All rights reserved. Terms and Conditions | Product Warranty.

To go to a specific product page:

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

Specific Documents

This document does not presume to cover the complete range of deployment requirements for Spectralink 84-Series Wireless Handsets.

For quick setups and easy deployments, please see the *Spectralink Installation and Configuration Tool Administration Guide*.

Please refer to the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper for security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality within enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephones*. This document identifies issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

This document has a brief discussion about wireless security. For more information and for assistance in determining which security method to use, see *Understanding Wireless Security on Your Spectralink 84-Series Wireless Telephones*.

The comprehensive *Spectralink 84-Series Wireless Telephone Administration Guide* covers all configuration parameters for the 84-Series Wireless Telephones.

Barcode Administration Guide Provides information about barcode symbologies and how to configure and implement the barcode feature on the handset. The *Spectralink 84-Series User Guide* also contains information about using the barcode feature.

For implementation of barcode application see the *Quick Barcode Connector* document. The *Spectralink 84-Series User Guide* also contains information about deploying the barcode feature.

The *Spectralink 84-Series User Guide* offers comprehensive instructions on using each of the features deployed on the handsets.

Technical Bulletins detail workarounds to existing issues and provides expanded descriptions and examples. These are available under the Technical Bulletins tab on the 84-Series handset page.

Release Notes describe the new and changed features, and resolved issues in the latest version of the software. Find them under the Downloads tab.

The *Web Developer's Guide* is your guide for the development of applications that run on the Browser on the Spectralink 84-Series Wireless Handsets. Contact your service consultant for more information.

AP Configuration Guides show you how to correctly configure access points and WLAN controllers (if applicable) and identify the optimal settings that support Spectralink 84-Series handsets. The guides can be found at the View Certified page.

Conventions Used in This Guide

Icons

Icons indicate extra information about nearby text.



Warning

The *Warning* icon highlights an action you must perform (or avoid) to avoid exposing yourself or others to hazardous conditions.



Caution

The *Caution* icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, successful feature configuration and/or affect phone or network performance.



Spectralink recommends

Our recommendations for successful deployments.



Note

The *Note* icon highlights information of interest or important information that will help you be successful in accomplishing a procedure or understanding a concept.



Tip

The *Tip* icon highlights information that may be valuable or helpful for users to know, such as special techniques, shortcut methods, or information that will make user tasks easier to perform.



Web

The *Web Info* icon highlights supplementary information available online such as documents or downloads on support.spectralink.com or other locations.



Timesaver

A time-saving tip is typically used to mention or highlight a faster or alternative method for users who may already be familiar with the operation or method being discussed.



Admin Tip

This tip advises the administrator of a smarter, more productive or alternative method of performing an administrator-level task or procedure.



Power User

A Power User Tip is typically reserved for information directed specifically at high-level users who are familiar with the information or procedure being discussed and are looking for better or more efficient ways of performing the task. For example, this might highlight customization of a feature for a specific purpose.



Troubleshooting

This element can be used in any type of document and is typically used to highlight information to help you solve a relevant problem you may encounter, or to point to other relevant troubleshooting reference information.



Settings

The Settings icon highlights information to help you zero in on settings you need to choose for a specific behavior, to enable a specific feature, or access customization options.

Typography

A few typographic conventions, listed next, are used in this guide to distinguish types of in-text information.

<i>Convention</i>	<i>Description</i>
Bold	Highlights interface items such as menus, soft keys, file names, and directories. Also used to represent menu selections and text entry to the phone.
<i>Italics</i>	Used to emphasize text, to show example values or inputs, and to show titles of reference documents available from the Spectralink Support Web site and other reference sites.
<u>Underlined blue</u>	Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.
Bright orange text	Used for cross references to other sections within this document. If you click on text in this style, you will be taken to another part of this document.
Fixed-width-font	Used for code fragments and parameter names.

This guide also uses a few writing conventions to distinguish conditional information.

<i>Convention</i>	<i>Description</i>
<MACaddress>	Indicates that you must enter information specific to your installation, phone, or network. For example, when you see <MACaddress>, enter your phone's 12-digit MAC address. If you see <installed-directory>, enter the path to your installation directory.
>	Indicates that you need to select an item from a menu. For example, Settings> Basic indicates that you need to select Basic from the Settings menu.

Part I: Getting Started

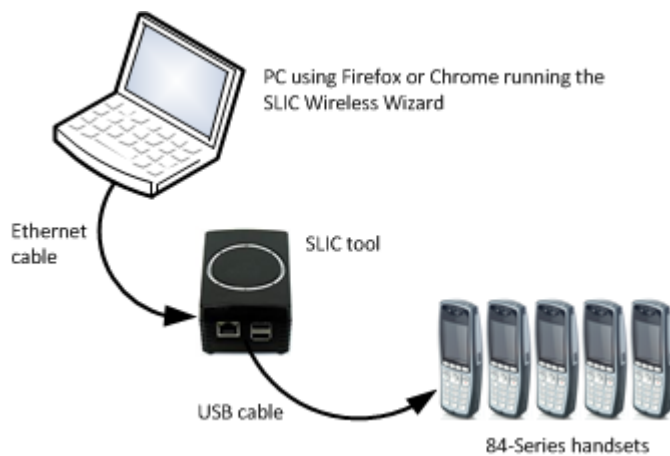
Part I: Getting Started covers basic information you will need to understand the hardware and software components that comprise a wireless SIP implementation. This Part introduces you to SIP and managing the .cfg files that the 84-Series handset requires.

- Handset usage scenarios
Three common deployment scenarios are introduced. Each of these requires a different deployment approach and information.
- Infrastructure requirements
Covers network components, QoS issues, WLAN security and system requirements.
- Understanding Wireless Telephone Provisioning
Provides an overview of phone provisioning and how the different scenarios are deployed.

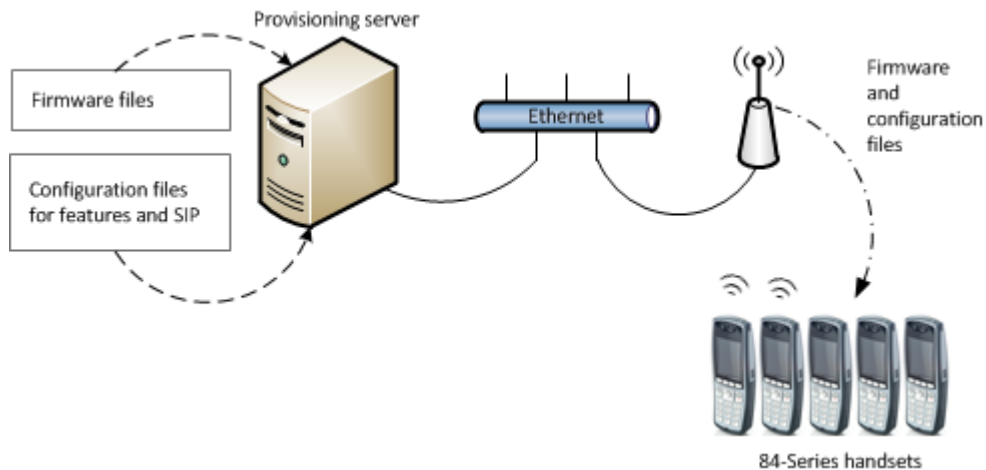
Chapter 1: Quick Start with SLIC

Use the Spectralink Installation and Configuration (SLIC) tool for a simple and speedy two-step setup process. Detailed information about this tool is provided in the *Spectralink Installation and Configuration Tool Administration Guide* available online. You can procure the tool from your service representative. Details on wireless configuration parameters are available in Chapter 8, section: [Configure wireless.cfg](#).

- 1 Connect the Spectralink Installation and Configuration (SLIC) Tool to a PC and start the browser to open the Wireless Wizard and configure wireless settings. Then use SLIC to load the settings onto the handset. The handset will associate with the wireless LAN.



- 2 Download firmware software from the Spectralink support site. Load this software onto the provisioning server. Configure SIP and feature settings by using the SLIC Feature Wizard or you can custom configure your files. Once these files are loaded into the provisioning server, the handset picks them up over-the-air.



Chapter 2: Handset Usage Scenarios

How you provision and deploy your Spectralink 84-Series handsets depends on the usage scenario you will employ. Key factors in determining which scenario applies to your installation depend on three mutually exclusive usage criteria.

Read through this document to get an idea of what a basic deployment looks like and then develop your own configuration tree that incorporates all the features you intend to deploy in your facility.

The Three Scenarios

The three scenarios outlined below cover any type of installation of any size. We recommend using one of these scenarios for simplicity of configuration, ease of maintenance and consistency of installations. This increases the efficiency of support across your entire user base and improves service to the wireless telephone user.

Determine which scenario applies to your installation then use that strategy to deploy the telephones.

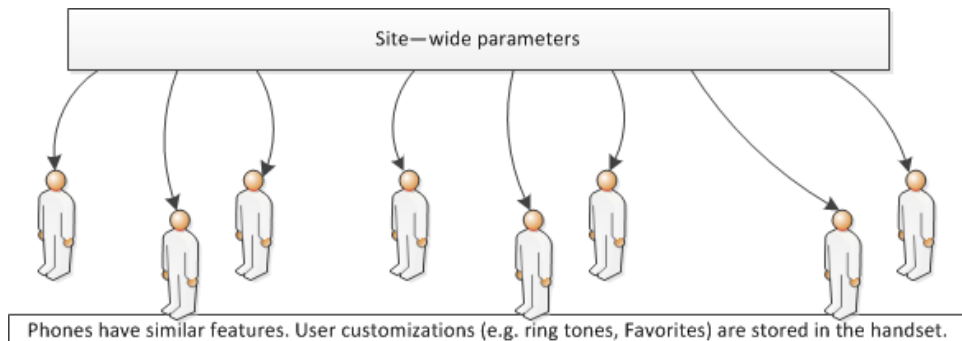


Tip: Combining scenarios

Technically, these three usage criteria are not mutually exclusive but programming and maintenance are challenging if they are combined. Due to serious management and deployment issues, we consider these mutually exclusive for the purposes of this document. If you wish to combine these criteria, contact your service representative for installation assistance from a Deployment Specialist.

Flat Deployment

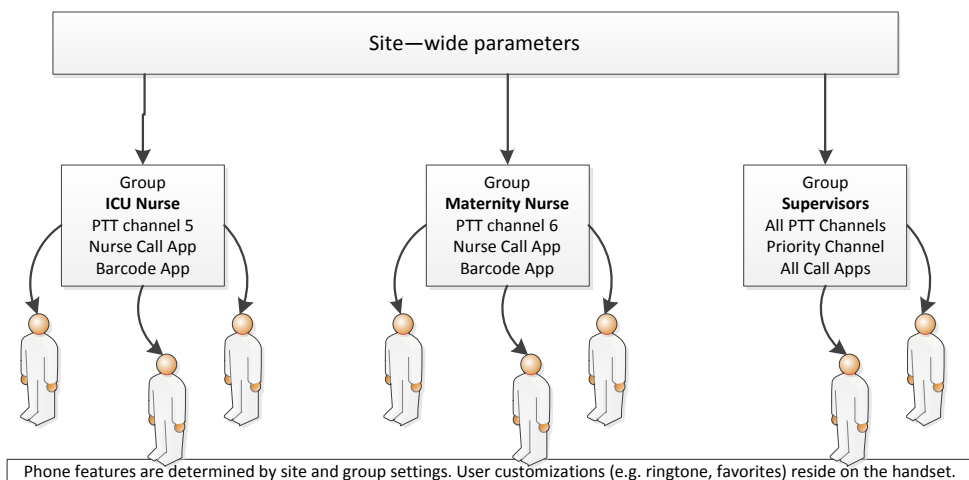
In the simplest deployment, all phones use virtually the same features, like ordinary office desk phones. This scenario is common in smaller or more homogenous facilities where handsets are assigned by extension and there is little variation in the features assigned to different users.



Group Deployment

Some facilities require different features for different users. Push-to-talk channels, for example, are frequently assigned in groups. For example, in a hardware store different channels may be assigned to customer service, plumbing and hardware but supervisors must monitor all channels. In another example, a hospital setting may require different PTT channels for maternity and ICU nurses while facilities staff could be assigned completely separate channels and all supervisors monitor all channels.

The simplest way to configure groups and make them easily maintainable is to set up specific group files and assign them to individual users as shown in the following diagram. This is a more involved deployment but yields benefits in ease of maintenance of complex installations.



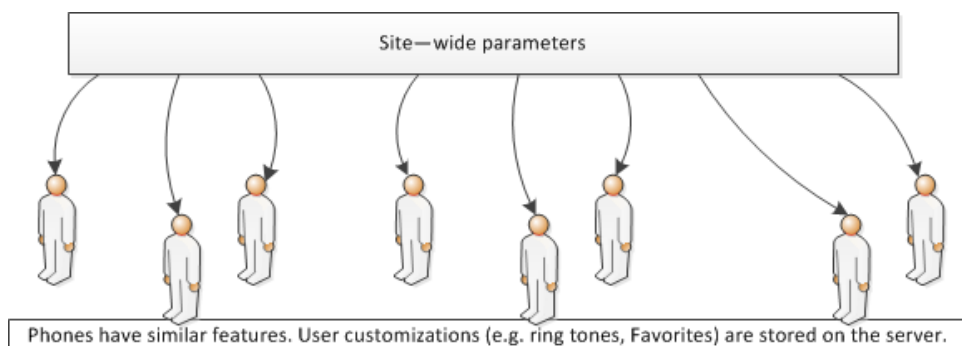
**Power Tip: More on configuring Groups**

Groups can be deployed under the Flat Deployment and User Profiles scenarios by including group parameters in individual user files. This is a workable alternative in a limited setting where simplicity of deployment is the primary consideration and future maintenance would not be a burden. Contact Customer Support and request a Deployment Specialist for help on setting up group parameters in per-user files.

User Profiles Deployment

User profiles are important when you want to separate phone assignment from the phone hardware. With User Profiles, any user can pick up any phone and log into it and the phone will have that user's personal settings. This type of deployment is frequently used in shift situations where convenience and accountability are important.

Although the structure is similar to the Flat Deployment scenario, they are conceptually quite different as user information such as call logs and contacts is stored on the server, not in the individual handset's memory. User Profiles give you a high degree of deployment flexibility since you can have more extensions and users than you have phones.



Listing Handsets/Users to be Deployed

Determine what handset models you will be deploying and who will be using them. We recommend that you use a spreadsheet to track the handsets and users. The list you make will vary depending on your scenario. You can use the configuration spreadsheet as a starting point. It is on the 84-Series webpage under the Download tab.

For Flat and Group Deployments, phones are linked to extensions. You will need to assign each phone to an extension by its MACaddress. The MACaddress is a unique identifier found on the label inside the battery compartment of each handset that follows the convention 00.90.7A.xx.yy.xx. The last three sets of numbers and letters are unique for each phone. Ensure that there is a column for the MACaddress on the list you create.

Label example:



Power Tip: Assigning phones to users

When you get your shipment of phones, unpack them and assign them to a user or extension by MACaddress by entering each phone's MACaddress next to an extension on your list. This way you will establish the correspondence between the extension and the phone from the start. Using the data on the list you create from the start will help to avoid confusion later when you start configuring the parameters.

- In a Flat deployment installation, the phones are assigned to specific extensions. List all the phones you intend to deploy with a column reserved for the MACaddress---
- If you are configuring Groups the phones are assigned to specific extensions. List all the phones you intend to deploy with a column reserved for the MACaddress. Identify what Groups you will deploy and add a column for the Group Name. Use the Group tab in the sample spreadsheet to help you identify the parameters you need to define for each group.
- If you use User Profiles, you need to list all the users. You may separately list all the phones but users and phones are not tethered to one another and only the Users list matters when determining features and extensions.



Admin Tip: OCS or Lync configuration

If you are deploying Instant Messaging or other features which use OCS or Lync®, you will need to add a second row for each user to enter the parameters required by these applications.

The affected parameter names are included in this table for future reference. They are defined later in this document.

Setting column	What it is	Affects:
MACAddress or	Phone's MACAddress (find it on the label in the battery compartment format 00.90.7A.xx.xx.xx.	File name of <MACAddress>-ext.cfg file
UserProfile	User Profile ID that will be used for the user profile configuration file name. For identification and maintenance purposes, this is usually the person's name.	File name for <UserProfile>.cfg file
Name of user	When using the MACAddress to assign phones, you need a concordance with a user name in order to facilitate file maintenance.	Info only
Type	Telephony, OCS or Lync (represents server type line appearance will register against.)	Info only
Address	Call server IP Address or Fully Qualified Domain Name	[reg.x.server.x.address]
Port	SIP Call server port number (Default is 5060 if not specified)	[reg.x.server.x.port]
Extension	SIP device extension *** If your SIP domain is programmed on the call server for the handsets you must include the domain with the Extension*** (do not include @sipdomain for AudioCodes) ie. extension@sipdomain	[reg.x.address]
UserID	SIP Extension user ID	[reg.x.auth.userId]
Password	SIP extension authentication password (Required for digest authentication) (Leave blank for AudioCodes)	[reg.x.auth.password]
Display Name	SIP Extension Caller-ID display information	[reg.x.displayName]
Line Label	SIP Extension label that appears on the handset display	[reg.x.label]
Profile Pwd	User Profiles default password	[prov.login.localPassword]
VM Pilot Number	For Nortel and Avaya Call Servers you may want to provide the VM pilot number	[msg.mwi.x.callBack]
Subscribe To MWI	Some Call Servers require an extension to subscribe to get MWI (Avaya, for example). Enter the phone extension here if this is required.	[msg.mwi.x.subscribe]

<i>Setting column</i>	<i>What it is</i>	<i>Affects:</i>
QBC Target	If using phone in single end-point mode, this is the PC host name or static IP address the phone will connect to	[qbc.connect.ipAddress-hostname]
OAI Virtual MAC	If using User Profiles, the Virtual MAC to use as the OAI UserID An OAI Virtual MAC address is an 8 bit number unique for each phone. It often includes a base number then an offset equal to the extension. As example the number 12345678 is a unique number for one phone. The next phone could use 12345679. Another strategy for extension beginning at 4100 is for OAI Virtual MAC assigned as 12344100, then 12344102, then 12344102, etc.	[oai.userId]
Group parameters	If deploying Groups, you will need to establish which Group uses which parameter. Read through this document for more information about Group settings.	Push-to-talk channels, applications, and barcode settings are typical Group parameters.

Sample File for Listing Users and Parameters

Refer to the spreadsheet UsersList.xlsx in the zip with the template configuration files for organizing the handset assignments and parameter requirements. You will use this information when you provision the configuration files. If you have purchased installation, the installer will use this file to create the configuration files for your system

Chapter 3: Infrastructure

Provisioning a wireless handset is somewhat more complex than plugging a phone cable into a wall jack and getting a dial tone. You will need to establish a wireless infrastructure specifically designed for voice communications that takes into consideration the unique quality of service requirements of voice transmissions. Then you will need to consider the issue of communication security and decide which method is appropriate for your facility.

Network Components

Delivering enterprise-grade VoWLAN (Voice over Wireless Local Area Network) means that wireless networks must be designed to provide the highest audio quality throughout the facility. Voice has different attributes and performance requirements than wireless data applications making VoIP WLAN pre-deployment planning necessary.

A Wi-Fi handset requires a continuous, reliable connection as the user moves throughout the coverage area of the facility. In addition, voice applications have a low tolerance for network errors, packet retries and packet delays. Whereas data applications are able to accept frequent packet delays and retransmissions, wireless voice quality will deteriorate with just a few hundred milliseconds of delay or a very small percentage of lost packets. Additionally, data applications are typically bursty in terms of bandwidth utilization; whereas voice conversations use a consistent and a relatively small amount of network bandwidth throughout the length of a conversation.

This chapter covers the basic elements in a relatively simple system. Recommendations for your specific requirements are part of the service Spectralink includes with the installation of Spectralink wireless telephones. The following information will give you an overview of what each component does and how it is used by the wireless telephones.

Recommended Reading

Please familiarize yourself with documents that contain additional information about security methods and issues, including using Virtual LANs, MAC filtering and authentication, firewalls and traffic filtering.

All Spectralink documents are available at <http://support.spectralink.com>.

Best Practices for Deploying Spectralink 84-Series Handsets White Paper

For additional information about making security decisions, read *Understanding Wireless Security on Your Spectralink 84-Series Wireless Phones*

For full information about deploying the bar code feature of the Spectralink 8450/8452/8453, read *Spectralink 84-Series Wireless Telephone Barcode Administration Guide*

Quality of Service

The Spectralink 84-Series handset uses Wi-Fi Multimedia (WMM), WMM Power Save and WMM Admission Control mechanisms to deliver enterprise-grade Quality of Service (QoS). The use of WMM and WMM Power Save are required. You can disable WMM Admission Control in the access points if needed. However the use of all three WMM specifications is highly recommended by Spectralink and is the default operating mode of the handset.

Refer to *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephones*.

AP Configuration Guides show you how to correctly configure access points and WLAN controllers (if applicable) and identify the optimal settings that support Spectralink 84-Series handsets. The guides can be found at the View Certified page.

WLAN Security

Wireless technology does not provide any physical barrier from malicious attackers since radio waves penetrate walls and can be monitored and accessed beyond the wall even from outside the facility. The extent of security measures used is typically proportional to the value of the information accessible on the network. The security risk for VoWLAN is not limited to the typical wired telephony concerns of eavesdropping on telephone calls or making unauthorized toll calls, but is equivalent to the security risk of the data network that connects to the APs. Several different security options are supported on Spectralink 84-Series Wireless Telephones. Determining the proper level of security should be based on identified risks, corporate policy and an understanding of the pros and cons of the available security methods.

Security Methods

The security methods available for Spectralink Wireless Telephones are industry standard implementations used in typical Enterprise VoIP installations. The scope of this document does not include a complete analysis of security methods. Refer to *Best Practices for Wireless Security* for detailed information.

<i>Wireless Security Method</i>	<i>Security in Enterprise Environments</i>	<i>Audio</i>	<i>Ease of Configuration and Other General Information</i>
WEP	Poor	Excellent	Easy to administer, little processing overhead, adequate security for many home Wi-Fi networks. Easily compromised with hacking tools readily available on the internet. Every phone can decrypt every other phone's data. Still in use on some older enterprise networks.
WPA-PSK	Acceptable	Excellent to Good	Acceptable security for many small business Wi-Fi networks. Each phone negotiates a key (see TKIP below) with the AP so phones can't decrypt each other's data, although a sophisticated hacking device that

<i>Wireless Security Method</i>	<i>Security in Enterprise Environments</i>	<i>Audio</i>	<i>Ease of Configuration and Other General Information</i>
			knows the PSK can decode anyone's traffic. The problem can be minimized with periodic rotation of long, hard-to-hack passwords.
WPA2-PSK	Acceptable to Good	Excellent to Good	Good security for most small business Wi-Fi networks. Similar to WPA with the addition of AES/CCMP, one of the most secure encryption algorithms available. The PSK limitation is still an issue, however.
WPA2-Enterprise ¹	Excellent	Excellent to Poor	Excellent security for enterprise Wi-Fi network. PSK is replaced by some form of EAP and a RADIUS server, and each phone is configured with its own username and password, making the conversation between phone and AP completely private. The processing requirements of a RADIUS server, however, can compromise handoffs, so a fast-roaming technique such as OKC or CCKM must be employed.

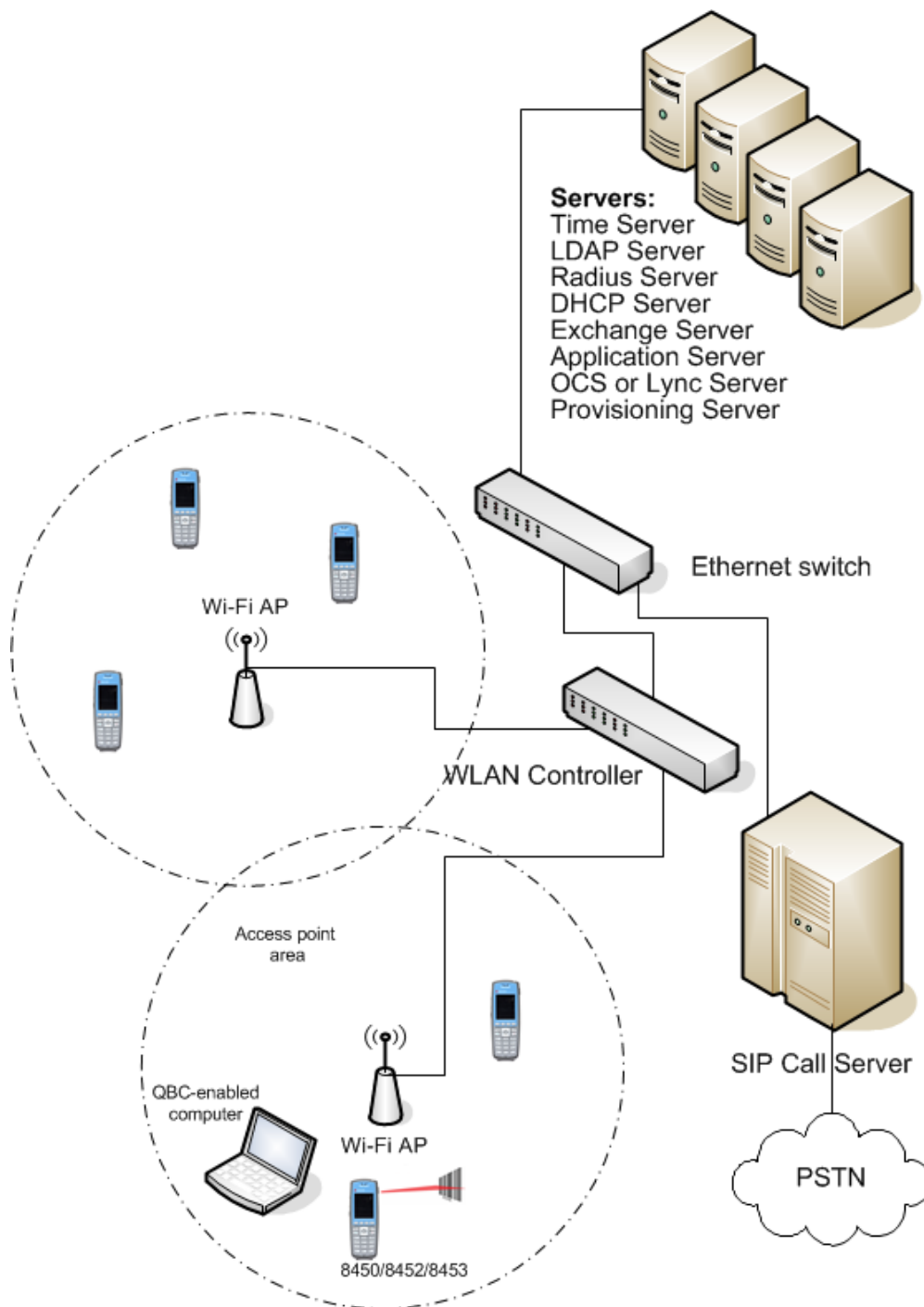
¹ WPA2-Enterprise variables:

84-Series handsets use authentication types: EAP-TLS, EAP-FAST or PEAPv0 with MSCHAPv2. EAP-TLS uses a certificate to authenticate both the device and server. EAP-FAST is used by products of Cisco, its creator, and by a growing number of other WLAN vendors. It uses a PAC file, which is similar to a certificate. PEAPv0 with MSCHAPv2 is the most common form of PEAP, which uses a certificate to authenticate the server.

84-Series handsets use either of two fast-handoff techniques as they roam among APs: CCKM or OKC. CCKM is used exclusively by Cisco APs. OKC is used by most non-Cisco APs.

System Diagram

The following diagram shows the Spectralink components residing on a typical network with APs and wireless LAN Ethernet Switch.



**Tip: Are multiple servers necessary?**

Sometimes a single piece of hardware may provide multiple services, for example some AP controllers can also provide radius services. Consult your service provider for more information about how to tailor your system configuration for your requirements.

System Requirements

A typical installation requires the following components:

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

Optional components:

- OCS or Lync Server
- Exchange Server
- LDAP Server
- Application Server

System Components

Spectralink 84-Series handsets.

Available in several models, the 84-Series handsets provide essential communication resources for facility wide implementation. Each model has a unique hardware ID that is printed on the label.

Handset hardware ID numbers

<i>Model Name</i>	<i>Hardware ID</i>
SL8440	3111-36150-001
SL8450	3111-36152-001

<i>Model Name</i>	<i>Hardware ID</i>
SL8452	3111-36154-001
SL8441	3111-67360-001
SL8453	3111-67361-001

8440

The basic model that includes basic and advanced wireless telephone features.

8441

An accelerometer has been added to the 8440 that enables it to utilize the Personal Alarm feature.

8450

The features of the 8440 model plus barcode scanning for 1D scanning for use with or without the Quick Barcode Connector application.

8452

The features of the 8440 model plus barcode scanning for both 1D and 2D scanning for use with or without the Quick Barcode Connector application.

8453

An accelerometer has been added to the 8454 that enables it to utilize the Personal Alarm feature.

Servers

Provisioning Server

A provisioning server is required to distribute firmware and configuration files to the handsets after they connect to the WLAN and network. The Spectralink 84-Series Wireless Telephones support FTP, TFTP, HTTP, HTTPS (for security) and FTPS provisioning servers for provisioning the phones. FTP is the default protocol and this document explains how to use the FTP option. The provisioning server may be on a different subnet than the APs and/or handsets.

Time Server

Simple Network Time Protocol Server or SNTP server. When WPA2 Enterprise security is used, the handset will use this data to confirm the PAC or certificate has a valid date and time. If an NTP Server is not available, the certificate will be assumed valid and operate accordingly, without the date and time check.

RADIUS Server

A RADIUS authentication server must be used to provide username/password-based authentication using RSA certificates for EAP-TLS, PEAPv0/MSCHAPv2 or PAC files for EAP-FAST.

The following authentication servers have been validated for use with Spectralink 84-Series handsets:

- Juniper Networks Steel-belted Radius Enterprise Edition (formerly Funk), v6.1
- Microsoft® Internet Security and Acceleration (ISA) Server 2003, Windows 2008 NPS
- Cisco Secure Access Control Server (ACS), v5.2, 4.1
- FreeRADIUS v2.1.10, 2.0.1 and 1.1.7

Other RADIUS servers may work properly with Spectralink handsets, but have not been tested. Inquiries on untested servers will receive limited, “*Best Effort*”, support.

DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, subnet mask, default gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data, and are configured by network administrators with settings that are appropriate for a given network environment. The handset will use the DHCP options shown in the following table if DHCP use is enabled. The DHCP setting will usually take precedence if it is set and if it is available but can be overridden by certain parameters.

Option	SIP Parameter	Meaning
1	NA	Subnet mask
3	NA	Default gateway
6	DNSSVR	DNS server
7	LOGSRVR	Syslog server logging
15	DOMAIN	Domain name
42	SNTPSRVR	NTP Server
43	sec.TLS.customCaCert.x	Auto discovery of the root CA certificate. If this setting is unavailable, set the parameter per this guide.
66	TFTPSRVR	TFTP server

Consult with your service provider if you choose to use static configuration.

SIP Call Server

The call server provides SIP telephony support.

Access points

Enterprise-grade Wi-Fi access points provide the connection between the wired LAN and the wireless LAN. VIEW Certified APs must be positioned in all areas where Spectralink handsets will be used to ensure seamless radio coverage. The number, type and placement of access points will affect the coverage area and capacity of the wireless system. Careful planning of the WLAN is necessary to ensure excellent voice quality. An 'optimized for voice' WLAN will yield great benefits to the wireless telephone user community.

APs must be properly configured to support the corresponding QoS and security methods selected for the 84-Series handset.

Ethernet switch

One or more Ethernet switches interconnect multiple network devices. Enterprise Ethernet switches provide the highest performance networks, which can handle combined voice and data traffic, and are required when using the Spectralink 84-Series Wireless Telephones.

Ensure the WLAN and network infrastructure provides connectivity from the wireless telephone to all its required network resources (SIP Server, etc.) once the 84-Series handset connects to the network and obtains an IP address.

Spectralink 84-Series Wireless Telephones cannot roam with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a Layer-3 tunnel across subnets that enable the handsets to roam. Without this capability, any call in progress will be dropped when the user moves out of range and the handset must be power cycled in order to resume functionality in the new subnet area. Consult your AP vendor document for more information about Layer 3 tunneling.

If you do not have Layer 3 capability, ensure that the SSID your phones associate with uses the same subnet on all APs for proper operation.. The handset can change subnets if DHCP is enabled and the handset is powered off then back on when within range of APs on the new subnet. Note that the wireless telephones cannot "roam" across subnets, since they cannot change IP addresses while operational.

Chapter 4: Understanding Wireless Telephony Provisioning

The Spectralink 84-Series Wireless Telephone is a Wi-Fi device that provides users with a wireless extension to the SIP call server. By seamlessly integrating into a SIP environment, wireless telephone users are provided with high-quality mobile voice communications throughout the workplace, giving users the freedom to roam throughout the workplace while providing all the features and functionality of a wired SIP desk phone.

Three provisioning methods exist; the central provisioning server, the Spectralink Installation & Configuration Tool (SLIC), and the local phone user interface. Only the central provisioning server method can provision all settings. The SLIC tool provides wizards that help you configure the parameters that allow the handset to associate with the wireless network and configure the most frequently-used SIP configuration options. The local phone interface does not offer every setting and is tedious to administer when deploying any number of phones. This document explains how to use a central provisioning server to configure and deploy the Spectralink 84-Series handsets. Find out more about the SLIC tool in Chapter 1: [Quick Start with SLIC](#) and from the *Spectralink Installation and Configuration Tool Administration Guide*.

What is Provisioning?

Instead of painstakingly going through the menus on each phone to set required parameters, parameters are programmed on a central provisioning server and delivered over the air to all Spectralink 84-Series handsets in the system.

The provisioning concept is essentially very simple: programmable parameters configure hardware settings and implement features. The parameters are enabled or disabled and given a value or values as applicable. These parameters are contained in configuration files or .cfg files that are configured by the system administrator and reside on a provisioning server. There can be only a few or many .cfg files for each 84-Series handset, as determined by the system administrator.

The strength of the Spectralink provisioning mechanism and also its challenge is that the system administrator has the flexibility to manipulate a large number of parameters to implement the unique requirements of any given installation. A beginner can find that building configuration files and setting up a provisioning system is a daunting task, especially in a robust implementation with 3,000 parameters that offer every possible communication system feature.

Therefore this document suggests certain guidelines that, if followed, will give even an inexperienced administrator a successful implementation. This document does not presume to cover every possible feature or every setting in any given feature. It covers the most commonly used features. Once those features are configured and working, the remaining features and

settings can be addressed with increased confidence by the telephony administrator by referring to more advanced references. The configuration process outlined in this document provides a basic structure upon which more complex features may be provisioned and deployed.

The Provisioning Process

Usually a laptop or other easily-accessible PC is used to configure all the .cfg files. It also functions as the initial provisioning server to download the wireless files to the phones using a microB USB cable. Files destined for the central provisioning server are also configured on the laptop and then transferred to the central provisioning server either over the network or by a jump drive or other method.

Deployment itself is a two-part process: First the wireless file is downloaded into each handset through MicroB USB cable and then the handset is able to access the configuration files on central provisioning server.

The provisioning process as described in this document goes through this recommended sequence:

- 1** Configuration of the parameters for the central provisioning server according to the deployment scenario selected.
- 2** Setting up the central provisioning server:
 - a** The central provisioning server uses a file transfer protocol such as FTP and it must be set up for this.
 - b** The central provisioning server must have a specific file structure to store and manage the files that it delivers to and receives from the wireless telephones. This structure must be established.
- 3** Loading the files onto the central provisioning server.

Ensure that the files are on the central provisioning server before powering up the phones. This is so that once they connect to the central provisioning server through the wireless and wired LAN, they can retrieve the files they need and are immediately operational.
- 4** Configuration of the wireless parameters.
- 5** Setting up the initial provisioning server as an FTP server.
- 6** Downloading the wireless files onto the phones.

The wireless configuration files need to be loaded into the phone before it can access the wireless LAN and request the rest of the configuration files from the central provisioning server. Until its initial configuration is loaded (using a MicroB USB cable) the 84-Series handset will not connect to the WLAN or network.

After the file transfer is complete between the initial provisioning computer and the 84-Series handset, the USB cable can be disconnected and the next phone can get

started. Meanwhile, the handsets that have been loaded are busy associating with the wireless LAN, finding the central provisioning server and obtaining the rest of the configuration files. Once it has all these files, it is fully provisioned and may be tested and deployed anywhere in the facility.

7 Testing and correcting.

Always deploy a few phones first to make sure that all the configuration parameters were done correctly and they operate as desired.

8 Full deployment.

Once the few test phones work as desired, download the wireless files to the rest of the phones per step 6.



Settings: Sequence variations

This document covers the configuration of the central provisioning server files first. You could just as easily configure the wireless files first. In some situations, it is desirable to deploy test phones wirelessly first to verify those settings before setting up the central provisioning server. If you have any questions, please contact a Deployment Specialist to direct you through this process.

Managing Configuration Files

Although configuration (.cfg) files can be set up in many different ways, for ease of explanation and uniformity of implementation, we recommend using specific names in a specific structure. If you purchased onsite installation support, similar files are already installed in your system. If you are going to deploy the handsets yourself, follow the instructions in this Guide to build your own configuration structure.

Before the handset is configured, it is a blank slate. It does not know who or what it is or what it is supposed to do. Its identity is its MACaddress, a network machine number assigned to it at the factory which is printed on its label. The .cfg files will provide it with the parameters it needs to associate with the wireless LAN using an IP address, link a name and/or extension to the IP address, and provide many telephony parameters so that it functions correctly in your facility.

Viewing the .cfg File Templates

As you move through the configuration process, you will be opening and configuring parameters in several different .cfg files. The template files form building blocks for further customization. Once you become familiar with the process and organization, you can use them to devise the structure that suits your deployment.

Where are the Templates?

You will find 84-Series configuration templates that match the recommendations in this Guide bundled with the handset software. Download the software zip to any convenient location for now. Extract the files. The templates are located in the Config folder. The other files in the software zip are explained in [Downloading Spectralink 84-Series Software Files to the Central Provisioning Server](#).



Config folders on the Web

From time to time a revised Config folder may become available in the Downloads area on the website.

Configuration Folder Contents

Once extracted, the folders and files in the Config.zip are a complete set of all the parameters available to you. They are arranged in a structure so that you can easily identify the files you will need.

Each of these folders and files is explained in Part II Configuration.



Admin Tip: Different templates for Lync and non-Lync

SIP telephony requirements are different from Lync telephony requirements. Therefore you will see different scenario configuration files for the Lync and SIP software loads. They have the same name, but different telephony parameters. Please use the templates that come with your software version for best results.

Features folder	
	barcode.cfg
	directory.cfg
	oai.cfg
	PersAlarms.cfg
	ptt.cfg
	RTLS.cfg
Scenarios folder	
	Flat_Deployment folder
	00000000000000000000.cfg
	site.cfg
	MACAddress-ext.cfg
	Group_Deployment folder
	MACAddress.cfg
	site.cfg
	group.cfg
	identity.cfg
	User_Profiles_Deployment folder
	00000000000000000000.cfg
	site.cfg
	login.cfg
Troubleshooting folder	
	logging.cfg
	everything.cfg
USB_Setup folder	
	00000000000000000000.cfg
	wireless.cfg
00000000000000000000-directory~.xml	

What is the *schema* file?

The *schema* file is named handsetConfig.xsd and it contains all parameters and their valid values and is used in verifying the correctness of .cfg files, the parameter values, and in troubleshooting. It is located in the root area of the provisioning server to ensure it is readily available when needed.

Viewing and Editing .cfg Files

In order to view, edit and create the configuration files, you will need to use an XML editor. Many XML editors are available. Here are a few to consider.

The XML editor used in the screen shots in this document is a free editor provided by Microsoft, *XML Notepad*. The value of this program is its tree view GUI which provides an easy way to create, edit and view XML files. It also verifies the XML structure of files created by a text editor

and provides errors if the structure is incorrect. The downside is that it can corrupt the lengthy security certificates used by our phones and the GUI may not be that easy to work with. It may also remove hierarchical structures of XML files created in a text editor if it is used to edit the file, leaving the text file more difficult to view.

XML Notepad can be downloaded from this site:

<http://www.microsoft.com/en-us/download/details.aspx?id=7973>

If you are using security certificates, we recommend that you use a text editor such as *Notepad++*. *Notepad++* is a text editor that uses colors to emphasize the XML structure. The XML Plugin must be downloaded and installed so that it works correctly. This editor has been found to maintain the integrity of the security code which may become corrupted with other XML editors. However, you need to be conversant with XML code to use this editor as it has no GUI. *Notepad++* is free and available at this site:

<http://notepad-plus-plus.org/>.

XML Marker by Symbol Click is a free text editor which may prove useful for file viewing. It shows both the text view and the GUI tree view. Edits are done in the text view so you need to be conversant with XML code to use this editor successfully. It may have field limitations which makes it unworkable for editing if you use lengthy certificates.

XML Marker is available at:

<http://symbolclick.com/>.

Foxe is an editor from First Object that shows the tree view and text view and allows you to make edits in either. It apparently does not have the field limitations of XML Notepad so you could use it if you have lengthy certificates.

Foxe is free and available at:

http://www.firstobject.com/dn_editor.htm



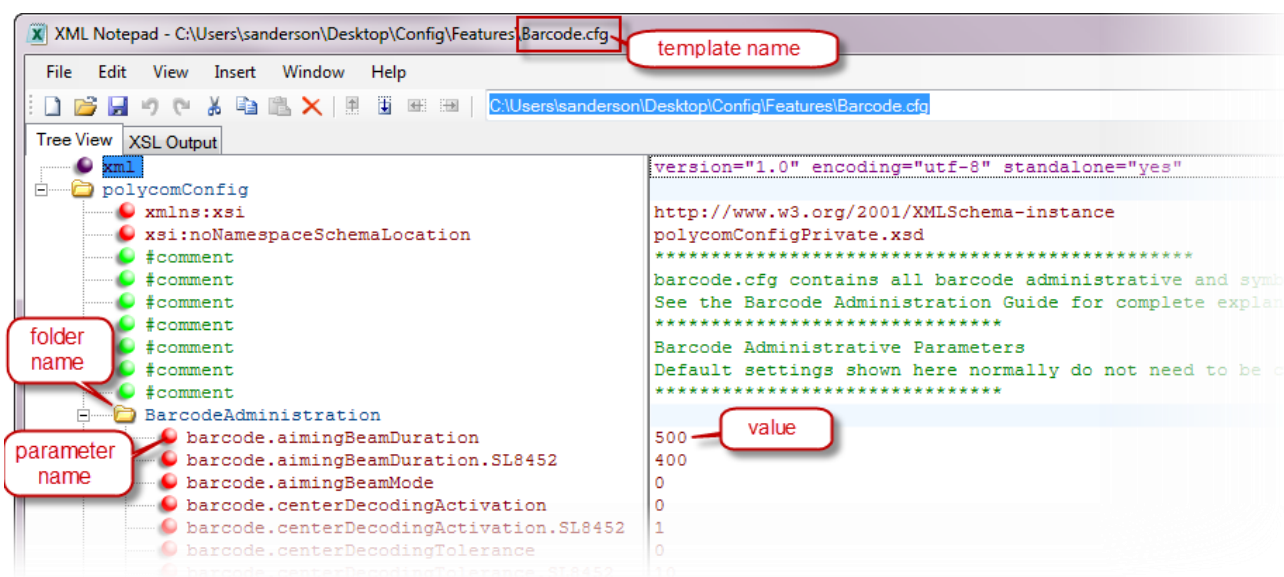
Tip: How to view and edit files when you use security certificates

If you use a text editor to edit the .cfg files, check them for errors in an XML editor such as XML Notepad. However, if you use XML Notepad to change the file, you will destroy the hierarchy and when you open it in the text editor the attributes of a tag will be in one long line instead of neatly separated.

Therefore we recommend that you use the text editor for editing and the XML editor for viewing and checking. If you are not using security certificates, you can use XML Notepad or one of the other GUI editors for both viewing and editing.

Please download and install an XML editor so you can follow along with the rest of this document.

Example .cfg file with both tree view and text view displayed



The above example shows a portion of the barcode.cfg file, a feature template that contains the barcode parameters. You can see the screen has two parts, the “tree” view is on the left and text and values are on the right. The first few rows contain necessary XML stuff that you can safely ignore. The comments in green provide important information about the file and how to use it.

The folder and parameter structure start below the initial comments. The folder names are somewhat explanatory about the type of parameter they contain. The parameters use a nested structure to organize and differentiate them. In this example, all barcode parameters start with “barcode.” and then have descriptive text to explain the parameter. The values are set on the right side. In many cases, default values are shown. Any value shown on the right can be overwritten.

Sometimes comments are interspersed with parameters. Comment text is positioned before the related parameters. Read them for critical information about the parameters to follow.

Different XML editors use different editing tools. For the most part, you can drag-and-drop, copy and paste, open and save in the usual way but you may need to practice with the xml tools you select.

Creating New .cfg Files

Unless you are an expert with XML, you will find it easiest to create new .cfg files by opening an existing file and saving it as a new name. The templates are designed to make this easy so that usually only a few values need to be changed to customize the file. Some filenames must be very specific and you will find precise naming instructions in the configuration sections in Part II.

When you need to refine the .cfg files to suit your own requirements, parameters can be copied from sample files provided with the downloaded code and pasted into the files you have developed for this initial deployment. Or you may decide to establish your own feature structure by locating the parameters you wish to modify in one of the sample files, editing the contents accordingly and saving it with a file name that conforms to your file structure strategy.

**Power Tip: Automating the configuration process**

Deployment Specialists use a custom batch process to automatically generate the per-phone files.

Types of .cfg Files

Configuration files are basically differentiated by the number of phones that use the parameters set in the file.

Top Level .cfg Files

When the phone locates the central provisioning server, it first looks for a file with its MACaddress as the filename, such as 00907a0cd967.cfg. If it does not find this file, it will look for the master configuration file, 000000000000.cfg.

Either one of these two top level files will direct the phone to:

- The phone's software which is usually loaded into the root directory of the central provisioning server.
- Configuration files that contain the parameters it needs.
- Directory information that tells the phone where to upload and find information on the central provisioning server.

The two top level files serve identical purposes but which one is utilized depends on which scenario you select. The value of the MACaddress file is that it is unique for each phone and is necessary when you need to direct specific phones to specific files such as recommended for groups and is therefore used in Group Deployment. The master configuration file is used for the Flat and User Profile Deployments.

The only parameters you might need to change in either one of these files are the APP_FILE_PATH, CONFIG_FILES and the DIRECTORIES if you choose to configure them.

APP_FILE_PATH

The APP_FILE_PATH directs the handset to its application file. The default value for the lync software is lync.ld. The default value for the standard software is sip.ld. These identifiers are also included in the software firmware filenames for the two different versions.

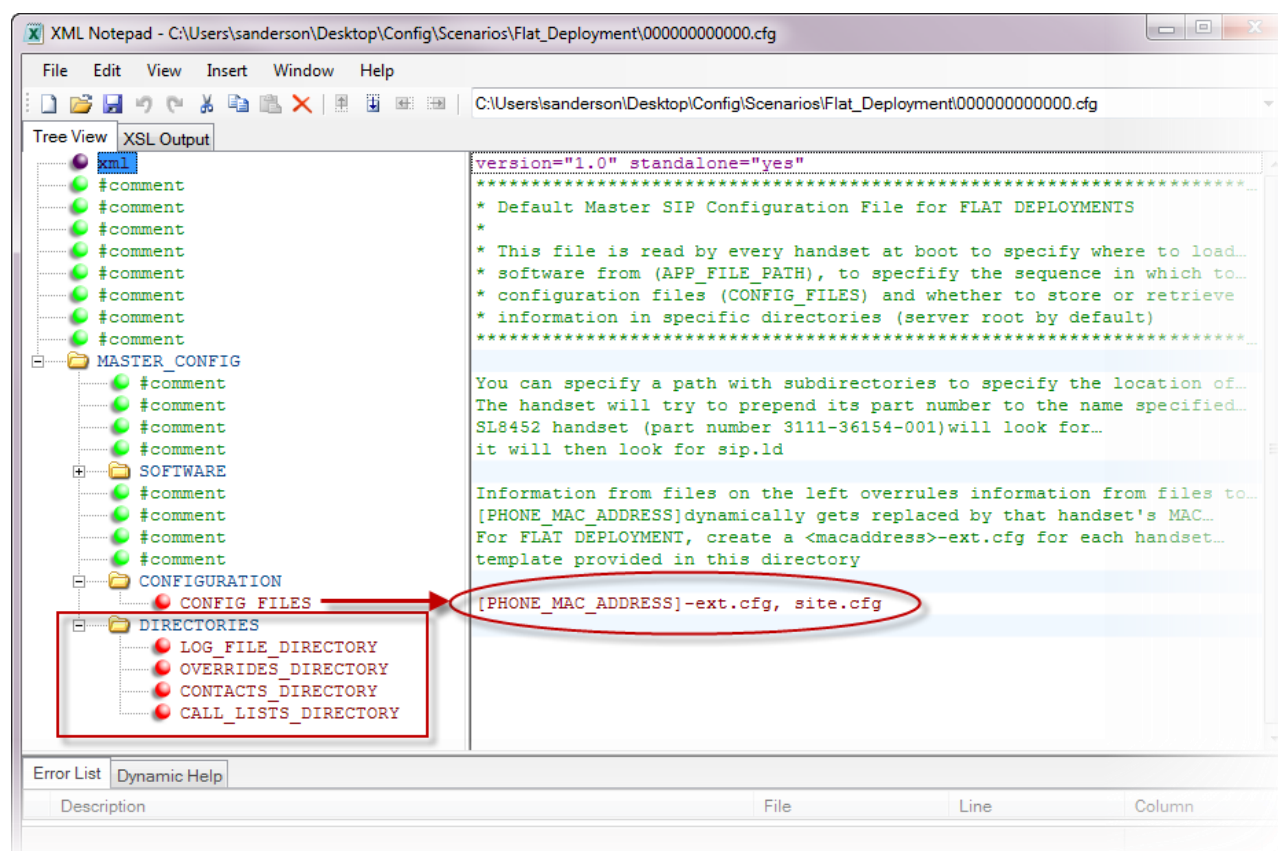
How the Handset Finds the Software

When a phone running 4.3.0/4.4.x or later software boots, it will automatically look for the `slink84xx.sip.ld` or `slink84xx.lync.ld`. This is a hardcoded filename that is not dependent on the `APP_FILE_PATH` parameter in the `000000000000.cfg` or `[MACaddress].cfg` files.

However, if the `APP_FILE_PATH` parameter is deleted, then the phone does not look for any files and uses whatever software is already on the phone. This is pre 4.3.x behavior.

If the phone cannot find the `slink84xx.sip.ld` or `slink84xx.lync.ld` file it will look for a filename using the same algorithm as pre 4.3.x software. For example, an 8440 phone will look for a file named `3111-36150-001` pre-pended to the value of `APP_FILE_PATH`. If that file can't be found, then it looks for `APP_FILE_PATH` as a standalone file.

Example 000000000000.cfg file for FLAT Deployment



CONFIG_FILES

The `CONFIG_FILES` parameter lists the configuration files that the phone needs to find for its operational parameters. In the Flat Deployment screen example, a variable `[PHONE_MAC_ADDRESS]` in the filename directs the phone to its per-phone .cfg file. For Flat Deployment when you create the individual per-phone files, they must be named with the phone's MACaddress plus a `-ext`, such as `00.90.7A.0C.D9.67-ext.cfg`.

Notice the `site.cfg` file in the `CONFIG_FILE` list. The `site.cfg` file is present in all deployment scenarios. It holds system and telephony parameters that are common to all phones.

The config files used by the different scenarios are covered in more detail later in this chapter.

The order that the `.cfg` files are listed determines the order in which the phone will obtain its parameters. The first time the phone gets a parameter is the value it will use. If the same parameter occurs in a later file, it will be ignored. In our example, you can see that the per-phone file is first in the sequence of `.cfg` files which means that the parameters set in this file will take precedence. We recommend deleting duplicate parameters to avoid conflicts and confusion.

DIRECTORIES

The top level file can contain directory information that tells the phone where to store and find certain information such as logs and overrides. Without setting up these separate directories, the phone will put all the information into the root folder on the central provisioning server, making it very large and very difficult for an administrator to find data. We recommend that you set up these file paths here and set up a corresponding file structure on the central provisioning server as explained at the end of this chapter.

The template provides a directory parameter but does not have any values set. Here is an example of named directories:

LOG_FILE_DIRECTORY	\Log_Files
OVERRIDES_DIRECTORY	\Overrides
CONTACTS_DIRECTORY	\Contacts
CALL_LISTS_DIRECTORY	\Call_Lists
USER_PROFILES_DIRECTORY	\UserProfiles

- **LOG_FILE_DIRECTORY** This is the directory where the phone will write its log files.
- **OVERRIDES_DIRECTORY** Parameters set in the `.cfg` files can be overridden when changed in the Web Configuration Utility or in the phone menus using its keypad. This directory stores these overrides by MACaddress so that they are available when the phone restarts.
- **CONTACTS_DIRECTORY** Contacts are stored by MACaddress in this directory as a backup so that they can be reloaded when the phone reboots.
- **CALL_LISTS_DIRECTORY** Call lists are stored by phone or by User Profile.
- **USER_PROFILES_DIRECTORY** . The individual User Profile login.cfg files are stored here.

General-to-Specific Criteria

Aside from the top level `.cfg` files, other criteria establish additional types of `.cfg` files. The template `.cfg` files are arranged according to how many phones are affected by the parameters in the file:

- General settings: system wide settings are set in the site.cfg file,
- A few phones: features can be deployed that apply only to certain groups,
- A specific phone (or user): extension information is set in a per-phone file.

**Admin Tip: Lync Telephony Server Variation**

The .cfg files provided by the software include a per-phone file for each scenario. If you are using a Lync telephony server, you may not need to configure these files because the Lync server already knows about them. See the chapter on telephony server variations for more information if you are using a Lync telephony server.

Flat Deployment

In a Flat Deployment, each phone is deployed to a specific extension and all phones have similar parameters. In this deployment, phones are typically linked to extensions which are then assigned to users. You will need to create one .cfg file for each extension/user, unless you are using a Lync telephony server. See Chapter 5: Telephony Server Variations.

In our example, these three files are provisioned:

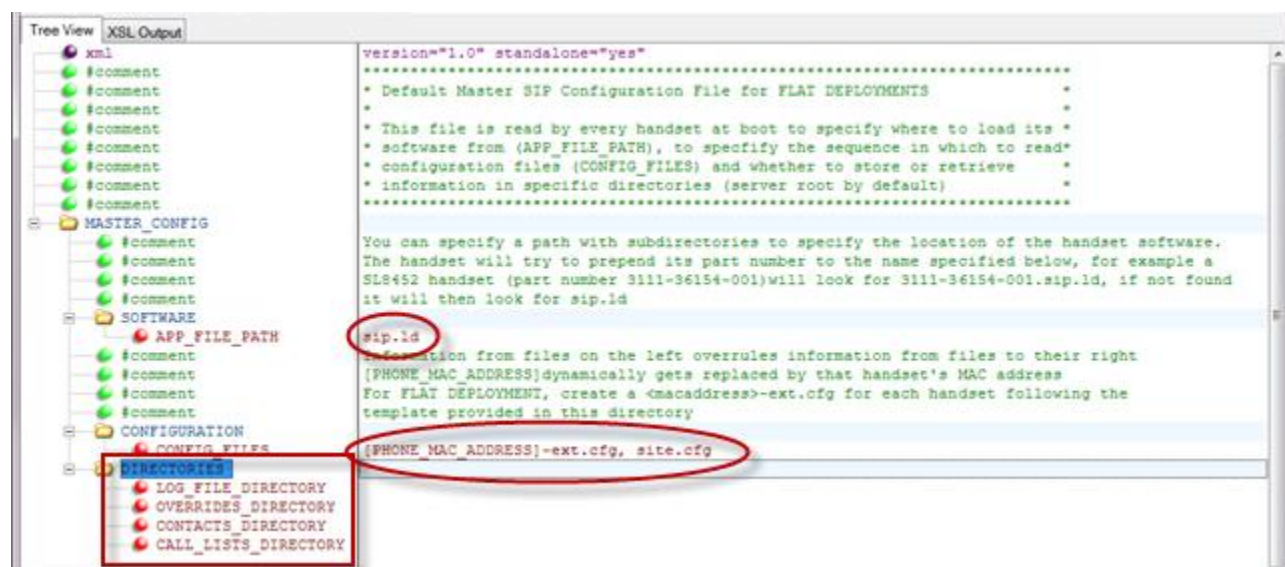
- 000000000000.cfg
- Site.cfg
- <MACaddress>-ext.cfg (one file for each extension/handset)

000000000000.cfg

When provisioning a flat deployment, you will use the default master template file (000000000000.cfg) to direct the handsets to other cfg files it will need.

In the Flat Deployment scenario, you only need two files, the per-phone file and site.cfg which holds all the system and feature parameters you will deploy.

We recommend that you specify directories.



In this scenario a variable is used—[PHONE_MAC_ADDRESS]—to direct the handset to its own phone-specific MACAddress .cfg file.



Admin Tip: Naming the phone-specific configuration file

The [PHONE_MAC_ADDRESS]-ext.cfg file uses a variable to point to the MACAddress files you create for each phone/extension. The '-ext' part of the filename used in this document is not necessary or could be replaced by some other identifier. The important thing is that whatever identifier you use here is also used on each of the MACAddress files you create for each phone.

Do not use the following file names as your per-phone file name:

<MACAddress>-phone.cfg,
 <MACAddress>-Web.cfg,
 <MACAddress>-app.log,
 <MACAddress>-boot.log, or
 <MACAddress>-license.cfg.

These file names are used by the phone itself to store user preferences (overrides) and logging information.

Site.cfg

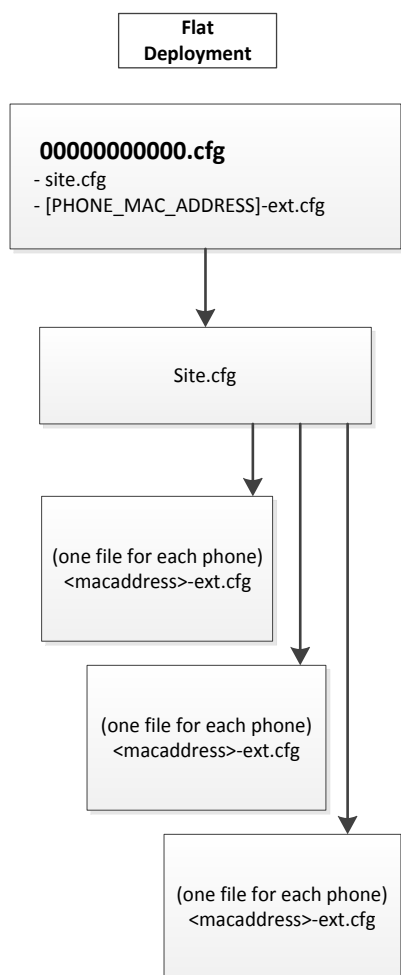
The site.cfg template contains most common parameters including network and telephony information that pertains to all of the handsets, such as SIP servers, dial plan, etc.

MACAddress-ext.cfg

You must create a specific <MACAddress>-ext.cfg file for each phone/extension you deploy. The User spreadsheet you completed that lists each extension/user and the MACAddress of the phone assigned to that extension will help you create these files.

These files must be named with the identical structure as the variable used by the phone to find it. Therefore when the variable [PHONE_MAC_ADDRESS]-ext.cfg is used, the phone-specific files must be named <MACAddress>-ext.cfg.

You will use the MACAddress-ext.cfg template to create the files for each extension/user. It contains the most common parameters, including network and telephony information, that pertain to all of the handsets, such as SIP servers, dial plan, etc.



Group_Deployment

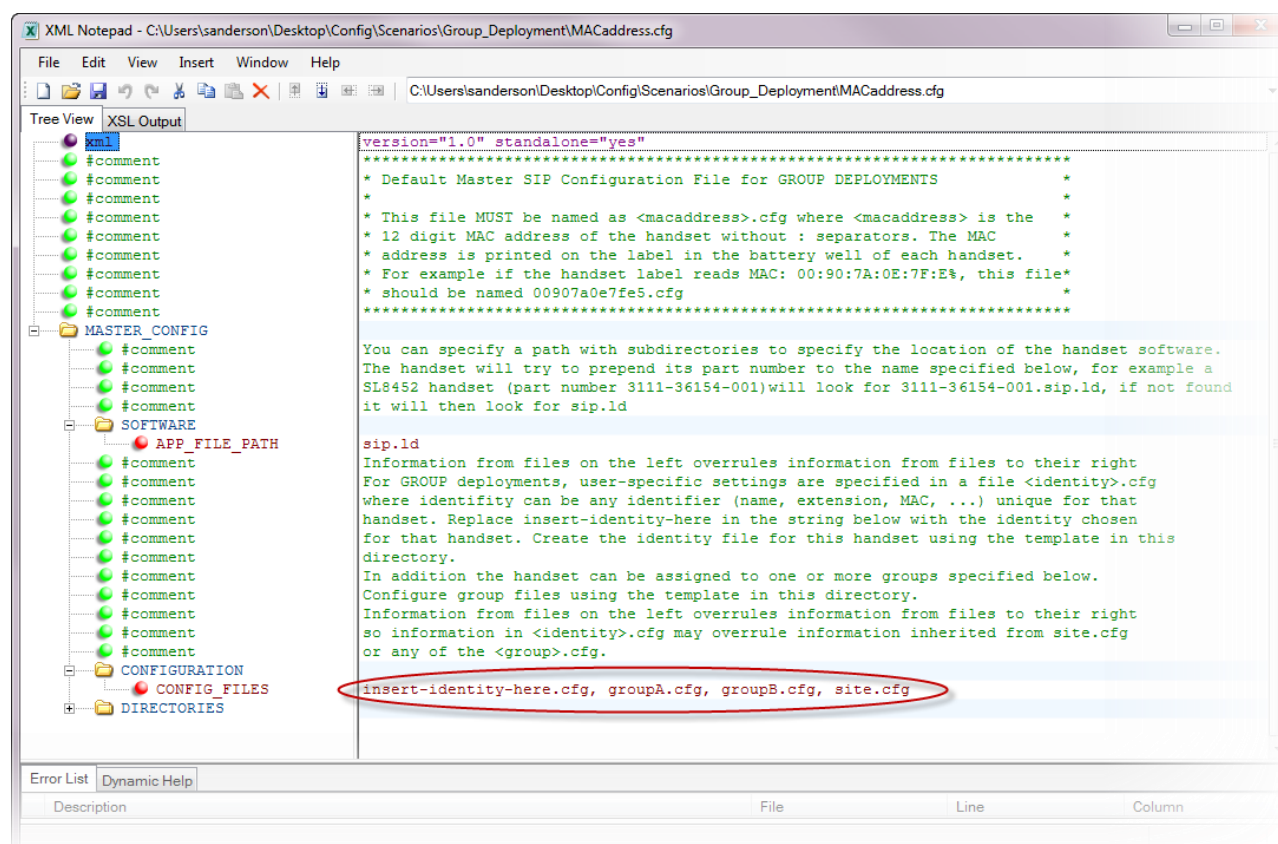
Group deployment is more complex than Flat deployment but far easier to manage if you need to differentiate users into groups. In this deployment, you will need to create a <MACAddress>.cfg file for each phone. During deployment, the phone looks for this file and uses it for direction to other .cfg files. Having individual MACAddress files as the first step (instead of using the generic 000000000000.cfg file) allows you to direct the handset to a specific Group.cfg file and then to its individually named identity-specific file. These files can be named with the extension number such as 3033.cfg or with the identity of the user such as JohnDoe.cfg or Clerk01.cfg. Note that you do not have to assign every user to a Group. You can have a generic user type that does not belong to any Group and these users will use the site-wide parameters in the site.cfg file. In our example, these templates are used:

- MACAddress.cfg
- site.cfg
- group.cfg
- identity.cfg

MACAddress.cfg

When using Groups, you need to create a <MACAddress>.cfg file for each phone. During deployment, the phone looks for this file and uses it for direction to other .cfg files that have been configured to be used by this specific handset. In our example these are Site.cfg, GroupABC.cfg and <identity>.cfg.

Example screen for MACAddress.cfg, the top level .cfg file for Group Deployment



In the example screen the `CONFIG_FILES` use descriptive filenames for the per-phone .cfg file and the group.cfg files.

Site.cfg

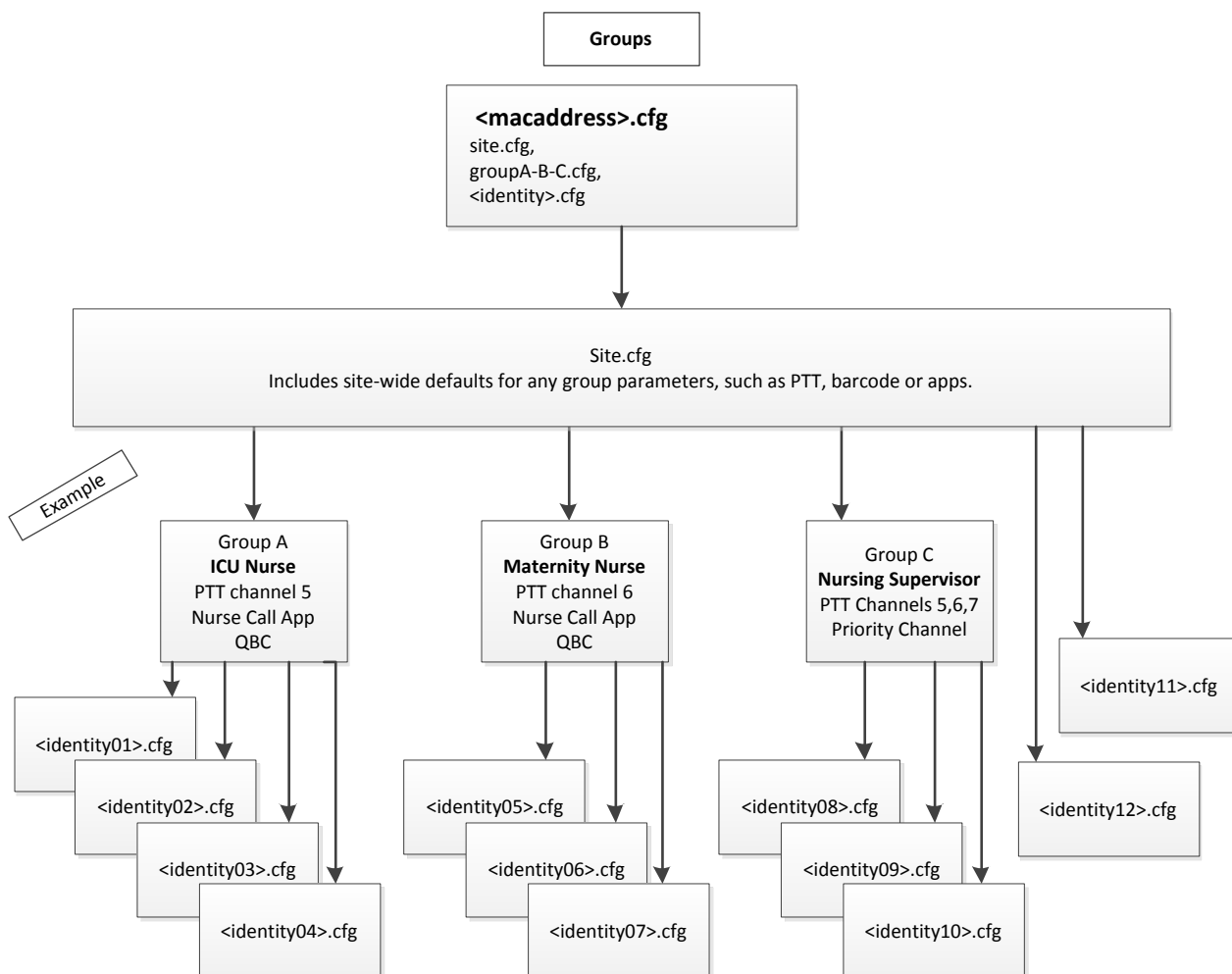
The template that contains most common parameters including network and telephony information that pertains to all of the handsets, such as SIP servers, dial plan, etc.

Group.cfg

When using Groups, you will need to create a Group.cfg file for each group you deploy. Replace "Group" with the name of the Group. Such names usually reflect the group's function such as `ICUnurse.cfg` or `HardwareDept.cfg`. See the sample spreadsheet for an example of what type of parameters are typically deployed for Groups.

identity.cfg

You will need to create a specific `<identity>.cfg` file for each handset you deploy to a specific extension. Typically this file is named for the extension assigned to the user, such as `3033.cfg`.



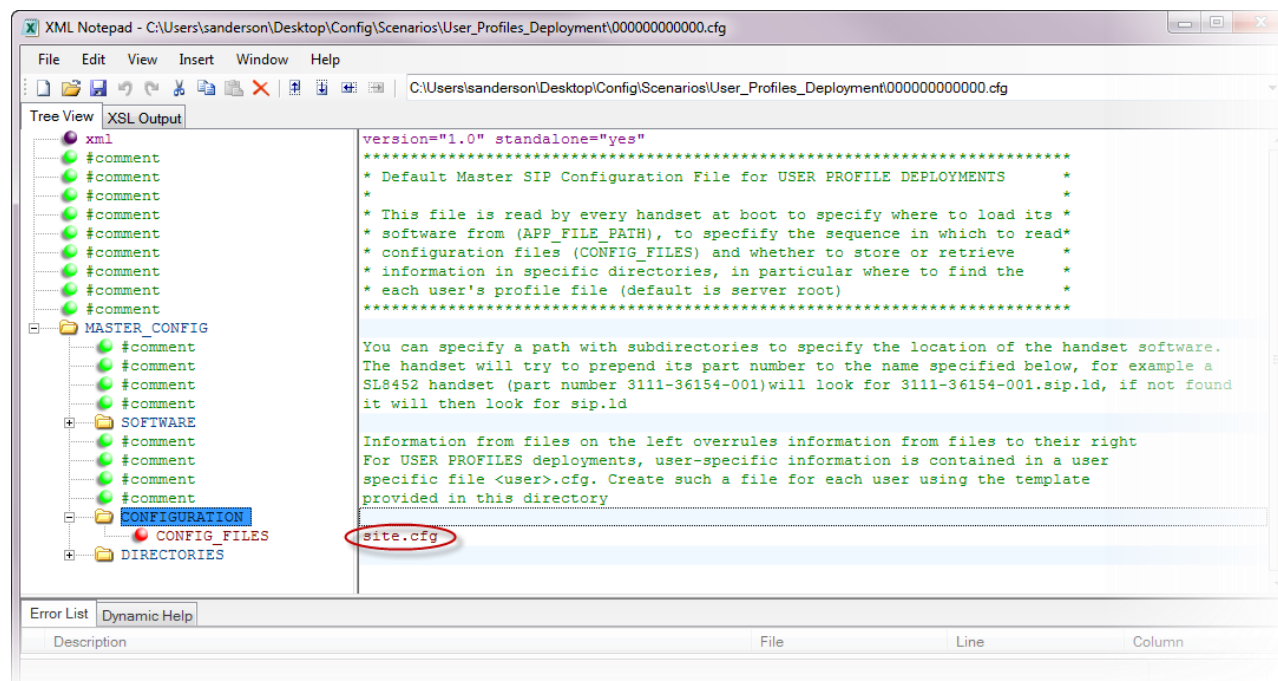
User_Profiles_Deployment

In a User Profiles deployment, the master configuration file 000000000000.cfg is only used to point to the site.cfg file which contains the requirement for the user to log on in order to access the phone's features. Since User Profiles are not linked to individual handsets, the phone specific file is not referenced in the master configuration file. This deployment is also known as "basket of phones" where any phone can be selected out of a supply and used by anyone who has log on credentials. You need to create a file for each User Profile. The name of the file is the user's login name and the password is stored in the <login>.cfg file.

Because phones are not linked to extensions, User Profile information is stored on the central provisioning server instead of in the handset's memory. Server files are discussed in Chapter 7.

000000000000.cfg

When deploying User Profiles, you will use the default master template file (000000000000.cfg) which directs the handsets to the site.cfg file. The login.cfg file is not referenced.



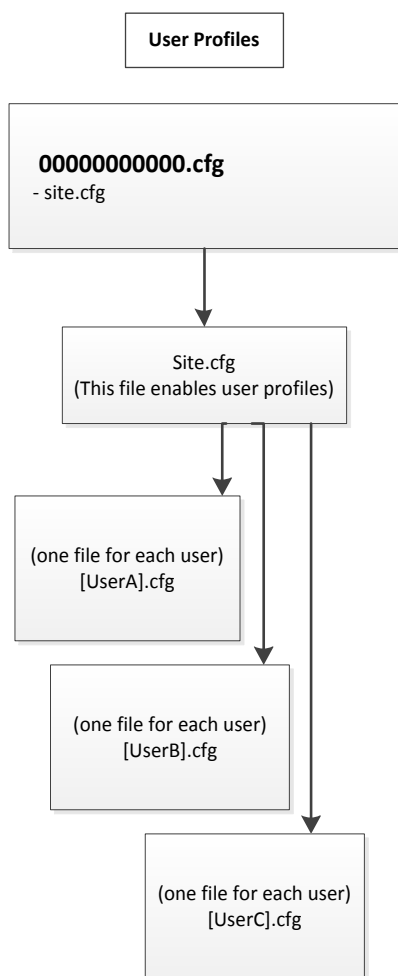
site.cfg

The template that contains most common parameters including network and telephony information that pertains to all of the handsets, such as SIP servers, dial plan, etc.

This file also contains the log on requirements for User Profiles.

login.cfg

If you are using User Profiles, you will need to create a separate .cfg file for each user that provides login information and preferences specific to that user. These files are often named psmith.cfg (for pauline smith) or 1100.cfg (for extension 1100). User Profiles allow you to create many more separate .cfg files for individuals or extensions than you have physical phones to deploy.



Features Deployment

Features files can be used as a resource to drag-and-drop parameters into other files or they may be used as feature deployment files by directing the handset to them in the 000000000000.cfg file or MACaddress.cfg file.

The Features folder contains cfg files that act as repositories for the parameters of that feature:

- Push-to-talk (ptt.cfg)
- Barcode symbologies and administration including QBC (barcode.cfg)
- Ekahau location services (RTLS.cfg)
- Custom applications (oai.cfg)
- Corporate directory (directory.cfg)

Part II: Configuration

Part II: Configuration covers the essential information you need to know in order to set the parameters in the handsets so that they work in your facility.

- Listing what parameters need to be set.

In coordination with the spreadsheet you have already started, this Chapter 4 goes into detail about what parameters are requested by each file. It explains the templates and their use and the settings that are required by the different scenarios.

- Telephony server variations covers the difference you will encounter if you set up a Lync telephony server vs a non-Lync server.

Variations between servers are also covered in the various Interop Guides that are published on the website. However, there are significant variations between Lync telephony and the other SIP telephony servers and these are covered in Chapter 5.

- Configuring the files.

Chapter 6 covers the actual configuration of the files for the central provisioning server.

- Configuring wireless parameters.

Wireless parameters are configured separately for the central provisioning server files because they have to be downloaded onto the phones with a USB cable.

Chapter 5: Determining What Parameters You Will Need to Configure

Before jumping into configuring the files, take a moment to ensure that you know the values for all the parameters you will need to set.

Using the Template Spreadsheet

The Configuration Parameters Spreadsheet is divided into wireless, system, group and user settings by tabs. Use it as a starting point and customize it according to your requirements. You may need to add parameters or delete ones you will not use. If you are using Groups, customize the Group tab and add additional Group tabs if you have more than one. If you keep these parameters separate, your .cfg file provisioning will be that much smoother. You can find this spreadsheet under the Downloads tab on the 84-Series webpage.

Refer to the scenarios to determine which .cfg files you will need to configure.

Wireless Settings

Wireless parameters are located in the wireless.cfg template. They include:

The phones' administrative password

Provisioning server information

- Server type (FTP,TFTP, HTTP, HTTPS)
- Server name or IP
- User name
- Password

Radio settings

- SSID
- Domain (Country)
- 2.4GHz or 5GHz or both
- If 5GHz, which bands?
- Transmit power settings

Security parameters for one of these types:

- None
- WEP
- WPA-PSK
- WPA2-PSK
- WPA2-Ent

QoS (consult your AP documentation)

- AC mandatory

DHCP enable?

DNS server information

- Hostname
- Domain
- IP address
- Alternate IP address

SNTP

- Server name
- GMT offset

System and Telephony Settings

System parameters are located in the site.cfg template. Each deployment scenario has a slightly different version. Use the template for your scenario to avoid confusion.

Logging

- File size
- Frequency of uploads

Dial plan

- Many parameters are possible, we have provided two of the most common.

Syslog server name

Lync Server base profile

or

openSIP Server

- SIP Server address & port
- Dial plan
- Call Forwarding
- Do Not Disturb
- Voicemail parameters

For User Profiles

- Login requirement

Features (commonly-deployed Global feature settings)

- App URLs
- Emergency Dial
- Exchange Calendar (IP address)
- Instant Messaging parameters
- OAI
- QBC

Per-Phone (User) Settings

Per –phone parameters are located in the per-phone file which is different for each scenario. Use the template for your scenario to avoid confusion. The parameters for each scenario are identical except a User Profiles section and a Lync section are added if you are deploying User Profiles.

Calls per line key

openSIP Telephony line registrations

For User Profiles

- Password
- Note that user profiles .cfg file includes some Lync telephony parameters that are in the site.cfg files for the two other scenarios.



Admin Tip: Exception for the Lync telephony server

If you are deploying a Lync telephony server, you may not need to configure per-phone .cfg files. If you are deploying User Profiles, you will need a per-user file to validate the profile login password.

Feature(s) and Group(s) Settings

The Features folder contains a file for each feature listed here. If a feature applies only to a Group, the parameters can be moved to a Group .cfg file. Parameters can be moved to the site.cfg file if a feature applies to the entire deployment. Alternatively, if a feature applies to the entire deployment, a feature .cfg files can be used individually as part of the string in the top level .cfg file.

Applications

- URL
- Label (name)

Barcode and QBC (refer to *Barcode Admin Guide*)

QBC

Corporate directory

- address
- User ID (if required)
- Password (if User ID is required)

OAI

- Gateway IP address

Personal Alarms

- Motion Alarms
- Duress Button
- Suspend Timeout
- Location Services
- Set Silent Profile Ring
- API detail

PTT or Emergency Dial

- Emergency Dial description and number
- Default channel
- Priority channel
- Emergency channel
- Available channels
- Subscribed channels
- Allow transmit channels
- Channel labels

Chapter 6: Telephony Server Variations

For our purposes, telephony servers fall into two categories: Lync and non-Lync. The Lync telephony server manages a number of telephony parameters that therefore do not have to be set in the .cfg files.

If your site.cfg file has two telephony sections---one for Lync and one for openSIP---delete the one you will not use to avoid configuration conflicts.

Lync Telephony Server

For full information about Lync interoperability, see *Interoperability Guide Spectralink 84-Series Wireless Telephones and Microsoft Lync Server 2010* or *Interoperability Guide Spectralink 84-Series Wireless Telephones and Microsoft Lync Server 2013*.

Microsoft Lync compatibility

Spectralink software is available in two variants – Microsoft® Lync® and non-Lync (or open SIP). Starting with Spectralink software 4.3/4.4 and continuing to 4.5/4.6, even numbered releases support both Lync and open SIP and odd numbered releases support open SIP only.

Spectralink Software 4.7.0 is based on Spectralink Software 4.5.0 and 4.6.1. This release merges the non-Lync (4.5.0) and Lync (4.6.1) release branches back into one release train. Subsequent releases continue with the merged approach.

“Non-Lync” versions of the 8440/41/52/53 do not support any Lync capability. A Lync-enabled handset supports Lync telephony, IM, calendaring, and Exchange. A handset without Lync support does not support any Lync functionality including IM, calendaring, and exchange. Handsets cannot be upgraded from non-Lync to Lync-enabled in the field. If customers are unsure if Lync capability will ever be needed, we recommend the purchase of Lync-enabled handsets.

Handsets purchased without Lync capability will not run Lync software releases, e.g. 4.6.x. Handsets with Lync compatibility will run Lync and non-Lync software releases.

Manufacturing date	Support Lync?
Prior to June 2013	Yes
June 2013 and later	2 handset variations: Lync-enabled: supports Lync non-Lync: does not support Lync



Tip

All 84-Series handsets manufactured before June 2013 support Lync.

All handsets have product ID's that identify them as Lync or non-Lync compatible.

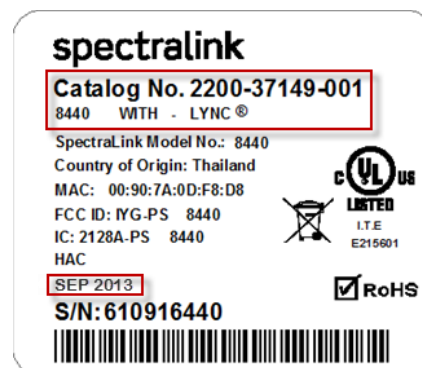
84-Series Product IDs with Microsoft Lync Support

Model	Lync SKUs
8440:	2200-37149-001, 2200-37150-001 2200-37174-101, 2200-37175-101
8441:	2200-37290-001, 2200-37290-101
8450:	2200-37152-001, 2200-37153-001 2200-37176-101, 2200-37177-101
8452:	2200-37172-001, 2200-37173-001 2200-37198-101, 2200-37199-101
8453:	2200-37294-001, 2200-37294-101

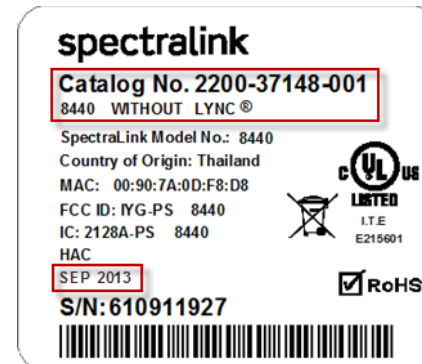
84-Series Product IDs without Microsoft Lync Support

Model	Open SIP SKUs
8440:	2200-37147-001, 2200-37148-001 2200-37165-101, 2200-37164-101
8441:	2200-37288-001, 2200-37288-101
8450:	All 8450 models support Lync.
8452:	2200-37163-001, 2200-37162-001 2200-37161-101, 2200-37160-101
8453:	2200-37292-001, 2200-37292-101

Label example



Label example



Admin Tip

Handsets manufactured prior to June 2013 are not differentiated on the label in the battery compartment as to Lync or non-Lync. All handsets manufactured before June 2013 are Lync compatible. For handsets built during or after June 2013, check the label text. The product ID and the “with Lync” or “without Lync” text on the label will confirm whether or not the handset is Lync-enabled.

Code variants are differentiated as Lync or non-Lync by their filenames when the zip file is extracted:

Lync compatible: slnk84xx.lync.ld

Non-Lync slnl84xx.sip.ld

It is possible (though not recommended) to run non-Lync code on a Lync enabled phone. To easily tell the difference between the firmware versions, the build id of the version number is structured to indicate the firmware type.

For instance, the complete version number for the 4.7.0 GA release is 4.7.0.x327. For non-Lync releases, the x is set to 2. For Lync releases the x is set to 1.

- Lync – 4.7.0.1327
- non-Lync – 4.7.0.2327

The first digit of the build id will always identify the type of firmware based on the description above.

You can download either code stream from the website but the Lync code is hardware compatible only as detailed above.

Lync Interoperability Overview

The Lync telephony server handles many parameters in the background through a Base Profile. The phones require an initial sign-in procedure using network credentials once it is deployed. After the user has signed in for the first time, the phone will not require it again unless the user logs out.

The Lync server already knows about the phone, therefore per-phone files may not be needed for Flat Deployment or Group Deployment.

User Profile Deployment is a special case. A per-user file is needed---the login.cfg file---because the password the user gives must be validated. Due to certain conflicts between the Lync sign in process and the login process required by User Profiles, the Base Profile cannot be used. Instead we have to spell out Lync parameters. Some Lync parameters are located in the site.cfg file as they need to be activated before the user logs on and others are located in the login.cfg file as they need to be activated after the user logs on.



Caution: Using a Lync Telephony Server with User Profiles

You must set up a default user when using User Profiles in a Lync telephony server environment in order to make emergency calls without logging in. Contact a Deployment Specialist for help in setting up default user parameters.

Be sure to use the templates for the scenario you are going to deploy as they contain the exact parameters you will need.

OpenSIP Telephony Server

The Spectralink 84-Series handsets have been tested with several SIP servers. Special interoperability guides have been produced and are available on the Spectralink website. See the References section at the front of this document for directions to these documents.

The openSIP telephony parameters are located in the site.cfg file and are as you would expect. They cover things like dial plan, voicemail and instant messaging. Warning: Do not confuse using Lync for IM with using a Lync telephony server.

Consult a Deployment Specialist if you need help setting up your system.

Chapter 7: Configuring Central Provisioning Server .cfg files

This chapter is used to configure files that reside on the central provisioning server.

Finalize your Deployment Scenario Structure

Draw a diagram of your deployment structure to determine if additional design considerations need to be explored before provisioning.

Before you start to configure the files, be sure you know:

- Which deployment scenario you will use,
- What .cfg files you need to configure,
- What parameters you need to set,
- What filenames will be used and
- Which .cfg files go with which phones if you are using separate features configuration files or deploying Groups.

Organize the Files

You will be working on a computer, such as a PC laptop, that is convenient and accessible to the network. Create a suitable file structure so that each of the files you create can be easily retrieved when you need to move them to a different location.

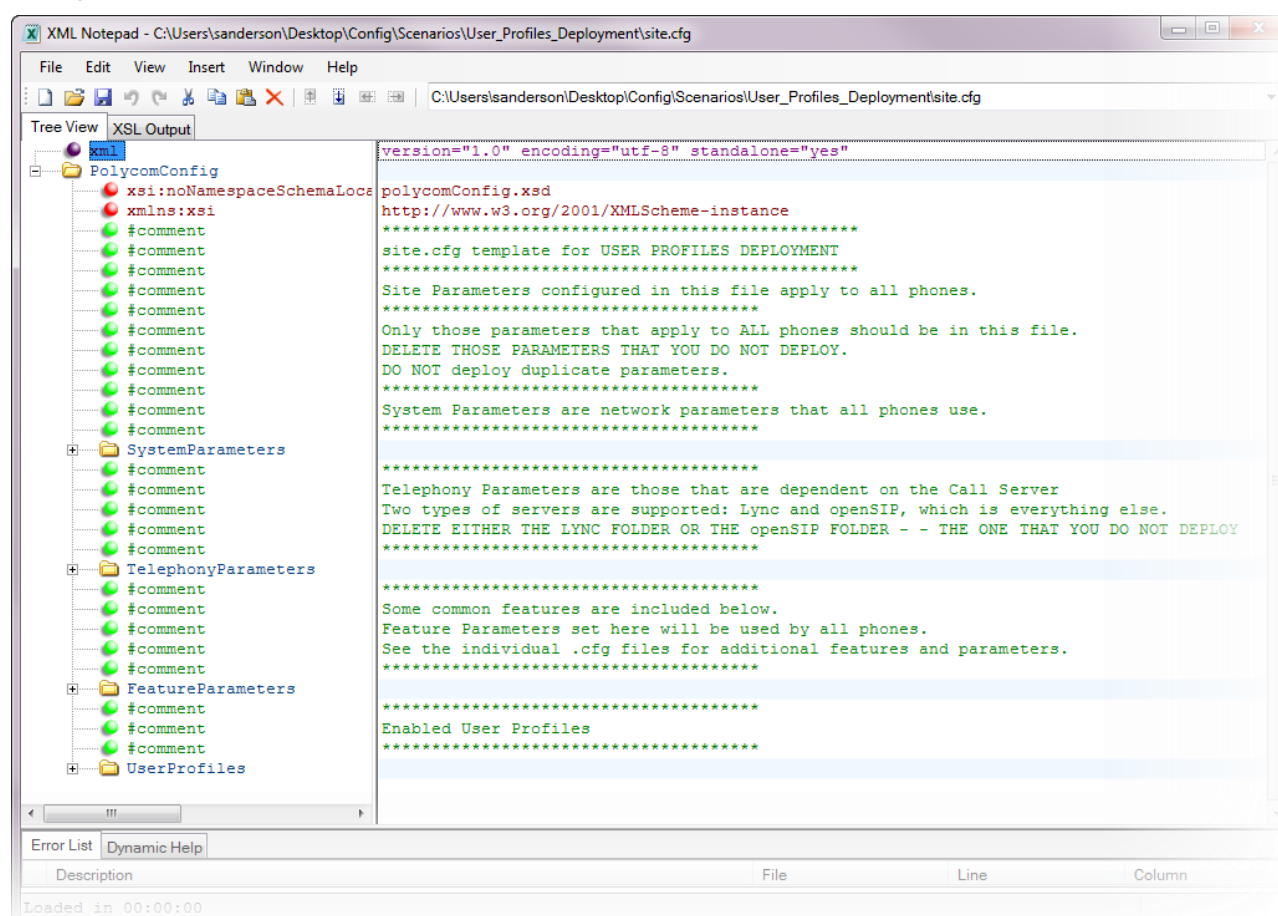
Configure site.cfg

All three scenarios reference the site.cfg file, which is positioned as the last file in the CONFIG_FILE list. Positioning it is a neat way to ensure that any per-user or group file parameters have precedence. The site.cfg file contains a wide range of telephony and system configuration parameters. We will step through these just as we did with the wireless parameters.

The file is separated into four areas:

- System Parameters: Network parameters that all phones use.
- Telephony Parameters: Parameters that are dependent on the call server.
- Feature Parameters: Some commonly-deployed features are included.
- User Profile (this folder is only in the site.cfg file found in the User Profile Deployment folder): Requires a login in order to use the phone.

site.cfg template



System Parameters

Log and syslog parameters are in the System folder.



When you will see a separate .set parameter

Only the device.x parameter uses the mechanism that requires a set=1 parameter to confirm the parameter value. The device.x parameter is disabled by set=0. You will not see the .set parameter used with any other type of parameter.



Log

Unless otherwise specified, all values are recommended settings and do not need to be changed.

Parameter	Permitted Values	Default
log.render.file.upload.period	positive integer	86400
Time in seconds between log file uploads to the provisioning server. Note: The log file will not be uploaded if no new events have been logged since the last upload.		
log.render.file.size	positive integer, 1 to 180	32
Maximum size of flash memory for logs in Kbytes. When this size is about to be exceeded, the phone will upload all logs that have not yet been uploaded, and erase half of the logs on the phone. The administrator may use Web browser to read all logs on the phone.		
log.render.file.upload.append.sizeLimit	positive integer	512
Maximum log file size that can be stored on provisioning server in Kbytes.		
log.render.level	0 to 6	4
Specifies the lowest class of event that will be rendered to the log files. This is the output filter from the internal memory-based log system. The log.render.level maps to syslog severity as follows: 0 -> SeverityDebug (7) 1 -> SeverityDebug (7) 2 -> SeverityInformational (6) 3 -> SeverityInformational (6) 4 -> SeverityError (3) 5 -> SeverityCritical (2) 6 -> SeverityEmergency (0) For more information, refer to the next section on Syslog.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
log.render.stdout	0 or 1	0
Set to 1. Spectralink recommends that you do not change this value. Note that on Spectralink handsets, the default value is 0.		

Syslog



Spectralink recommends: Monitoring wireless events

Spectralink recommends that you provision a syslog server so that the wireless telephony events can be monitored.

The syslog server name can be an IP address or fqdn (fully qualified domain name).

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
device.syslog.serverName	dotted-decimal IP address OR domain name string	Null

The syslog server IP address or domain name string.

device.syslog.renderLevel	0 to 6	3
Specify the logging level that will display in the syslog. Note that when you choose a log level, you are including all events of an equal or greater severity level and excluding events of a lower severity level. The logging level you choose determines the lowest severity of events that will be logged. 0 or 1: SeverityDebug(7). 2 or 3: SeverityInformational(6). 4: SeverityError(3). 5: SeverityCritical(2). 6: SeverityEmergency(0).		

Telephony Parameters

If your site.cfg file has two telephony sections---one for Lync and one for openSIP---delete the one you will not use to avoid configuration conflicts.



Caution: Deleting unused parameters

If both types of server parameters are present in your site.cfg file, you **MUST** delete either the Lync or openSIP folder. Keeping both sets of parameters in your file could cause the phone to malfunction.

Lync

Starting with UCS 4.1.0, the "base profile" feature allows you to set up Lync telephony by setting a base profile rather than by setting each telephony parameter to a Lync-compatible value. User Profiles Deployment cannot use the base profile and the site.cfg file for User Profiles has other Lync parameters. Do not change them unless instructed by a Deployment Specialist.

Parameter	Permitted Values	Default
Device.baseProfile	Lync	Null

If using Lync, set the value to Lync.

User Profiles

The Lync Telephony parameters in the User Profiles site.cfg file should not be changed. They have been preset for proper Lync operation.

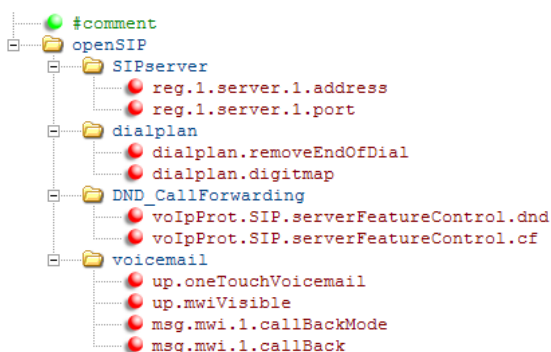


Note: Consult the Lync Interoperability Guide

The Lync Interoperability Guide for your Lync Server is the definitive guide for understanding your Lync deployment and configuring Lync parameters. Interoperability Guides are available on the 84-Series webpage.

Open SIP

OpenSIP servers are basically all those that are not Lync.



```

openSIP servers are basically all those that are not Lync.

mysipserver.domain.com
5060

1
x.T

1
1

1
1
registration
  
```

SIP Server

The SIP server is the server that accepts and manages the registrations for the phones.

Parameter	Permitted Values	Default
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.port	0, 1 to 65535	0
The port value entered here must match the port used in the SIP server to accept connection requests. The template value is 5060. The Nortel CS1K SIP server uses 5070.		
volpProt.SIP.enable	0 or 1	1
A flag to determine if the SIP protocol is used for call routing, dial plan, DTMF, and URL dialing. If set to 1, the SIP protocol is used.		

Dialplan

Parameter	Permitted Values	Default
dialplan.removeEndOfDial	0 or 1	1
If set to 1, strip trailing # digit from digits sent out.		
dialplan.digitmap	string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435	[2-9]11 0T +011xxx.T 0[2-9]xxxxxxxx +1[2-9]xxxxxxxx [2-9]xxxxxxxx [2-9]xxxT
The digit map used for the dial plan. The string is limited to 2560 bytes and 100 segments; a comma is also allowed; a comma will turn dial tone back on; '+' is allowed as a valid digit; extension letter 'R' is used as defined above. This parameter enables the phone to automatically initiate calls to numbers that match a digit map pattern. Typically the value x.T as given in the template is all that is needed.		

DND_CallForwarding

Parameter	Permitted Values	Default
volpProt.SIP.serverFeatureControl.cf	0 or 1	0
If set to 1, server-based call forwarding is enabled. The call server has control of call forwarding. If set to 0, server-based call forwarding is not enabled. This is the old behavior.		
volpProt.SIP.serverFeatureControl.dnd	0 or 1	0
If set to 1, server-based DND is enabled. The call server has control of DND. If set to 0, server-based DND is not enabled. This is the old behavior.		

Voicemail

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
up.oneTouchVoiceMail	0 or 1	0
If set to 1, the voicemail summary display is bypassed and voicemail is dialed directly (if configured).		
up.mwiVisible	0 or 1	0
If set is 0, the incoming MWI notifications for lines where the MWI callback mode is disabled (<code>msg.mwi.x.callBackMode</code> is set to 0) are ignored, and do not appear in the message retrieval menus. If set to 1, the MWI for lines whose MWI is disabled will display, even though MWI notifications have been received for those lines.		
msg.mwi.x.callBackMode	contact, registration, disabled	registration
The message retrieval mode and notification for registration x. <code>contact</code> – a call is placed to the contact specified by <code>msg.mwi.x.callback</code> . <code>registration</code> – the registration places a call to itself (the phone calls itself). <code>disabled</code> – message retrieval and message notification are disabled.		
msg.mwi.x.callBack	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@spectralink.com)	Null
The contact to call when retrieving messages for this registration if <code>msg.mwi.x.callBackMode</code> is set to <code>contact</code>		

Feature Parameters

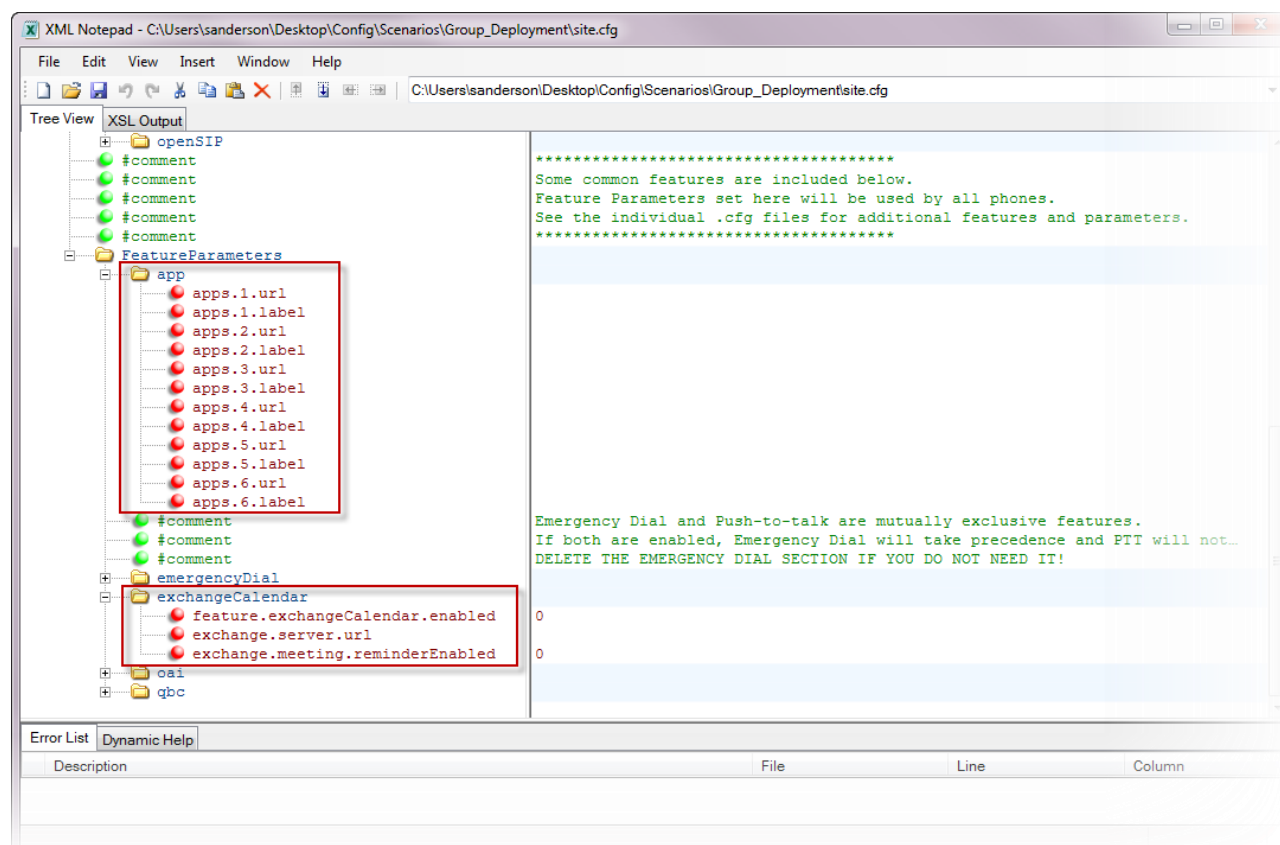
Some commonly used features are included in the site.cfg file. Features that are used by all phones can be included in this file.

The features that do not have separate .cfg files are explained below.

- Applications
- Exchange calendar
- Instant Messaging (IM)

Please see the section “Deploying Features” for an explanation of the other features’ parameters.

Features that are not covered in a separate .cfg file



Applications

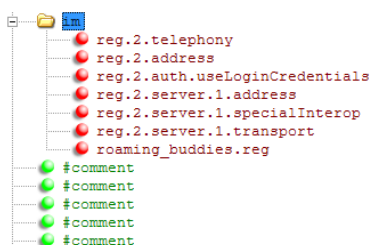
Parameter	Permitted Values	Default
apps.x.label The descriptive text that displays in the Applications menu	String	null
apps.x.url² The URL of an application		
The label and URL of up to 12 applications (for x = 1 to 12).		

Exchange Calendar

Parameter	Permitted Values	Default
feature.exchangeCalendar.enabled	0 or 1	0
If 0, the calendaring feature is disabled. If 1, the feature is enabled.		
exchange.server.url	String	Null
The Microsoft Exchange server address.		
exchange.meeting.reminderEnabled	0 or 1	1
If 0, meeting reminders are disabled. If 1, they are enabled.		

IM (Instant Messaging)

In our IM example, reg2 becomes the IM line. Lync2010 is deployed. For User Profiles Deployment, the reg.2 parameters are located in the login.cfg file.



```
0
username@company.com
1
lync2010
TLS
2
If IM/Presence is enabled in site.cfg, it will use the second line registration reg.2
The sample above shows how to configure the IM/Presence line, which must be done in the
user-specific file
For IM, DHCP option 43 must point to the certificate server. If this cannot be done,
refer to the deployment guide for manual certificate installation
```

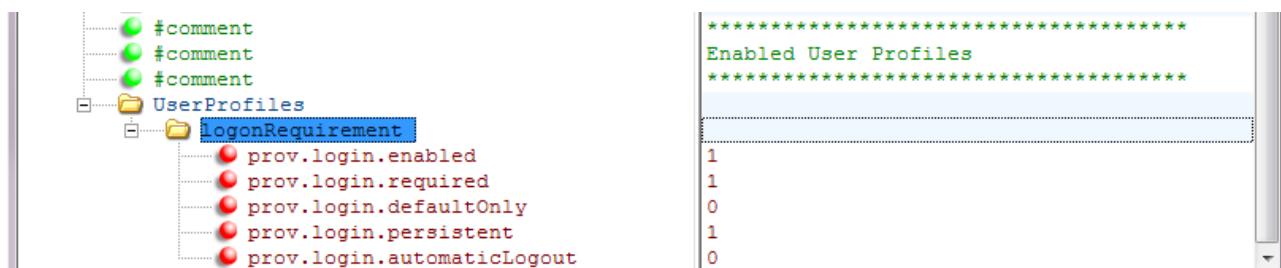
Parameter	Permitted Values	Default
feature.messaging.enabled	0 or 1	0
If 0, the instant messaging feature is disabled. If 1, the feature is enabled.		
feature.presence.enabled	0 or 1	0
If 0, the presence feature — including buddy managements and user status — is disabled. If 1, the presence feature is enabled with the buddy and status options.		
reg.x.telephony	0 or 1	1
If 0, telephony calls are not enabled on this registration (use this value if the registration is used with Microsoft Office Communications Server 2007 R2 or Microsoft Lync 2010/2013. If 1, telephony calls are enabled on this registration.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
reg.x.auth.useLoginCredentials	0 or 1	0
If 0, login credentials are not used for authentication to the server on registration x. If 1, login credentials are used for authentication to the server. <i>Note:</i> This must be set to 1 for instant messaging on the Spectralink handsets.		
reg.x.server.y.address	dotted-decimal IP address or hostname	Null
The IP address or host name of a SIP server that accepts registrations. If not Null, all of the parameters in this table will override the parameters specified in <code>voIpProt.server.*</code> . <i>Notes:</i> If this parameter is set, it will take precedence even if the DHCP server is available. If this registration is used for Microsoft Office Communications Server 2007 R2 on Spectralink handsets, this parameter must be in the form <code>OCShostname.OSCdomain_name</code> . reg.2.server.1.address. the address to use to contact and register with the Lync server for IM and Presence.		
reg.x.server.y.port	0, 1 to 65535	Null
The port of the sip server that specifies registrations. If 0, the port used depends on <code>reg.x.server.y.transport</code> .		
reg.x.server.y.register	0 or 1	1
If the outbound proxy can route calls without the phone being registered to it, set this value to 0..		
reg.x.server.y.specialInterop	standard, ocs2007r2, lcs2005, lync2010, lync2013	standard
Specify if this registration should support Microsoft Office Communications Server 2007 R2 (ocs2007r2), Microsoft Live Communications Server 2005 (lcs2005), Microsoft Lync 2010 (lync2010) or Microsoft Lync 2013 (lync2013). <i>Note:</i> 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. Null or DNSNaptr - if <code>reg.x.server.y.address</code> is a hostname and <code>reg.x.server.y.port</code> is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If <code>reg.x.server.y.address</code> is an IP address, or a port is given, then UDP is used. TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails. UDPOnly - only UDP will be used. TLS - if TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. TCPOnly - only TCP will be used.		
roaming_buddies.reg	1 to 34	Null
The index of the registration which has roaming buddies support enabled. If Null, the roaming buddies feature is disabled. <i>Note:</i> This parameter must be set if the call server is Microsoft Live Communications Server 2005, Microsoft Office Communications Server 2007 R2, or Microsoft Lync.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
sec.TLS.customCaCert.x	String	Null
The custom certificate for TLS Application Profile x (x= 1 to 6). This parameter is not in the template but may need to be added. It is not required if you use DHCP option 43 to tell the phone where to get its certificate automatically but if that is not available , then add the certificate using this parameter.		
sec.TLS.profileSelection.SIP	a TLS profile	PlatformProfile1
The TLS platform profile or TLS application profile to use for SIP operations. Permitted values are:		
<ul style="list-style-type: none"> • PlatformProfile1 • PlatformProfile2 • ApplicationProfile1 • ApplicationProfile2 • ApplicationProfile3 • ApplicationProfile4 • ApplicationProfile5 • ApplicationProfile6 		
volpProt.SIP.mtls.enable	0 or 1	1
If 0, TLS with mutual authentication is disabled. If 1, TLS with mutual authentication is enabled. Used in conjunction with Microsoft Lync 2010/2013.		
volpProt.SIP.IM.autoAnswerDelay	0 to 40, seconds	10
The time interval from receipt of the instant message invitation to automatically accepting the invitation. If users have a PC that is logged to their IM account, should thePC auto-answer incoming IMs if no action is taken on the phone?		
Yes: volpProt.SIP.IM.autoAnswerDelay="30"		
No: volpProt.SIP.IM.autoAnswerDelay="10"		

User Profiles

When deploying User Profiles, you must specify that a login is required in order to use the phone.



The phone uses the `profile.login.enabled="1"` parameter to present a login prompt. In our template, login is enabled and required, other users besides the default user can log in, users remain logged in when the handset reboots, if `prov.login.persistent="1"` is set. The user must log out as the user is never automatically logged out.

Parameter	Permitted Values	Default
prov.login.enabled	0 or 1	0
If 0, the user profile feature is disabled. If 1, the user profile feature is enabled.		
prov.login.required	0 or 1	0
If 1, a user must log in when the login feature is enabled. If 0, the user does not have to log in.		
prov.login.defaultOnly	0 or 1	0
If 1, the default user is the only user who can log in. If 0, other users can log in.		
prov.login.persistent	0 or 1	0
If 0, users are logged out if the handset reboots. If 1, users remain logged in when the phone reboots.		
prov.login.automaticLogout	0 to 46000	0
The time (in minutes) before a non-default user is automatically logged out of the handset. If 0, the user is not automatically logged out.		

Configure the Per-phone .cfg File

All three scenarios use nearly identical per-phone files. They all contain the line registrations that the phone will need to, well, to be telephones.

Both the Flat and Group Deployment scenarios have per phone files that are linked directly to the phones' MACaddress. In these two scenarios, phones are assigned to an extension and usually deployed to a single user. The files are differentiated by their filenames.

The per-user template provided for each scenario only contains those parameters that are required by that single phone or user. Feature settings or system settings are not in the per-phone .cfg file. They could be, but maintenance issues get very complicated when system settings that belong in site.cfg are dispersed through the other .cfg files.



Admin Tip: Lync Telephony Server Variation

The .cfg files provided by the software include a per-phone file for each scenario. If you are using a Lync telephony server, you may not need to configure these files in a Flat or Group Deployment because the Lync server already knows about the phones and their registrations. You will need a per-user file when deploying User Profiles as the password must be validated at login.

See Chapter 5 for more information if you are using a Lync telephony server.

Filenames for per-phone or per-user .cfg files

Each scenario has a specific naming protocol for the per-phone or per-user .cfg files that it uses.

Flat Deployment

In the Flat Deployment scenario the per-phone .cfg filename you see in the top level .cfg file is [PHONE_MAC_ADDRESS]-ext.cfg. Here a variable is being used to direct the phone to its per-phone .cfg file. When you create the individual per-phone files, they must be named with the phone's MACaddress plus this suffix -ext, such as 00907A0CD967-ext.cfg.



Admin Tip: Naming the phone-specific configuration file

The [PHONE_MAC_ADDRESS]-ext.cfg file uses a variable plus an extension identifier to point to the MACaddress files you create for each phone/extension. The '-ext' part of the filename used in this document could be replaced by some other identifier. The important thing is that whatever identifier you use here is also used on each of the MACaddress files you create for each phone.

Do not use the following file names as your per-phone file name: <MACaddress>-phone.cfg, <MACaddress>-Web.cfg, <MACaddress>-app.log, <MACaddress>-

boot.log, or <MACAddress>-license.cfg. These file names are used by the phone itself to store user preferences (overrides) and logging information.

Group Deployment

In the Group Deployment scenario the per-phone .cfg filename you see in the top level .cfg file is identity.cfg. Because the MACAddress is already identified by using a top level .cfg file with the phone's MAC address, you can use any filename as an identifier for the per-phone file.

Usually per-phone filenames are named for the extension, such as 3303.cfg or the user, such as jdoe.cfg. You will reference this .cfg file in the top level MACAddress.cfg file you will create for each phone in the next section.

User Profiles Deployment

When User Profiles are deployed, phones are not assigned to users or extensions by MACAddress. Any phone can be used by any user who has login credentials. The filename of the per-phone .cfg file must be its login name. The password is included in the parameters for validation. Example: Mary Smith has a login name of msmith and therefore her per-phone .cfg file must be named msmith.cfg. Her password is benji and benji must be entered for the password value in her msmith.cfg file.

Per-Phone .cfg Files

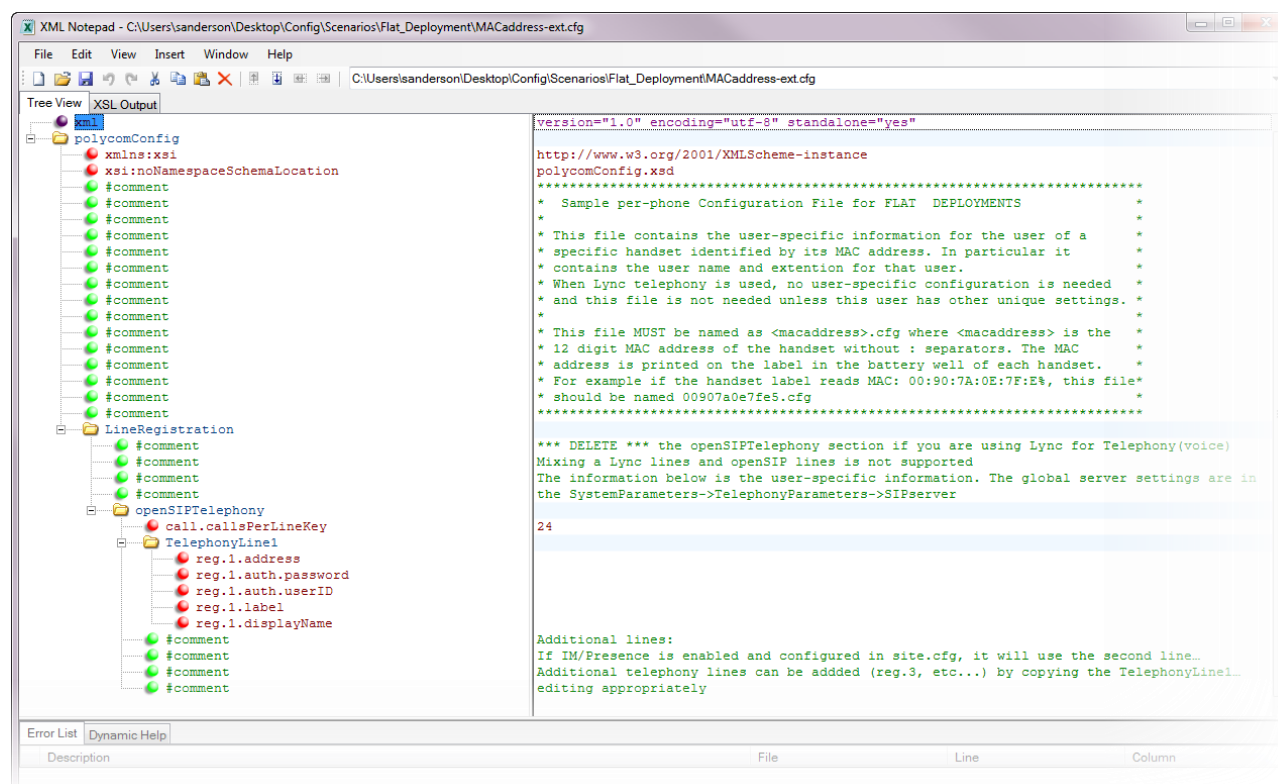
Flat and Group Deployment scenarios use identical per-phone files. The files must be named according to the convention described previously but otherwise, the same template design is used. If you are using a Lync telephony server, these per-phone files may not be needed. See Chapter 5: Telephony Server Variations.

User Profiles Deployment requires a per-user file no matter what type of server you are using. The per-user file validates the login password and contains essential parameters if you are using a Lync telephony server.

Flat Deployment and Group Deployment

Select the per-phone template according to your deployment scenario. For Flat Deployment, the per-phone file is called MACAddress-ext.cfg. For Group Deployment, the file is called identity.cfg. Use the template file to build each per-phone.cfg file you need to create. If you have completed a spreadsheet that lists all the users, you will have a handy reference for the extension and the MACAddress of each phone.

Per-phone .cfg file template



A typical per-phone file will simply use an extension number for these parameters:

reg.1.address="8451" reg.1.auth.password="8451" reg.1.auth.userId="8451"

reg.1.displayName="8451" reg.1.label="8451". These parameters will provide unique information to connect this phone to the SIP server.

Parameter	Permitted Values	Default
call.callsPerLineKey	1-4, 1-8, 1-24	4, 8, 24
Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines. Note that this parameter may be overridden by the per-registration parameter of reg.x.callsPerLineKey.		
reg.x.address	string address	Null
The user part (for example, 1002) or the user and the host part (for example, 1002@Spectralink.com) of the registration SIP URI or the H.323 ID/extension.		
reg.x.auth.password	string	Null
The password to be used for SIP server extension for this registration. If the password is non-Null, it will override the password entered into the Authentication submenu on the Settings menu of the phone.		
reg.x.auth.userId	string	Null
User ID to be used for SIP server extension for this registration. If the User ID is non-Null, it will override the user parameter entered into the Authentication submenu on the Settings menu of the phone.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
reg.x.label	UTF-8 encoded string	Null
The text label that displays next to the line key for registration x. If Null, the user part of <code>reg.x.address</code> is used.		
reg.x.displayName	UTF-8 encoded string	Null
The display name used in SIP signaling and/or the H.323 alias used as the default caller ID.		

Per-User .cfg Files

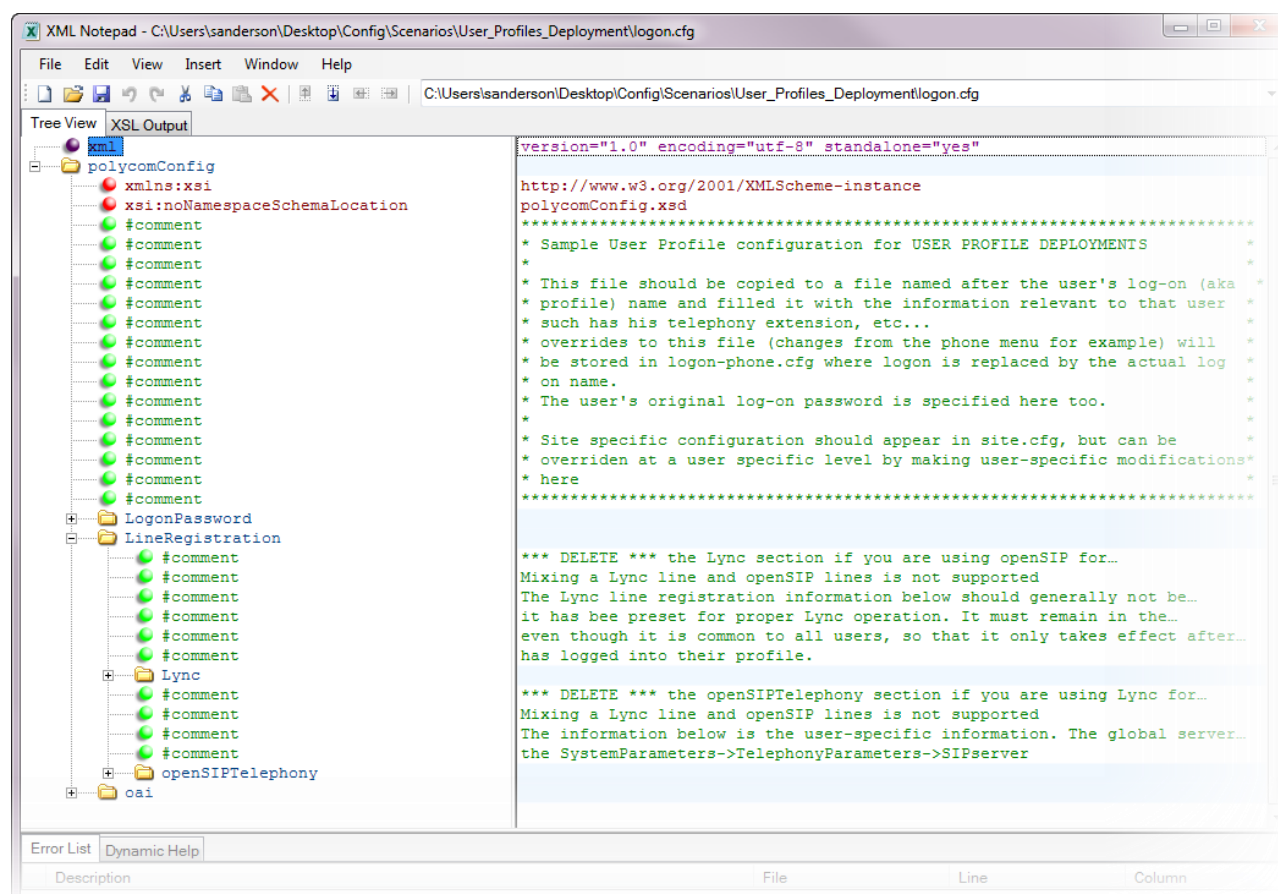
In User Profiles Deployment, phones are not deployed per-phone; they are deployed per-user so that you can have many more users than you have phones.

User Profiles Deployment

The per-user file is called `login.cfg` in the template. You will notice that this file has two different line registration folders---one for Lync and one for openSIP---similar to the `site.cfg` file. Like you did in the `site.cfg` file, delete the one that you will not be using.

The `login.cfg` file is named for the user's login name. After the user enters the name on the phone, the password must be entered. The `login.cfg` file needs to validate the password and therefore the login password parameter is contained in this file.

Per-user login.cfg file for User Profiles Deployment



Parameter	Permitted Values	Default
prov.login.localPassword	String	123
The password used to validate the user login. It is stored either as plain text or encrypted (an SHA1 hash).		
Lync Line Registration		
The Lync line registration information should not be changed. It has been preset for proper Lync operation. It must remain in the login.cfg file, even though it is common to all users, so that it only takes effect after the user has logged into their profile.		
OpenSIP Telephony Registration		
The openSIP registration is the same as used for Flat and Group Deployments except for IM parameters. See Flat/Group per-phone parameters.		
For IM, the line registrations are in the login.cfg file instead of in the site.cfg file. See the IM section in the site.cfg configuration section for parameter names and values.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
OAI		
oai.userId	String of eight hexadecimal characters	Null

The lower four bytes of the six-byte OAI handset identifier in the OAI gateway. If OAI is provisioned in the site.cfg file, you can use this parameter to provide a user ID to 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.

Example: "ffff315" 8 bit virtual hexadecimal address to identify each handset when User Profiles are used. This example shows base "ffff" prepended with extension 315. Each handset shall have its own virtual ID.

If the oai.userId is not used, then the 84-Series handset MACaddress is used to register the handset with the OAI. The oai.userId is used with UserProfiles but is not needed for the standard profile.



Caution: Using a Lync Telephony Server with User Profiles

You must set up a default user when using User Profiles in a Lync telephony server environment in order to make emergency calls without logging in. Contact a Deployment Specialist for help in setting up default user parameters.

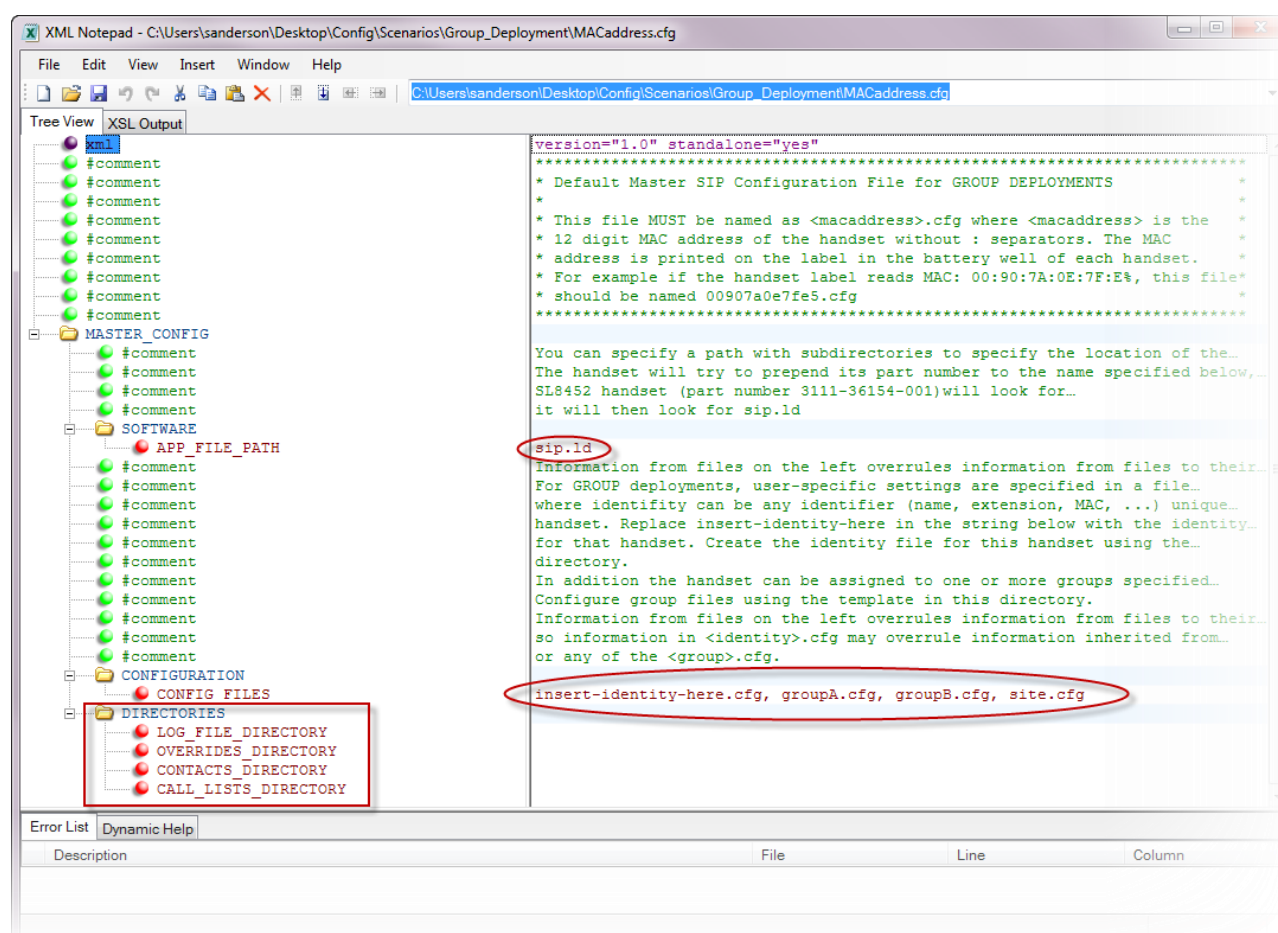
Configure the <MACAddress>.cfg file

In Group Deployment, you will need to create a top level .cfg file for each phone. This top level file will reference the per-phone file you created in the previous section and the feature.cfg and Group.cfg files you create.

Refer to the spreadsheet you customized. It should list the extension/person, the MACAddress of the phone assigned to that extension and the name of the group(s) you assigned to that extension/person.

- 1 Open the MACAddress.cfg template in the Group_Deployment folder.

The MACAddress.cfg template



- 2 Edit the software path as needed.
- 3 Replace the CONFIG_FILES values with the filenames you create:

Template value	Type of .cfg file	Example name
insert-identity-here.cfg	per-phone file	3303.cfg

<i>Template value</i>	<i>Type of .cfg file</i>	<i>Example name</i>
GroupA.cfg	Custom group file	ICUnurse.cfg
GroupB.cfg	Custom group file	MaternityNurse.cfg
site.cfg	System parameters	site.cfg

- 4** Enter values for the DIRECTORIES (You will set up these directories in the central provisioning server).
- 5** Save as the MACaddress of the phone assigned to the identity you have entered in CONFIG_FILE list. E.g. 00907A0CD967.cfg.
- 6** Repeat for all phones.

You will have as many unique MACaddress.cfg files as you have phones to deploy.

Deploying Features

Some commonly-used features are included in the site.cfg file. The templates include .cfg files for several features that may not be as familiar or may be only partially deployed. These .cfg files can be used as a resource to add features and parameters to existing site.cfg or group.cfg files. In some cases, you may want to deploy a feature by including its .cfg file in the CONFIG_FILE list of the top level .cfg file. Be aware of duplicate parameters and ensure that you do not set conflicting parameters that will cause confusion later.

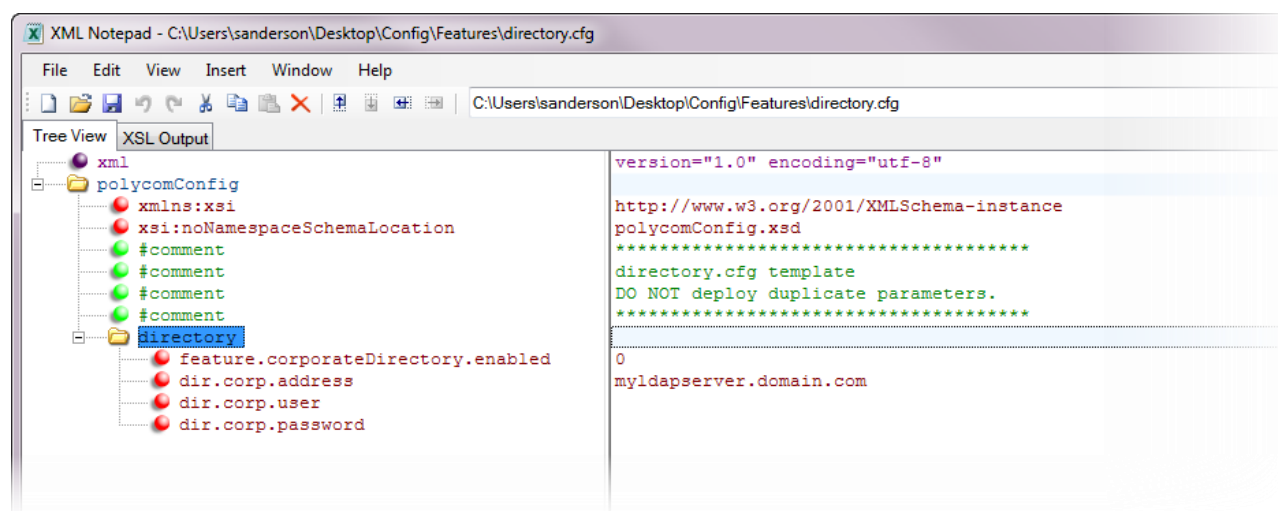
Templates are provided for these features:

- Barcode
- Directory
- OAI
- Personal Alarms
- PTT
- RTLS

Barcode

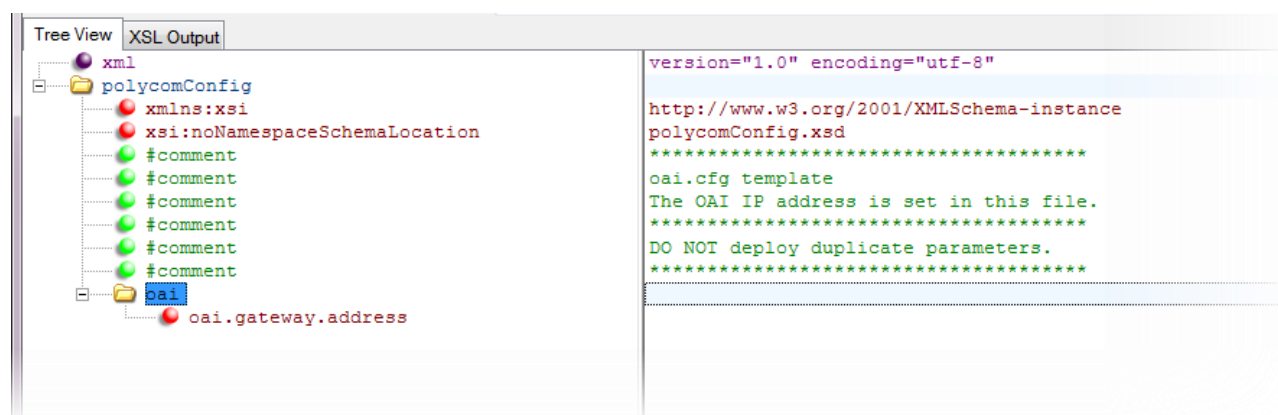
The barcode.cfg file includes settings for QBC which is also in the site.cfg file. You can deploy barcodes with just that much but if you need to tweak those settings or use additional symbologies, refer to the *Barcode Administration Guide* for detailed information and a list of all barcode parameters.

Corporate Directory



Parameter	Permitted Values	Default
feature.corporateDirectory.enabled	0 or 1	0
If 0, the corporate directory feature is disabled. If 1, the feature is enabled.		
dir.corp.address	dotted-decimal IP address or hostname or FQDN	Null
The IP address or hostname of the LDAP server interface to the corporate directory. For example, <i>host.domain.com</i> .		
dir.corp.password	UTF-8 encoded string	Null
The password used to authenticate to the LDAP server.		
dir.corp.user	UTF-8 encoded string	Null
The user name used to authenticate to the LDAP server.		

OAI



Parameter	Permitted values	Default
oai.gateway.address	IP address	Null
The address of the OAI server.		

Personal Alarms

Spectralink 8441 and 8453 handsets offer personal monitoring and duress call functionality, including “man down” alarms, “running” alarms and duress calls to an emergency number. Duress call alarms can also be deployed within the functionality of the 8440 and 8452 models. See the *Spectralink 84-Series Wireless Telephone Administrative Guide* for detailed information about this feature.

Push-to-talk (PTT)

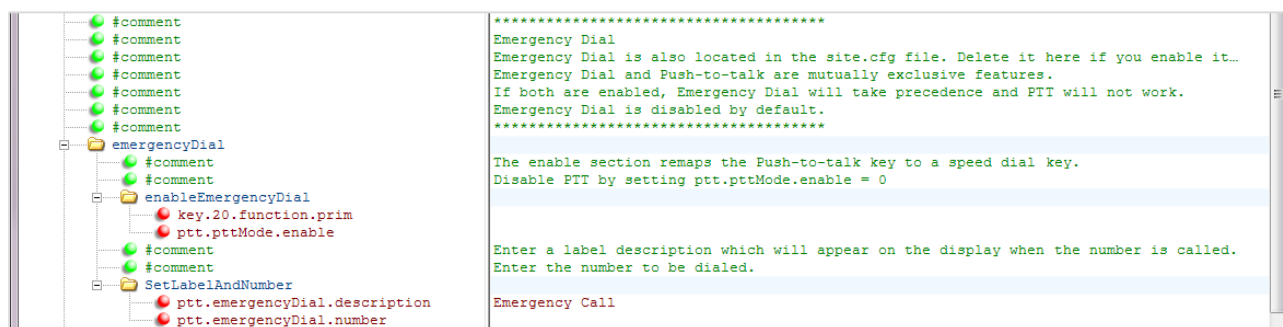
PTT and Emergency Dial parameters are both included in the ptt.cfg file as they both use the large Talk button on the left side of the handset.

Parameters from this file can be moved to the site.cfg and/or a group file.

Emergency Dial

Emergency Dial is also located in the site.cfg file. They are mutually exclusive features. If you enable Emergency Dial in the site.cfg file, PTT cannot be deployed. If both are enabled, Emergency Dial will take precedence and PTT will not work. Emergency Dial is disabled by default.

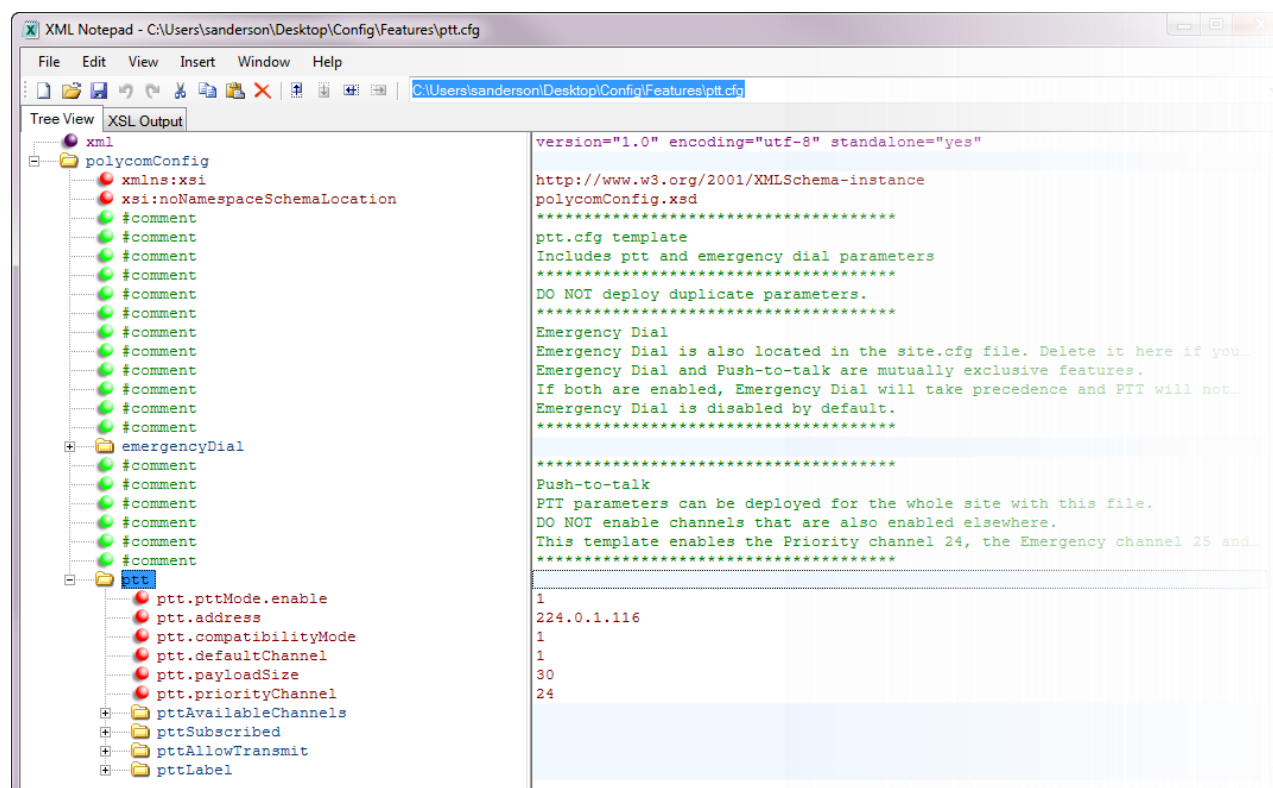
Emergency dial is enabled by mapping the PTT key on the left side of the phone to a speed dial function instead.



Parameter	Permitted values	Default
key.20.function.prim	SpeedDial	Null
Maps speed dial key 20 to the PTT button if set.		
ptt.pttMode.enable	0 or 1	Null
If Emergency Dial is enabled, disable PTT by setting this value to 0.		
ptt.emergencyDial.description		Null
Enter a label description which will appear on the display when the number is called.		
ptt.emergencyDial.number		Null
Enter the number to be dialed.		

PTT

Push-to-talk channels are frequently deployed in groups so that only certain people receive and send transmissions on specific channels.



Channels 1-25 are listed for each of the four folders. For each of these four types of settings, the channels are listed and you can set the value according to your deployment requirements.

- Available = the channel will appear on the phone and can be subscribed to.
- Subscribed = the channel is active and incoming transmissions will be heard.
- Allow Transmit = the user may transmit on the channel.
- Label = the name of the channel that will appear on the handset's screen during transmissions.

Parameter	Permitted Values	Default
ptt.pttMode.enable	0 or 1	0
If 0, push-to-talk is disabled. If 1, push-to-talk is enabled.		
ptt.address	multicast IP address	224.0.1.116
The multicast IP address to send page audio to and receive page audio from. Use default.		
ptt.compatibilityMode	0 or 1	1
If 0, the PTT protocol behavior is not compatible with Spectralink handset models 8020/8030 or older. If 1, all PTT protocol behavior is compatible with the older Spectralink handsets, even if some configuration parameters are incompatible. For example, if this parameter is enabled and <code>ptt.codec</code> is set to G.722, the G.726QI codec will be used for outgoing PTT audio to maintain compatibility.		
ptt.defaultChannel	1 to 25	1
The PTT channel used to transmit an outgoing page if the user does not explicitly specify a channel.		

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
ptt.payloadSize The audio payload size in milliseconds. Use default.	10 to 80	20
ptt.priorityChannel The channel assigned for priority pages.	1 to 25	24
ptt.emergencyChannel The channel assigned for emergency pages.	1 to 25	25
ptt.channel.x.available Make the channel available to the user	0 or 1	1
ptt.channel.x.allowTransmit Allow outgoing broadcasts on the channel	0 or 1	1
ptt.channel.x.label The label to identify the channel	string	ch1: All, ch24: Priority, ch25: Emergency, others: Null
ptt.channel.x.subscribed Subscribe the phone to the channel	0 or 1	ch1, 24, 25: 1, others: 0

A push-to-talk channel x, where x= 1 to 25. The `label` is the name used to identify the channel during broadcasts.

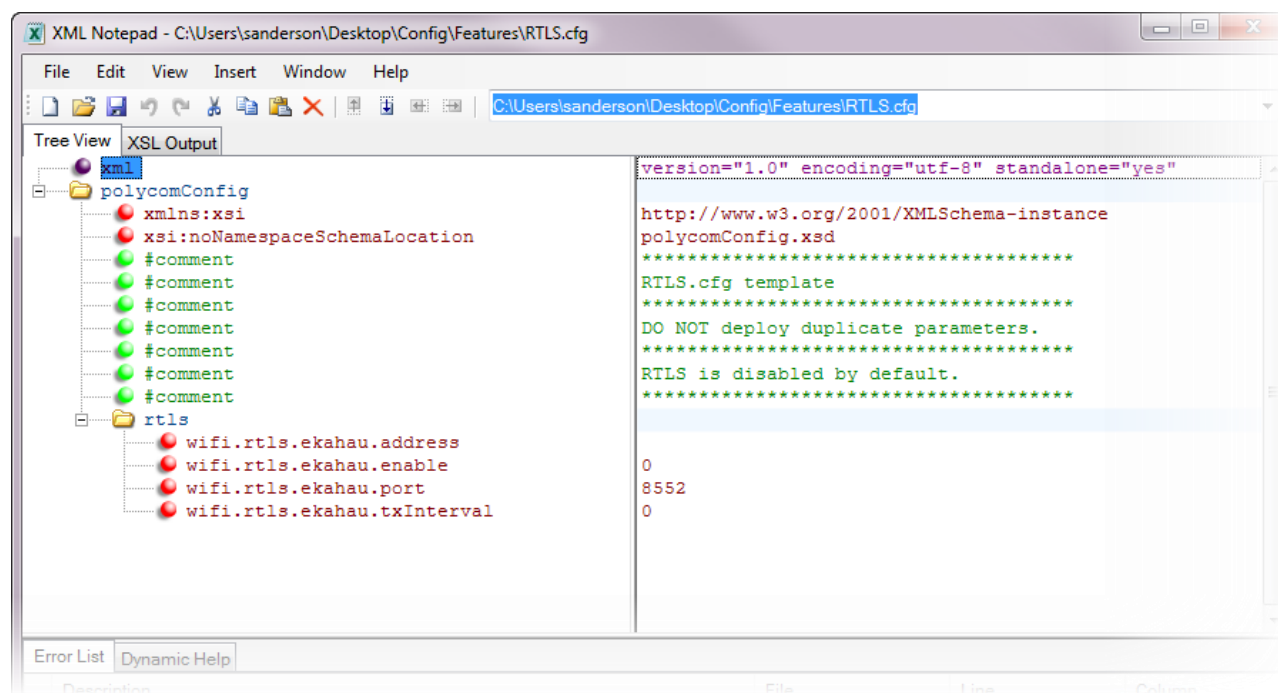
If `available` is disabled (0), the user cannot access the channel or subscribe and the other channel parameters will be ignored. If enabled, the user can access the channel and choose to subscribe.

If `allowTransmit` is disabled (0), the user cannot send PTT broadcasts on the channel. If enabled, the user may choose to send PTT broadcasts on the channel.

If `subscribed` is disabled, the phone will not be subscribed to the channel. If enabled, the phone will subscribe to the channel.

RTLS

This parameter configures the use of the Ekahau Location System for the Spectralink handsets.



Parameter	Permitted Values	Default
wifi.rtls.ekahau.address	IP-address	169.254.10.10
The IP address of the Ekahau Positioning Engine.		
wifi.rtls.ekahau.enable	0 or 1	0
If 0, the Ekahau Real-Time Location System (RTLS) is disabled. If 1, the Ekahau RTLS is enabled.		
wifi.rtls.ekahau.port	0 to 65535	8552
The port number of the Ekahau Positioning Engine.		
wifi.rtls.ekahau.txInterval	0 to 2	0
The maximum time between 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.		

Save the Central Provisioning Server .cfg Files

Save the files you have created in a separate folder in a convenient location. Later you will copy these to the central provisioning server.

Ensure that the .cfg files have the correct extension. Some XML editors append “.xml” to a filename when the file is saved. For example site.cfg.xml. Rename any files and delete the .xml extension so that they only show the .cfg extension.

Chapter 8: Configuring Wireless Parameters (without SLIC)



Admin Tip: Using SLIC

The Spectralink Installation and Configuration (SLIC) tool is the preferred and recommended method for configuring wireless parameters. See Chapter 1: **Quick Start with SLIC** for additional information.

For those using SLIC, this chapter provides detailed information about wireless configuration parameters.

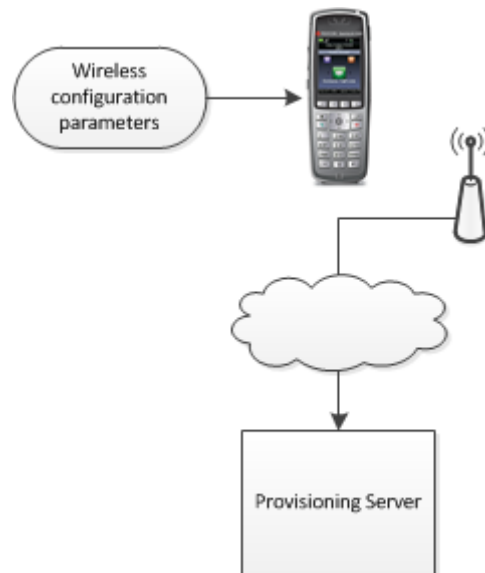
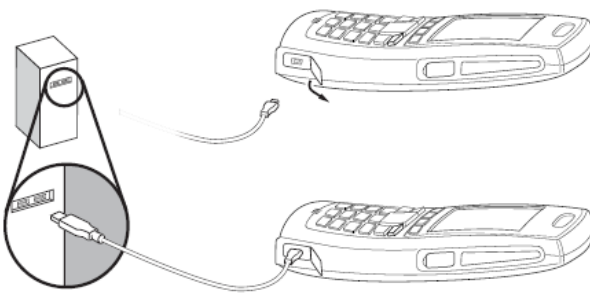
Wireless parameters are configured on an initial provisioning computer by filling in the values in the wireless.cfg file using an XML editor, then loading the file into each phone over a USB MicroB. These parameters enable the phone to associate with the wireless LAN and find the central provisioning server and other components. Once the central provisioning server is accessed, the handset gets the rest of the files and parameters it needs from it.

This chapter explains how to configure the wireless parameters. The deployment chapter explains how to load them into the handset.

Load the file into each handset

then

the handset associates with the wireless LAN and accesses the provisioning server



Prepare to Configure the Wireless Settings

Wireless settings are listed in Chapter 4. Review the list and ensure you have the necessary information before you start.

You can use the same computer to provision the wireless settings that you used to configure the central provisioning server .cfg files in Chapter 5. Just be sure to keep the wireless settings in a separate folder.

The USB_Setup folder

Two files are in the USB_Setup folder. You only need to configure the wireless.cfg file.

- 000000000000.cfg
- wireless.cfg

The 000000000000.cfg file directs the handset to the wireless.cfg file to obtain the parameters it needs. The 000000000000.cfg template is already set up for this and needs no changes. Save this file to a convenient location. Do not change the filename.



Admin Tip: Save the USB_Setup files

Save the wireless.cfg configuration file and initial 000000000000.cfg file in a separate secure folder you will be able to locate when it is time to download them to the phones. We will describe how to use these files to get your phone onto the wireless network in a later section of the Guide.

Configure wireless.cfg

The wireless.cfg file contains the parameters (settings, provisioning server IP and protocol, set the Regulatory Domain for the local domain, turn on the proper 802.11a/b/g radio and enable channels, etc.) that the phone requires in order to associate with the wireless LAN.



When you will see a separate .set parameter

Only the device.x parameter uses the mechanism that requires a set=1 parameter to confirm the parameter value. The device.x parameter is disabled by set=0. You will not see the .set parameter used with any other type of parameter. The device.x parameters are those which are loaded during the initial provisioning process with the wireless.cfg file. Examples are: device.set="1", device.dhcp.enabled.set="1", device.dhcp.enabled="1", etc.



Settings: Each <device/> Parameter has a Corresponding .set Parameter with One Exception

Note that each <device/> parameter has a corresponding .set parameter that enables or disables the parameter. There is one exception to this rule: the `device.sec.TLS.customDeviceCertX.set` parameter applies to both `device.sec.TLS.customDeviceCertX.publicCert` and to `device.sec.TLS.customDeviceCertX.privateKey`.

USBnet

USBnet configuration allows the wireless parameters to be written to the phone and then disables the USB connection to prevent future conflicts once the phone is connected to the central provisioning server. Do not change the template values.

```
<WriteDeviceConfig
  device.set="1">
  <!--USBnet is only used for initial provisioning. -->
  <!--Disabling it here prevents system conflicts after configuration is done.-->
  <usbnet
    device.usbnet.enabled="0"
    device.usbnet.enabled.set="1" />
  </WriteDeviceConfig>
```

Parameter	Permitted Values	Default
device.set	0 or 1	0
If set to 1, use the <code>device.xxx</code> fields that have <code>device.xxx.set=1</code> . Use the 1 value for initial provisioning.		
device.usbnet.enabled	0 or 1	0
If 0, USBNet is disabled. If 1, USBNet is enabled. USBNet must be disabled here.		

PhoneAdminPassword

The Admin Password is the password that is required to access the Advanced settings in the phones' Settings menu. This password protects the phones from being inadvertently disabled due to inexpert changes to its administrative settings. For efficient administration, this password should be the same for all phones and is therefore in this file.

The phones' admin password is configured here so it is not visible in the `site.cfg` file. The default value is 456. This is the password that a user must enter to access the Advanced Settings on the Settings menu on the phone.

Enter a value and change set to 1.

```
<!--Phone admin password is configured here so it is not visible in the site config file-->
<PhoneAdminPassword
  device.auth.localAdminPassword=""
  device.auth.localAdminPassword.set="0" />
```

Parameter	Permitted Values	Default
device.auth.localAdminPassword	string (32 character max)	456
<p>The phone's local administrative password. The minimum length is defined by sec.pwd.length.admin. If not defined, the default length is 1.</p> <p>Enter the default password or change it as desired in the device.auth.localAdminPassword parameter and change the set parameter to 1.</p>		

Special characters

Key	Number of presses								
	1	2	3	4	5	6	7	8	9
1	!		'	^	\	@	:	1	
*	.	*	-	&	%	+	;	()
0	/	,	_	\$	~	=	?	0	
#	#	>	<	{	}	[]	"	`



Special characters in passwords

Some passwords may contain special characters that the phone cannot produce. The special characters listed above are the only ones available in the phone. If your password contains other special characters, you will need to change it to include only those available in the phone.

Provisioning Server

Set the parameters for the central provisioning server requirements.

FTPS and HTTPS use TLS certificates for authentication and require a few more parameters.

```

<!-- ***** -->
<!-- * Configuration Provisioning * -->
<!-- ***** -->
<!--Provisioning Server types: 0-FTP, 1-TFTP, 2-HTTP, 3-HTTPS, 4-FTPS-->
<ProvisioningServer
    device.dhcp.bootSrvUseOpt="CustomAndDefault"
    device.dhcp.bootSrvUseOpt.set="0"
    device.dhcp.bootSrvOpt="160"
    device.dhcp.bootSrvOpt.set="0"
    device.prov.serverType=""
    device.prov.serverType.set="0"|
    device.prov.serverName=""
    device.prov.serverName.set="0"
    device.prov.user=""
    device.prov.user.set="0"
    device.prov.password=""
    device.prov.password.set="0" />

```

Parameters that apply to all types of provisioning servers.

Parameter	Permitted Values	Default
device.dhcp.bootSrvUseOpt	Default, Custom, Static, CustomAndDefault	Null
<p>Default The phone will look for option number 66 (string type) in the response received from the DHCP server. The DHCP server should send address information in option 66 that matches one of the formats described for <code>device.prov.serverName</code>.</p> <p>Custom The phone will look for the option number specified by <code>device.dhcp.bootSrvOpt</code>, and the type specified by <code>device.dhcp.bootSrvOptType</code> in the response received from the DHCP server.</p> <p>Static The phone will use the boot server configured through the provisioning server <code>device.prov.*</code> parameters.</p> <p>Custom and Default The phone will use the custom option first or use Option 66 if the custom option is not present.</p>		
device.dhcp.bootSrvOpt	Null, 128 to 254	160
When the boot server is set to <i>Custom</i> or <i>Custom+Option66</i> , specify the numeric DHCP option that the phone will look for.		
device.prov.serverType	FTP, TFTP, HTTP, HTTPS, FTPS	Null
The protocol the phone uses to connect to the provisioning server. <i>Note:</i> Active FTP is not supported for BootROM version 3.0 or later. <i>Note:</i> Only implicit FTPS is supported.		
device.prov.serverName	dotted-decimal IP address, domain name string, or URL	Null
<p>The IP address, domain name, or URL of the provisioning server, followed by an optional directory and optional configuration filename. This parameter is used if DHCP is disabled (<code>device.dhcp.enabled</code> is 0), if the DHCP server does not send a boot server option, or if the boot server option is static (<code>device.dhcp.bootSrvUseOpt</code> is <i>static</i>).</p> <p><i>Note:</i> If you modify this parameter, the phone will re-provision. The phone may also reboot if the configuration on the provisioning server has changed.</p>		
device.prov.user	string	Null
<p>The user name required for the phone to log in to the provisioning server (if required).</p> <p><i>Note:</i> If you modify this parameter, the phone will re-provision. The phone may also reboot if the configuration on the provisioning server has changed.</p>		

Parameter	Permitted Values	Default
device.prov.password	string	Null
The password for the phone to log in to the provisioning server. Note that a password may not be required. <i>Note:</i> If you modify this parameter, the phone will re-provision. The phone may also reboot if the configuration on the provisioning server has changed.		

If using FTPS or HTTPS, a certificate must be installed. See below [WPA2-Enterprise](#) for more information about managing Platform Profiles and their associated certificates. Essentially you will load the certificate and assign it to a Platform Profile and then use the following parameter to link it to the provisioning server.

Parameter	Permitted Values	Default
device.sec.TLS.profileSelection.provisioning¹	PlatformProfile1, PlatformProfile2	Null
The Platform Profile to use for provisioning.		

WirelessSettings

Wireless settings include those parameters that are necessary for establishing a wireless connection between the phones and access points. You will need to be familiar with your access points and their settings in order to set many of these parameters correctly.

SSID

You will need to enable Wi-Fi and set the value of the SSID in your system.

```
<WirelessSettings
  device.wifi.enabled="1"
  device.wifi.enabled.set="1"
  device.wifi.ssid=""
  device.wifi.ssid.set="1">
```

Parameter	Permitted Values	Default
device.wifi.enabled	0 or 1	1
If 0, the wireless interface is disabled. If 1, the wireless interface is enabled.		
device.wifi.ssid¹	String	Null
The Service Set Identifier (SSID) of the wireless network.		
device.wifi.dot11n.enabled	0 or 1	1
If 0, 802.11n support is disabled. If 1, 802.11n support is enabled.		

Wi-Fi Radio Settings

Some of these settings will be familiar from setting up other wireless devices and some pertain only to telephony radio usage. The frequencies that are permitted to wireless telephony devices are strictly regulated by country or domain and each country establishes its own set of rules.

If you are deploying 802.11n, set `device.wifi.dot11n.enabled` to 1. More information about 802.11n can be found in the Spectralink white paper *Deploying Enterprise-Grade Wi-Fi Telephony*. See the references section in the front of this document for more information.

Determine which domain you are in and the radio settings you will need by referring to the pertinent tables below.

Regulatory Domain

Set your regulatory domain by country/area.

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



Caution: North America regulatory domain warning

If you are in North America, only regulatory domain 1 is permitted. If any other domain is set, 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.

Parameter	Permitted Values	Default
device.wifi.radio.regulatoryDomain	1, 2, or 10	Null

The regulatory domain. The supported values are 1 (North America), 2 (Europe and 10 (Australia). The domain must be set in order for the phones to associate with the wireless LAN.



Note: Country code vs. Domain name

In former releases of the software, the domain name was referred to as the country code and the parameter was `device.wifi.radio.countryCode`.

Radio Frequency 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 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 84-Series handsets are to use (either 2.4 GHz or 5 GHz, not both).

You will need to set sub-bands for the 5 GHz frequency and transmit power for both frequencies.

Subbands for the 5GHz Band

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. Enable only the same bands and sub-bands as are configured on your wireless infrastructure, otherwise the handsets will waste time looking for a signal on the unused sub-bands and roaming performance will be impaired.



Warning Do not enable all sub-bands

Do not enable all bands and sub bands in the WLAN or the phone. This will cause the phone to have a very long channel scanning cycle which causes poor roaming and poor audio. See *Best Practices for Deploying Spectralink 84-Series Handsets* White Paper. The link is in the Recommended Reading section.



Caution: Sub-bands

The Spectralink 84-Series handset menus will display all four 5GHz 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 and available in the WLAN.

The following tables identify which channels are available in your domain.

For Regulatory Domain 1:

<i>Sub-band for 5 GHz Band</i>	<i>Channel</i>	<i>DFS (Yes/No)</i>
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:

<i>Sub-band for 5 GHz Band</i>	<i>Channel</i>	<i>DFS (Yes/No)</i>
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:

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

Transmit Power

For 2.4 GHz and each sub-band of 5 GHz, you will need to set the maximum transmit power level the handset will use. If the APs use transmit power control, the handset listens to TPC elements in the beacons or probe response frames and will reduce or increase its power to match what the AP advertises but never exceeds the power setting set here.

P1..P6 limits the TX power to the existing definition of P1..P6

- When TPC is enabled, it may further reduce the phone's transmit power from the power specified in the menu, but will never exceed it.
- if you set Tx for a sub-band that can't go that high, the phone will display a regulatory domain error

P7 is the highest power possible for that sub-band

- When TPC is enabled, it may further reduce the phone's transmit power
- P7 is also called "Auto" in various menus
- P7/Auto is the default setting

If no maximum is set, the handset uses the Auto/P7 settings for each channel activated.

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

For all Regulatory Domains:

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

* Indicates default setting

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

For Regulatory Domains 1 and 10:

<i>Maximum Power for 2.4 GHz Band</i>	<i>Definition</i>
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)
Auto/P7	MAX (maximum allowable power for that channel and data rate)

* Indicates default setting

For Regulatory Domain 2:

<i>Maximum Power for 2.4 GHz Band</i>	<i>Definition</i>
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)
Auto*	MAX (maximum allowable power for that channel and data rate)

* If P4 or above is selected for domain 2, the handset will broadcast at the maximum allowable power which is 12 mW.

Radio parameters

```

<WiFiRadioSettings
  device.wifi.radio.regulatoryDomain=""
  device.wifi.radio.regulatoryDomain.set="1"
  device.wifi.dot11n.enabled="1"
  device.wifi.dot11n.enabled.set="0">
  <WiFiRadioSettings.2_4GHz_band
    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" />
  <WiFiRadioSettings.5GHz_band
    device.wifi.radio.band5GHz.enable=""
    device.wifi.radio.band5GHz.enable.set="0">
    <band5GHz.subBand1
      device.wifi.radio.band5GHz.subBand1.enable=""
      device.wifi.radio.band5GHz.subBand1.enable.set="0"
      device.wifi.radio.band5GHz.subBand1.txPower=""
      device.wifi.radio.band5GHz.subBand1.txPower.set="0" />
    <band5GHz.subBand2
      device.wifi.radio.band5GHz.subBand2.enable=""
      device.wifi.radio.band5GHz.subBand2.enable.set="0"
      device.wifi.radio.band5GHz.subBand2.txPower=""
      device.wifi.radio.band5GHz.subBand2.txPower.set="0" />
    <band5GHz.subBand3
      device.wifi.radio.band5GHz.subBand3.enable=""
      device.wifi.radio.band5GHz.subBand3.enable.set="0"
      device.wifi.radio.band5GHz.subBand3.txPower=""
      device.wifi.radio.band5GHz.subBand3.txPower.set="0" />
    <band5GHz.subBand4
      device.wifi.radio.band5GHz.subBand4.enable=""
      device.wifi.radio.band5GHz.subBand4.enable.set="0"
      device.wifi.radio.band5GHz.subBand4.txPower=""
      device.wifi.radio.band5GHz.subBand4.txPower.set="0" />
  </WiFiRadioSettings>

```

Wi-Fi Security

Please refer to the Spectralink white paper *Understanding Wireless Security on Your Spectralink 84-Series Wireless Telephones* for detailed information about security choices. See the references section in the front of this document for the link.

Wireless security is configured using SLIC or using the USB method. Although tedious, methods that do not require certificates can also be configured manually by entering the information through the keypad using the Admin menus. For SLIC see *Spectralink Installation and Configuration Tool Administration Guide*. For the USB method see [Configuring Wireless Parameters \(without SLIC\)](#). These methods are supported:

- None

- WEP
- WPA-PSK, WPA2-PSK
- WPA2-Enterprise
 - EAP-TLS
 - PEAP
 - EAP-FAST



Caution: If using USB method, delete unused security parameters

You may only deploy one security method or no security method. To prevent configuration conflicts and consequent inoperability, delete the unused security folders.

Parameter	Permitted Values	Default
device.wifi.securityMode	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise	Null
The wireless security modes that are available.		

None

If you do not want to use any security method, enter **None** as the value.

Example: None configuration

```
<WiFiSecurity.None
  device.wifi.securityMode="None"
  device.wifi.securityMode.set="1"/>
```

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 84-Series handsets do not support key rotation. During operation, only one key can be used by the phone.

Parameter	Permitted Values	Default
device.wifi.wep.authType	0, 1	0
The Wi-Fi WEP authentication type. 0 = Open System, 1= Shared Key		
device.wifi.wep.defaultKey	1 to 4	1
Specifies which of the four keys from <code>device.wifi.wep.key1</code> to <code>device.wifi.wep.key4</code> is used.		
device.wifi.wep.encryptionEnable	0 or 1	1
If 0, WEP encryption is disabled. If 1, WEP encryption is enabled.		

Parameter	Permitted Values	Default
device.wifi.wep.key1	String	Null
device.wifi.wep.key2	String	
device.wifi.wep.key3	String	
device.wifi.wep.key4	String	
The WEP hexadecimal key with a 40-bit or 104-bit length, as specified by <code>device.wifi.wep.keyLength</code> .		
device.wifi.wep.keyLength	0 or 1	1
The length of the hexadecimal WEP key. 0 = 40-bits, 1 = 104-bits.		

Example WEP parameters

```
<WiFiSecurity.WEP
  device.wifi.securityMode="WEP"
  device.wifi.securityMode.set="0"
  device.wifi.wep.authType="0"
  device.wifi.wep.authType.set="0"
  device.wifi.wep.defaultKey="1"
  device.wifi.wep.defaultKey.set="0"
  device.wifi.wep.encryptionEnabled="1"
  device.wifi.wep.encryptionEnabled.set="0"
  device.wifi.wep.key1=""
  device.wifi.wep.key1.set="0"
  device.wifi.wep.key2=""
  device.wifi.wep.key2.set="0"
  device.wifi.wep.key3=""
  device.wifi.wep.key3.set="0"
  device.wifi.wep.key4=""
  device.wifi.wep.key4.set="0"
  device.wifi.wep.keyLength="1"
  device.wifi.wep.keyLength.set="0" />
```

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.

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 84-Series handsets can use either the PSK or passphrase form in the configuration.



WPA-Personal and WPA2-Personal Encryption

The Spectralink 84-Series handsets can use one encryption policy or the other but not both at the same time. Spectralink 84-Series handsets run on an SSID that uses either AES or TKIP, not both. If both are set the handset will not associate to the AP.

Parameter	Permitted Values	Default
device.wifi.psk.keyType The key type: key or passphrase.	0 or 1	1
device.wifi.psk.key The hexadecimal key or ASCII passphrase.	string	Null

The WPA(2) PSK key type and key. If the key type is 0, a 256-bit hexadecimal key is used. If the key type is 1, a string of 8 to 63 ASCII characters is used as the passphrase.

Example WPA-PSK / WPA2-PSK parameters

Delete the security mode you aren't using, either WPA-PSK or WPA2-PSK.

```
<!--WPA-PSK or WPA2-PSK-->
<!--Key Types: 0-preshared key(64 hex char), 1-Passphrase/Password (8-63 ASCII char)-->
<!--Delete the security mode, either WPA-PSK or WPA2-PSK you do not use.-->
<WiFiSecurity.WPA2PSK
  device.wifi.securityMode="WPA-PSK"
  device.wifi.securityMode="WPA2-PSK"
  device.wifi.securityMode.set="0"
  device.wifi.psk.keyType="1"
  device.wifi.psk.keyType.set="0"
  device.wifi.psk.key=""
  device.wifi.psk.key.set="0" />
```

WPA2-Enterprise

WPA2-Enterprise uses Extensible Authentication Protocol (EAP) types supported for authentication. The Spectralink 84-Series handsets support three common methods: EAP-TLS, PEAPv0/-MSCHAP/-v2 and EAP-FAST. All of these require that a certificate be installed on the handset so the phone can authenticate the RADIUS server (and prevent a man-in-the-middle attack). Each type uses a different approach for authentication.

- **EAP-TLS.** The server certificate is issued by a Certificate Authority (CA). Both the handset and the server contain a CA certificate that is authenticated by the corresponding server/device for mutual authentication, thus establishing a secure "tunnel" for communications.
- **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 server 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 Cisco refers to as 'Phase Zero Provisioning'.

Fast roaming techniques

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 each time it roams. Instead, the handsets can enable 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 84-Series handsets support both methods of fast roaming for WPA2-Enterprise.

Set WPA2-Enterprise method

For whichever method you deploy, you will need to set the method, the roaming and the username and password. Note that for EAP-TLS, the username is called the "identity". Note that for EAP-FAST you will also need to set in-band or out-of-band provisioning.

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
device.wifi.wpa2Ent.method	1=EAP-TLS, 2=EAP-PEAPv0/MSCHAPv2, 6=EAP-FAST	Null
The Extensible Authentication Protocol (EAP) to use for 802.1X authentication.		
device.wifi.wpa2Ent.roaming	0=OKC, 1=CCKM	Null
The WPA2-Enterprise fast roaming method. If OKC , Opportunistic Key Caching (OKC) is used. If CCKM , Cisco Centralized Key Management (CCKM) is used. The fast roaming methods allow part of the key derived from the server to be cached in the wireless network to shorten the time it takes to renegotiate a secure handoff.		
device.wifi.wpa2Ent.user	String	Null
The WPA2-Enterprise user name.		
device.wifi.wpa2Ent.password	String	Null
The WPA2-Enterprise password.		
device.wifi.wpa2Ent.eapFast.inBand Prov	0 or 1	
If 0, the PAC file is initially loaded into to the handset during configuration (called <i>out-of-band</i>). If 1, the PAC file is automatically loaded form the network (called <i>in-band</i>).		

Install certificate (if required)

WPA2-Enterprise methods require some sort of authentication. If you will deploy certificates at initial provisioning (the most secure method) then the certificates must be loaded and assigned in the wireless.cfg file in a 3-step process.

1 Loading the certificate

2 Assigning the certificate to a Platform Profile**3** Connecting the platform profile to the Wi-Fi (dot1x) method.

Two slots are available for certificates used by Wi-Fi: Platform1 and Platform2. When certificates are loaded and assigned for Wi-Fi security, the platform can also be used by other servers. More information is available in the Admin Guide about types of servers that can use certificates.

CA certificates are used by EAP-TLS and PEAP.

<i>Parameter</i>	<i>Permitted Values</i>	<i>Default</i>
device.sec.TLS.customCaCert1 (Platform Profile 1) device.sec.TLS.customCaCert2 (Platform Profile 2)	string	Null
Load the certificate.		
device.sec.TLS.profile.caCertList1 (Platform Profile 1) device.sec.TLS.profile.caCertList2 (Platform Profile 2)	Builtin, BuiltinAndPlatform1, BuiltinAndPlatform2, All, Platform1, Platform2, Platform1AndPlatform2	All

Although a number of different combinations are permitted, Spectralink recommends that you set the value to the Platform that corresponds to the customCaCert entered for `device.sec.TLS, customCaCertx`: Platform1 or Platform2.

device.sec.TLS.profileSelection.dot1x	PlatformProfile1, PlatformProfile2	PlatformProfile1
This setting links the certificates specified in the <code>CaCertListx</code> (1 or 2) to the Wi-Fi security method (dot1x) you specified in <code>device.wifi.wpa2Ent.method</code> .		

PAC files are used by EAP-FAST and do not use Platform Profiles.

<i>Parameter</i>	<i>Permitted Value</i>	<i>Default</i>
device.pacfile.data	String	Null
EAP-FAST only, optional. The PAC file (base 64 encoded). To generate a base 64-encoded PAC file, generate the PAC file using your authentication server and then convert it to base 64. You can convert the file to base 64 using the following openssl commands: <pre>\$ openssl enc -base64 -in myfile -out myfile.b64</pre>		
device.pacfile.password	String	Null
EAP-FAST only, optional. The password for the PAC file.		

Example configurations

EAP-TLS parameters

```

<!--EAP-TLS-->
<!--Enter username and install certificates-->
<!--WPA2 Enterprise Methods: 1-EAP-TLS, 2-PEAP, 6-EAP-FAST-->
  <WPA2Enterprise.EAP-TLS
    device.wifi.securityMode="WPA2-Enterprise"
    device.wifi.securityMode.set="1"
    device.wifi.wpa2Ent.method="EAP-TLS"
    device.wifi.wpa2Ent.method.set="1"
    device.wifi.wpa2Ent.user="[MACAddress]"
    device.wifi.wpa2Ent.user.set="1" />
  <!--Install Certificates-->
  <certificate
    device.sec.TLS.customCaCert1="[Certificate]"
    device.sec.TLS.customCaCert1.set="1"
    device.sec.TLS.profile.caCertList1="Platform1"
    device.sec.TLS.profile.caCertList1.set="1"
    device.sec.TLS.profileSelection.dot1x="PlatformProfile1"
    device.sec.TLS.profileSelection.dot1x.set="1" />

```

PEAP parameters

```

<!--PEAP-->
<!--Enter username and password and install certificates.-->
<!--WPA2 Enterprise Methods: 1-EAP-TLS, 2-EAP-PEAPV0-MSCHAPv2, 6-EAP-FAST-->
<!--PEAP does not require a certificate.-->
  <WPA2Enterprise.PEAP
    device.wifi.securityMode="WPA2-Enterprise"
    device.wifi.securityMode.set="1"
    device.wifi.wpa2Ent.method="EAP-PEAPV0-MSCHAPv2"
    device.wifi.wpa2Ent.method.set="1"
    device.wifi.wpa2Ent.user=""
    device.wifi.wpa2Ent.user.set="0"
    device.wifi.wpa2Ent.password=""
    device.wifi.wpa2Ent.password.set="0" />
  <!--Install Certificates (if desired)-->
  <!--By default PEAP uses certificate slot "Platform 1"-->
  <device.sec.TLS
    device.sec.tls.customCaCert1=""
    device.sec.tls.customCaCert1.set="0"
    device.sec.TLS.profile.caCertList1="Platform1"
    device.sec.TLS.profile.caCertList1.set="0"
    device.sec.TLS.profileSelection.dot1x="PlatformProfile1"
    device.sec.TLS.profileSelection.dot1x.set="0" />

```

EAP-FAST parameters

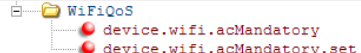
For out-of-band provisioning, delete the unused type of provisioning, in-band or out-of-band.

```
<!--EAP-FAST-->
<!--Enter username and password. Set inBand or outofBand provisioning.-->
<!--WPA2 Enterprise Methods: 1-EAP-TLS, 2-EAP-PEAPv0-MSCHAPv2, 6-EAP-FAST-->
<!--EAP-FAST can be configured with a certificate called a PAC file.-->
  <WPA2Enterprise.EAPFAST
    device.wifi.securityMode="WPA2-Enterprise"
    device.wifi.securityMode.set="1"
    device.wifi.wpa2Ent.method="EAP-FAST"
    device.wifi.wpa2Ent.method.set="1"
    device.wifi.wpa2Ent.user=""
    device.wifi.wpa2Ent.user.set="0"
    device.wifi.wpa2Ent.password=""
    device.wifi.wpa2Ent.password.set="0">

    <!--***DELETE*** unused InBand/OutofBand section from this file-->
    <!--Simply not filling in the unused ones may result in-->
    <!--duplicate parameter errors being reported by the handset-->
    <EAPFAST.InBandProvisioning
      device.wifi.wpa2Ent.eapFast.inBandProv="0"
      device.wifi.wpa2Ent.eapFast.inBandProv.set="0" />
    <EAPFAST.OutOfBandProvisioning
      device.wifi.wpa2Ent.eapFast.inBandProv="0"
      device.wifi.wpa2Ent.eapFast.inBandProv.set="0"
      device.pacfile.data="[PAC file]"
      device.pacfile.data.set="0"
      device.pacfile.password=""
      device.pacfile.password.set="0" />
```

Wi-Fi QoS

If the APs used in your facility enforce admission control or access control, this QoS setting must be configured. Consult your AP documents for specific information about AP requirements and the value of this parameter if not null.

	0
---	---

Parameter	Permitted Values	Default
Device.wifi.acMandatory	0 or 1	Null
If 0, the handset will attempt to connect regardless of whether or not admission control is enforced in the access point.		

DHCP



Spectralink recommends: Use DHCP

Unless you have a compelling reason to use static IP addresses, Spectralink recommends that you use a DHCP server and configure the server for required settings. The *Spectralink Administrators Guide* has additional DHCP settings.

DHCP	
device.wifi.dhcpEnabled	1
device.wifi.dhcpEnabled.set	1

DNS

Set the DNS parameters to appropriate values for your organization. This step is optional. The DNS parameters can be supplied by DHCP.

DNS	
device.hostname	
device.hostname.set	0
device.dns.domain	
device.dns.domain.set	0
device.dns.serverAddress	
device.dns.serverAddress.set	0
device.dns.altSrvAddress	
device.dns.altSrvAddress.set	0

Parameter	Permitted Values	Default
device.hostname The device hostname	string	Null
device.dns.domain The phone's DNS domain.	string	Null
device.dns.serverAddress The primary server to which the phone directs Domain Name System queries.	string	Null
device.dns.altSrvAddress The secondary server to which the phone directs Domain Name System (DNS) queries.	server address	Null

SNTP

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.

Set SNTP parameters to appropriate values for your organization. Typically you will establish the SNTP server name and the GMT offset for your time zone.



Settings: Configuring Your Phone for Local Conditions

Most of the default settings are typically adequate; however, if SNTP settings are not available through DHCP, you will need to edit the SNTP GMT offset, and (possibly) the SNTP server address for the correct local conditions. Changing the default daylight savings parameters will likely be necessary outside of North America. Disable the local Web (HTTP) server or change its signaling port if the local security policy dictates. Change the default location settings for user interface language and time and date format.

#comment	SNTP GMT Offset must be set in seconds
SNTP	
device.snntp.gmtOffset	
device.snntp.gmtOffset.set	0
device.snntp.serverName	
device.snntp.serverName.set	0

Parameter	Permitted Values	Default
device.snntp.gmtOffset	-43200 to 46800	Null
The GMT offset – in seconds – to use for daylight savings time, corresponding to -12 to +13 hours.		
device.snntp.serverName	dotted-decimal IP address or domain name string	Null
The SNTP server from which the phone will obtain the current time.		

Time Zones East of Greenwich

GMT offset	Time Zone Abbreviations	Seconds
GMT+1	CET = Central European Time FWT = French Winter Time (France) MET = Middle European Time MEWT = Middle European Winter Time SWT = Swedish Winter Time (Sweden)	3600
GMT+2	EET = Eastern European Time, USSR Zone 1	7200
GMT+3	BT = Baghdad Time, USSR Zone 2	10800
GMT+4	ZP4 = USSR Zone 3	14400
GMT+5	ZP5 = USSR Zone 4.	18000
GMT+6	ZP6 = USSR Zone 5.	21600
GMT+7	CXT = Christmas Island Time (Australia)	25200

<i>GMT offset</i>	<i>Time Zone Abbreviations</i>	<i>Seconds</i>
GMT+8	CCT = China Coast Time, USSR Zone 7 AWST = Australian Western Standard Time WST = Western Standard Time (Australia)	28800
GMT+9	JST = Japan Standard Time, USSR Zone 8	32400
GMT+10	EAST = East Australian Standard Time EST = Eastern Standard Time (Australia) GST = Guam Standard Time, USSR Zone 9	36000
GMT+11		39600
GMT+12	IDLE = International Date Line East NZST = New Zealand Standard Time NZT = New Zealand Time	43200
GMT+13	NZDT = New Zealand Daylight Time	46800

Time Zones West of Greenwich

<i>GMT offset</i>	<i>Time Zone Abbreviations</i>	<i>Seconds</i>
GMT-1	WAT = West Africa Time	-3600
GMT-2	AT = Azores Time	-7200
GMT-3		-10800
GMT-4	AST = Atlantic Standard Time (Canada)	-14400
GMT-5	EST = Eastern Standard Time (USA & Canada)	-18000
GMT-6	CST = Central Standard Time (USA & Canada)	-21600
GMT-7	MST = Mountain Standard Time (USA & Canada)	-25200
GMT-8	PST = Pacific Standard Time (USA & Canada)	-28800-
GMT-9	AKST Alaska Standard Time (USA) YST = Yukon Standard Time (Canada)	-32400
GMT-10	HST = Hawaii Standard Time HAST Hawaii-Aleutian Standard Time (USA) AHST = Alaska-Hawaii Standard Time (obs) CAT = Central Alaska Time	-36000
GMT-11	NT = Nome Time	-39600
GMT-12	IDLW = International Date Line West	-43200

Part III: Deployment

At this point, you have configured the .cfg files for wireless deployment and for the central provisioning server. The deployment process involves loading these files into their proper location so that the phone can use them. Deployment is a two-step process. The phones are loaded with the wireless parameters and then they associate with the wireless LAN and obtain the rest of the parameters from the central provisioning server. Therefore first we ensure the central provisioning server is set up and then we download the wireless parameters into the phones.

- Setting up the central provisioning server

The top level .cfg files and the site.cfg, group.cfg, any feature.cfg and per-phone or per-user.cfg files must be loaded onto a central provisioning server.

- Wireless deployment

The phones must be loaded with the wireless parameters before they can associate with the wireless LAN. This is done with each phone in turn using an initial provisioning server, usually a laptop, and a microB USB cable that connects the computer to the phone.

- Testing the handsets

We recommend deploying just a few phones at first and testing the features to ensure the parameters have been configured properly. Once you are satisfied that the handsets work as expected, then you can deploy the rest of them.

- Deploying additional phones or features

You may need to add new phones or send phones to RMA for service. This chapter explains how to decommission a phone, add a new or replacement phone and change the configuration or scenario.

Chapter 9: Set up the Central Provisioning Server

This chapter provides basic instructions for setting up a central provisioning server. If you are new to this process, it is important to read every section in this chapter.

A central provisioning server provides central management of software upgrades, language support, configuration management, and diagnostic logging. The handsets connect to the provisioning server over the wireless connection. The provisioning server provides the handsets with configuration parameters required to operate, such as the call server address, the line registrations, and the features that you want to enable on each of the handsets you deploy.

The provisioning server can be set up on the local LAN or anywhere on the Internet. Configuration, log, directory, and override files are normally located on this server. If you allow the phone write access to your provisioning server, the phone can use the server to upload files (such as logs, overrides, and call lists) and store the user's files. The phone is designed such that if it cannot locate a central provisioning server when it boots up, it will operate with internally saved parameters. This is useful when the central provisioning server is not available.



Caution: Provisioning server vs upgrade server

The upgrade server provided through the Web Configuration Utility is entirely different from the provisioning server discussed here. Please see the *Administration Guide* for further details.

Central Provisioning Server Requirements

Depending on the size of the installation, number of 84-Series handsets and any other devices which use the same server to load files, the power and speed of the server (and its system) should match the number of devices which will boot at the same time. In an Enterprise installation it can be common to have hundreds of devices boot and ask for their configuration files.

The amount of disk space required depends on the number of phones deployed. The requirements listed here are suitable for up to 1000 phones.

- O/S: Windows XP SP3 | Windows 2003 Server | Linux/Unix
- RAM: 2GB or more for workstations to 4GB or more for servers
- Disk: 1GB or more recommended for sites over 1000 phones
- Processor: 2GHz or greater
- Network: 1GB Ethernet recommended

A simple provisioning configuration uses File Transfer Protocol or FTP. Although many FTP servers are free, they require installation, and use logins and passwords. A free and popular server, FileZilla Server, is available for Windows. This application has been tested with the UC Software. See Appendix A for instructions about setting up an FTP server.



Tip: Choosing a Provisioning Protocol

By default, Spectralink sets FTP as the provisioning protocol on all Spectralink phones. This guide focuses on the FTP provisioning protocol. Other supported protocols include TFTP, HTTP, and HTTPS. For more information about using these other protocols, contact a Deployment Specialist.



Spectralink recommends: Using RFC-Compliant Servers

Spectralink recommends that you use RFC-compliant servers.

Set up Directories



Spectralink recommends: Configure separate directories

For organizational purposes, Spectralink recommends configuring separate directories for ease of management and maintenance.

Directories were discussed in earlier chapters in connection with the top level .cfg files where the directories are named and the path is the value. Example:

LOG_FILE_DIRECTORY	\Log_Files
OVERRIDES_DIRECTORY	\Overrides
CONTACTS_DIRECTORY	\Contacts
CALL_LISTS_DIRECTORY	\Call_Lists
USER_PROFILES_DIRECTORY	\UserProfiles

The name of the directory is set in the top level .cfg file and the actual folder must be created on the central provisioning server.

File Permissions

The phone will attempt to upload log files, configuration override files, and a directory file to the server if the file is changed. This requires that the phone's account has delete, write, and read permissions. The phone will still function without these permissions, but will not be able to upload files.

**Spectralink recommends: Read and write access**

Spectralink recommends that the phones have full read and write access to each directory.

**Tip: Allowing File Uploads to Your Provisioning Server**

Spectralink recommends that you allow file uploads to the provisioning server. File uploads allow event log files to be uploaded. Log files allow boot and operational status events to be saved to the server. These log files are very important when investigating issues or failures. These log files greatly ease our ability to provide customer support in diagnosing issues that may occur with the phone operation. Override files provide backup copies of changes users make to the handset and to the phone's configuration through the Web server and/or local user keypad interface.

The phone's server account needs to be able to add files that it can write to in the log file directory and the provisioning directory. It must also be able to access files in all directories mentioned in the <MACaddress>.cfg or 000000000000.cfg file. You may make all other files that the phone needs to read, such as the application executable and the standard configuration files read-only through file server permissions if additional security is desired.

Each phone may open multiple connections to the server.

If you know the phone is going to download a file from the server, you should mark the file as read-only.

Downloading Spectralink 84-Series Software Files to the Central Provisioning Server

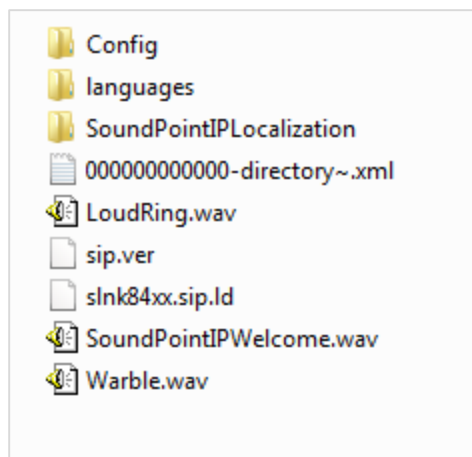
The central provisioning server has been set up as an FTP server. Log into it so that you are in the root directory.

Download the software from the Spectralink support website.

See the *Spectralink 84-Series Wireless Telephone Release Notes* for a detailed description of each file in the distribution and further information on determining which software release to use.

When you download a software version, a notice will display asking you to accept the download of the 84-Series software. Read the notice, click the button indicating that you have read the notice, and click the Submit button to continue the software download.

Extract the files from the distribution zip file. The files will extract with a specific folder hierarchy. Maintain this hierarchy.



If you have set up directories in the same folder, they will be included in the above list. The Config folder contains the templates. You have saved your edited files elsewhere. Leave the templates here.

View the 84-Series Software Files



Admin Tip

In previous software releases, several software filenames were provided based on the hardware id of the 84-Series handset. E.g. 3111-36150-001.sip.ld was the software for the 8440 handset model. With Spectralink Software Release 4.3.x/4.4.x and later, a unified software file is deployed that is applicable for all hardware models (the 8440, 8441, 8450, 8452, and 8453 handset models).

If you are upgrading your system or adding 8441/8453 handsets to an existing installation of 8440/8450/8452 handsets, please consult Appendix B for upgrading instructions.

Starting with the 4.7.0 release, both the non-Lync and MS Lync 84-Series handset models are supported within the same major release, but there are different firmware images for Lync and SIP handset models. See [Telephony Server Variations](#) for complete information about handset models.

- the non-Lync firmware file is named **slnk84xx.sip.ld**.
- the Lync firmware file is named **slnk84xx.lync.ld**.

Copy your custom .cfg files to the appropriate folders

Part II Configuration walked you through the creation of your own central provisioning server configuration files. Now these need to be loaded onto the server.

Load the central provisioning server .cfg files into the top level of the folder hierarchy. This includes the 000000000000.cfg or MACaddress.cfg top level files, the site.cfg and any group or feature .cfg files and any per-phone files.

If you are using User Profiles and have set up a USER_PROFILES Directory, load the per-user login.cfg files into it. If you have not created a special directory for them, load them into the top level.



Admin Tip: What about the wireless.cfg file?

The wireless.cfg file and the initial 000000000000.cfg file will be loaded directly into the handsets via the Micro B USB cable. Do not load them onto the central provisioning server.

Ensure the Provisioning Server is available on the LAN

Once the phones get their wireless .cfg file, they will immediately reboot and connect to the wireless LAN and seek the central provisioning server. Ensure they can find it by checking to see if it is available on the network.

Chapter 10: Wireless Deployment

The handsets will be able to associate with the wireless LAN after you download the wireless.cfg file that contains the wireless parameters into the handsets via a microB USB cable.



Power Tip: Load files onto provisioning server before doing this step

Once the phones receive their wireless parameters, they will associate with the wireless LAN and look for the provisioning server. In the last chapter, the provisioning server was configured and loaded with the .cfg files that the phones will request. Be sure that step is done before loading the wireless files into the phones.



Admin Tip: Not using SLIC?

The following section explains how to set up a temporary initial provisioning computer. This step is not needed if you are using SLIC for initial deployment. See *Spectralink Installation and Configuration Tool Administration Guide* for more information about using SLIC.

Identify a Suitable Initial Provisioning Computer

Because the handsets cannot access the wireless LAN before their wireless settings are configured, you will need to establish a wired connection between a computer and each handset and load the wireless settings via a USB Micro B connection. We will call this computer the initial provisioning computer. It is a temporary setup and does not require exceptional resources in the computer. Only one 84-Series handset is loaded at a time. Requirements are:

- USB port
- USB Micro B cable (available from Spectralink)
- Enough memory for the operation (minimal)
- FTP installed per Appendix A



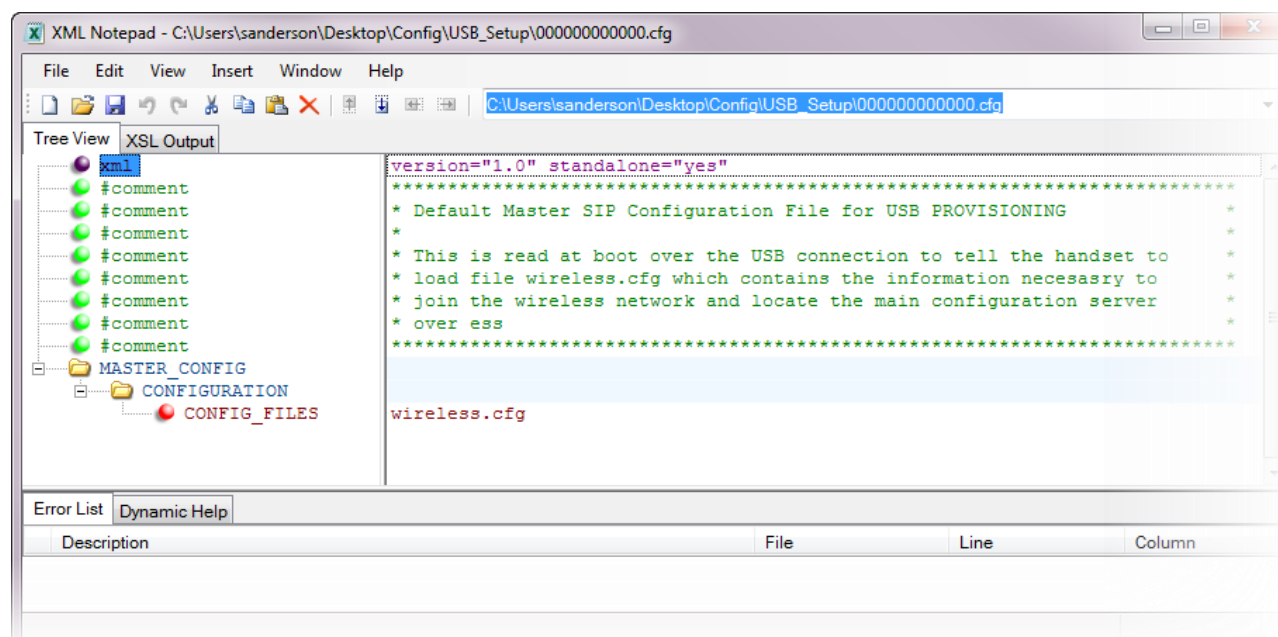
Settings: FTP username and password

When you set up the initial provisioning server as an FTP server, use **administrator** for the username and **admin123** for the password. Ensure all checkboxes are checked.

- The original 000000000000.cfg file from the USB_Setup folder.

- The wireless.cfg file configured in Chapter 7.

Screen shot of the 000's file pointing to wireless.cfg.



Enable the Handset's Network Capabilities

If the initial provisioning computer is not running Microsoft Windows 7, you will need to load a USB driver so that the computer can detect your Spectralink 84-Series handsets as a USB network device. Copy the correct 84xx.inf to it, using the steps itemized below, 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 Windows 7 or 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 Download and copy 84xx.inf onto your 32-bit computer or copy 84xx-64.inf onto your 64-bit computer from the Spectralink support site to an accessible location.

When the 84-Series handset is plugged in (using the USB cable) and the computer asks for a driver, specify the location where you saved the .inf file.

Download the Wireless Configuration to the Handsets

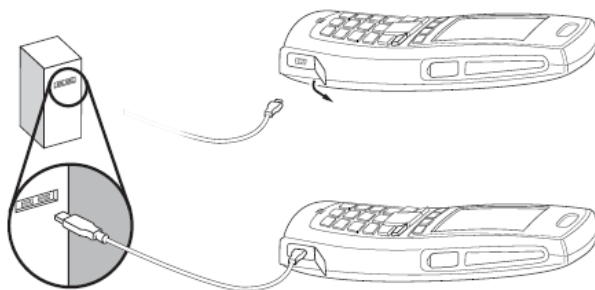
Each scenario has its own set of features to be tested and informs what sample set should be the first to deploy. Select a sample subset of phones for your initial deployment that will span the variety of features you have deployed to different users, or if all users will be deployed with the same features, choose two phones.



Admin Tip: Ensure the handset is at its default settings

Perform a Reset to Factory. [Navigate to **Settings> Advanced Settings> [Default Password is 456]> Administration Settings> Reset To Defaults> Reset To Factory.**] on any handset that has been modified from its out of the box configuration.

- 1 Ensure that the initial provisioning computer is functioning as an FTP server.
- 2 On the initial provisioning computer load the wireless.cfg file into the FTP root directory.
- 3 Apply power to 84xx handset.
- 4 Connect micro-USB cable between the 84xx handset and initial provisioning computer.



- 5 (Conditional) The Found New Hardware wizard opens. Connecting the handset to the initial provisioning computer launches the Found New Hardware wizard automatically. The Found New Hardware wizard only displays the first time you use each USB slot on your computer.
 - a Select No, not this time, and click Next.
 - b Select Install from a list or specific location (Advanced) and click Next.
 - c Select Search for the best driver in these locations.
 - d Select the check box for Include this location in the search:
 - e Browse to your 84xx.inf or 84xx-64.inf and click Next.
 - f The Linux USB Ethernet/RNDIS Gadget is installed.
 - g A warning will be displayed indicating this driver has not passed Windows Logo testing. Select Continue Anyway.

h Click Finish.

Depending on the USB port you choose on the initial provisioning computer, 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.

**Admin Tip: Always use the same USB port.**

If a different USB port is used the next time you download .cfg files to the phones, it will probably indicate it does not have a driver and needs to install one. Therefore use the same USB port for this operation every time you download these files to the phones.

- 6** The handset will download the wireless configuration and then reboot making a tweedle noise when finished.
- 7** (Conditional) If handsets do not immediately (within 10 seconds) download and reboot after plugging the USB into them, you can manually force the configuration download by navigating to the Settings menu on the handset: **Settings> (1)Basic Settings> (6)Update Configuration> Yes**. If you use this option, **Updating...** remains on the display until it is finished.
- 8** Once the handset reboots, disconnect the USB cable from 84xx handset and allow it to download the rest of its configuration files from the provisioning server.

**Caution: Do not disconnect the phone prematurely**

When the 84-Series handset reboots it has downloaded its wireless.cfg file and the USB cable can be disconnected. The phone will boot and connect to the WLAN to load the rest of its configuration files from the provisioning server.

**How long does it take for the handsets to download the rest of the configuration files?**

Note that when handsets connect to the WLAN they will request the rest of the .cfg files that are located on the provisioning server. The handsets may take 1-10 minutes to fully configure and be ready for testing or end user functionality.

- 9** Test the first few handsets to be sure your configuration is working as desired. Go to Chapter 9 to conduct a test of the phones before deploying the remaining phones.

**Admin Tip: Re-downloading the software**

If something has gone wrong and the configuration needs to be edited and the phone needs to be redeployed, reset factory defaults and start over at step 3 above.

- 10** Use the Optimizations pointers below if deploying a quantity of handsets.

Optimization Pointers for Quantity Deployment

You can speed up the deployment of the rest of the handsets by following these pointers:

- Ensure you have a fully charged battery for each handset.
- All handsets must be in factory default state. If handsets have been modified, return them to the factory default state.
- Install batteries and power up all handsets.
- One at a time, plug the USB cable into each handset. The handset will download the .cfg file and reboot. Unplug the handset and repeat with next handset.

**Caution: Do not overload the APs during initial deployment**

A single AP can handle many handsets during this initial configuration time. But may be over-loaded if too many 84-Series handsets are powered up and loading code or files. After 15 or so are loaded and fully functional, power off or move the handsets out of range so the number of handsets using the one AP is limited.

Which Phone Goes to Which User?

At the end of the deployment sequence, you will have a pile of phones to distribute to users throughout your facility. When you turn on the phone, the screen will display a label below the status bar. This label is commonly an extension, but it could be a name or a combination of a name and an extension. Use the label to determine which user should receive the phone. Refer to your User List as needed.

Storing Wireless Configuration Files

Maintenance chores will require that you occasionally reload a phone with the wireless.cfg file. Therefore you will want to maintain an initial configuration computer and store the files on it so that they are easily accessible when you need them. We recommend using a different computer

than the central provisioning server for this purpose due to usually conflicting FTP requirements between initial and central provisioning.

The wireless.cfg file and the 000000000000.cfg file in the USB_Setup folder are only used for the initial deployment of new phones, RMA replaced phones or after a phone is reset to factory defaults.

During deployment, the 000000000000.cfg and wireless.cfg files should be located on the initial provisioning computer in the directory identified by the FTP profile administrator with the password admin123.

Chapter 11: Testing the Handsets

Once the handsets have associated with the wireless LAN, loaded files from the provisioning server and registered with the SIP server it should be able to make and receive calls and utilize all other features that have been configured.

Wireless LAN Association

You can tell if the phone is associating with the wireless LAN by the state of the RF signal strength bar icons in the upper left hand corner of the display. A phone that is associating with the wireless network will have 1 to 4 white bars on its RF signal strength indication icon in the upper left hand corner of the screen when it has fully connected to the WLAN. If the phone cannot associate with the wireless network, it will display a red X over the RF signal strength icon.

Test Configured Features

Now is the time to test configured features, one at a time, to ensure they are working on a few representative phones before deploying all of them.



Caution: Testing parameter interaction is required

Though individual parameters are checked to see whether they are in range, the interaction between parameters is not checked. If a parameter is out of range, an error message will display in the log file and parameter will not be used.

Incorrect configuration can put the phones into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, and server B has a configuration file that specifies that server A should be used.

To detect errors, including IP address conflicts, Spectralink recommends that you test the new configuration files on two phones before initializing all phones.

Return to Chapter 9 and finish deploying the rest of the phones.

Chapter 12: Deploying Additional Phones or Features

After your initial installation you may decide to add more phones, expand the feature set or you may need to repair a phone and redeploy it. This chapter covers the sequence of actions you should take when these situations occur.

Adding New Phones

When you get new phones from the factory, they need to be provisioned and deployed in your facility in the same manner you used with the first set. This is why we stored your initial 000000000000.cfg and wireless.cfg files on the initial provisioning server—so you could find them again when phones needed to be added.

You will once again need to determine which Scenario you will be using per the discussion in Chapter 5. Are these new phones part of an already-established Scenario or are you expanding your system and deploying mac address specific phones or User Profiles that you did not have before? You will need to keep track of who will use each phone and the features that will be provisioned and activated.

Configuration

Configure the new phones according to the instructions for the selected deployment scenario.

At a minimum, you will need to create a new per-phone or per-use file for the new phones. If you are changing the scenario, consult with a Deployment Specialist before proceeding.

Deployment

Load the new per phone or per user configuration files into the provisioning server just like you did in Chapter 7.

Set up an initial provisioning computer just as you did in Chapter 8 Follow the directions in Chapter 8 for loading the configuration into the new phones.

Test

Test the new phones and each feature you have activated before distributing them to the end users.

Decommissioning for RMA

Unless specifically directed otherwise by Spectralink Product Support, perform a factory reset to clear out all facility and personal information on the handsets you will be returning to the repair center. Any local settings will be lost.

If you have User Profiles configured, all settings reside on the server unless changed locally. Therefore any individual preferences that are part of the User Profile are preserved.

Receiving Phones from RMA

When phones are received back from RMA as replacement phones, they can be re-deployed just as if they are new, with a few provisos.

RMA does not change the mac address. Therefore if you are using Group Deployment and already have the <MACAddress>.cfg file on the provisioning server, it will direct the phone to the specific user/extension it had before being repaired. Ensure the <MACAddress>.cfg file already exists or build a new one.

If you are using Flat Deployment, ensure the [MACADDRESS]-ext.cfg file already exists or build a new one to use for the same or a different user.

Changing Phone Configuration

If you have a User Profile that you want to rename or a <MACAddress>.cfg file that you want to direct to a different user/extension, you will need to change the appropriate .cfg file.

You may need to add PTT channels or reorganize the groups or perhaps change from using the generic 000000000000.cfg system as used in Flat Deployment to using the <MACAddress>.cfg system as defined by Group Deployment. Edit your spreadsheet first to ensure you have the system design you want and use it to edit the various.cfg files accordingly.

Adding New or Advanced Features

This document covers basic telephony functions and several very popular features. If you need more information about any of the features or want to deploy additional features, please see the Spectralink Administrator's Guide and the various Feature Profiles that will give you the data you need to configure your system.

Part IV: Troubleshooting

This chapter contains general troubleshooting and diagnosis information to help you solve common issues you might encounter when loading the initial parameters, deploying or using the Spectralink 84-Series Wireless Telephones 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 *Spectralink 84-Series Wireless Telephone Administration Guide*.

This chapter covers the following:

- Determining which .cfg files are loaded
- Determine which software version is loaded
- Check for connection to WLAN (initial connection)
- Check for connection to SIP server
- Calling using the SIP server
- Calling using URL dialing when SIP server dialing fails
- Setting Up Syslog
- User Accessible Network Diagnostics
- Wi-Fi Diagnostics
- Run Site Survey
- Access Point Issues

Chapter 13: Basic Troubleshooting

Config Files

Navigate to **Settings>Status>Platform>Configuration**. The configuration screen displays the IP address of the server, the protocol being used, the .cfg files and detailed information about each of the .cfg files.

Provisioning Methods and Override Files

Three provisioning methods exist; the central provisioning server, the Web Configuration Utility, and the local phone user interface. Only the central provisioning server method can provision all settings. The Web Configuration Utility and the local phone interface do not offer every setting.

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

- 1 Single phone keypad interface
- 2 Web Configuration Utility
- 3 Central Provisioning Server

If the central provisioning server permits file uploads, override settings created using the Web Configuration Utility will be saved in a file called <MACaddress>-web.cfg.

When parameters are changed using the phone's keypad, they are saved in a <MACADDRESS>-phone.cfg file on the central provisioning server as well as in flash memory.



Caution: Persistence of Web settings

Web configuration changes will continue to override the provisioning server-derived configuration until they are:

- deleted through the **Reset Web Configuration** menu selection or
- configured using the <device/> parameters
- the <MACaddress> web.cfg override file on the provisioning server is deleted.

Local configuration changes—made through the phone's user interface—will continue to override the central provisioning server-derived configuration until they are:

- deleted through the **Reset Local Configuration** menu selection
- configured using the `<device/>` parameters
- the `<MACAddress>-.phone.cfg` override file on the central provisioning server is deleted.

Clearing overrides on a single phone

On the phone, go to **Settings> Advanced> Administration Settings> Reset to Defaults**. Select one of the following options.

- **Reset Local Configuration** Clears the override file generated by changes using the phone user interface
- **Resert Web Configuration** Clears the override file generated by changes using the Web Configuration Utility.
- **Reset Device Settings** Resets the phone's flash file system settings that are not stored in an override file.
- **Format File System** Formats the the phone's flash file system settings and deletes the UC Software application, log files, and override files. Note that if the override file is stored on the provisioning server, the phone will re-upload the override file when you provision the phone again. Formatting the phone's file system does not delete the device settings.
- **Reset to Factory** Formats the phone's flash file system and deletes the device settings.



Caution: Reset to Factory

Do not reset the phone to its factory defaults unless you want to wipe out all configuration settings and reload them, starting with the `wireless.cfg` file.

Software Version

Navigate to **Settings> Status> Platform> Application> Main**.

Wireless Connection

Wireless problems might exist when the phone is first configured via the microB USB cable.

Navigate to **Settings> Status> Diagnostics> Warnings**.

<i>Symptom</i>	<i>Problem</i>	<i>Corrective Action</i>
No bars Bars with red X	The phone has not associated with an AP.	<ul style="list-style-type: none"> • Verify setting in your wireless.cfg file. • If settings are changed,

Connection to SIP Server and Calling

<i>Symptom</i>	<i>Problem</i>	<i>Corrective Action</i>
The line icon shows an unregistered line icon. (red check mark)	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.
		<p>Test calling using the SIP server: Dial the extension of another phone and press the green dial call button. When the other phone answers the call you are now in call and can speak to the other party. End the call by pressing the red end call button. If/when this phone is called it will ring and display the name or number of the calling party. Press the green start call button to answer the call.</p>
		<p>Calling using URL dialing when SIP server dialing fails: The 84-Series handset can make or receive calls using the IP address of another Spectralink phone. To make a call the phone must be connected to the WLAN AP (with no red X over AP signal strength bars), press the green start call button, then press Dial Mode soft key, select URL, enter the IP address of the phone to call, 192.168.2.100 (use the * key for the dots to separate the IP fields), then press the start call key. This is a way to test the phone to ensure it is working with the WLAN when the SIP server or its connection is not established.</p>

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"> 1 Select Settings> Basic Settings> Preferences> Time & Date. The Time & Date screen displays. 2 Scroll to Disable, and then press the Ok key. 3 Press the Home key. <p>The Home Screen no longer displays the time and date.</p>

Upgrading

Symptom	Problem	Corrective Action
The handset does not upgrade from the central 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 Spectralink 84-Series 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.
	The handset has been upgraded through the Web Configuration Utility See the <i>Administration Guide</i> for additional information.	<ul style="list-style-type: none"> • Navigate to Settings> Advanced Settings> Administrative Settings> Network Configuration> Provisioning Server> Upgrade Server. The address will be shown in this field. • In the override file for a particular handset, clear the value set by the WebUI, or edit the override file parameter to "" which will also delete the setting in the handset. • Do not use the WCU to upgrade the handsets.

Setting Up Syslog

For more information on setting up syslog, see the Technical Bulletin *Using Syslog for Logging of Complete SIP Messaging*.

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**.

Parameter values

The following rules apply when you set a parameter with a numeric value outside of its valid range:

- If the configuration file's value is greater than the allowable range, the maximum value is used
- If the configuration file's value is less than the allowable range, the minimum value is used.
- If a parameter's value is invalid, the value is ignored. Invalid parameters values can occur when enumerated type parameters do not match a pre-defined value, when numeric parameters are set to a non-numeric values, when string parameters are either too long or short, or when using null strings in numeric fields.
- All such situations are logged in the phone's log files.

A sample entry is: 000026.145|cfg |4|00|Prm|syslog.cfg: Unknown parameter "log.level.change.lp" found, ignoring.



Settings: Types of parameter values

The configuration parameters available in the Spectralink Software use a variety of values, including Boolean, integer, enumerated types, and arrays (a table of values). Each parameter included in the 84-Series template files is listed in this document along with its description, the default value, and the permissible values. If the value that has been configured does not match the allowable range of values it will be ignored and the error is logged in the phone's mac-app.log file. E.g. |cfg |4|00|Prm|syslog.cfg: Unknown parameter "log.level.change.lp" found, ignoring.

Chapter 14: Wi-Fi Diagnostics

The Wi-Fi diagnostics feature enables you to gauge the overall health of the Spectralink 84-Series handsets in relation to the rest of the system, particularly the Access Points (APs). These Diagnostics screens can be accessed from standby mode but the diagnostics data will be stale, showing the last update. There is an advantage to having the phone in call when using diagnostics mode. The data will be updated in real time to show the current data for all screens. Enter diagnostics mode when in call by calling another phone or answering a call normally, then press the return key (above the end call key) to access the carousel then the following:

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

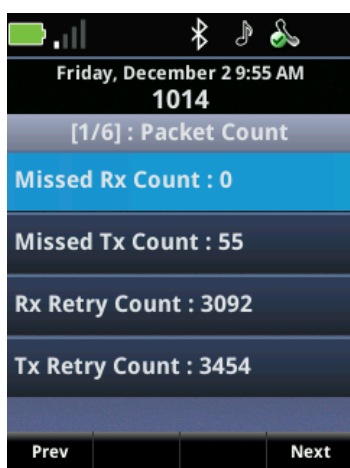


You can scroll forward or backward through these screens using the **Prev** and **Next** soft keys.

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

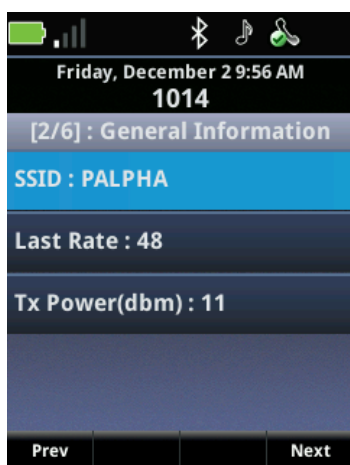
Screen 1 (Packet Count)

- 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 6 bytes of the AP's MAC address ch—Channel number

ss—Signal Strength

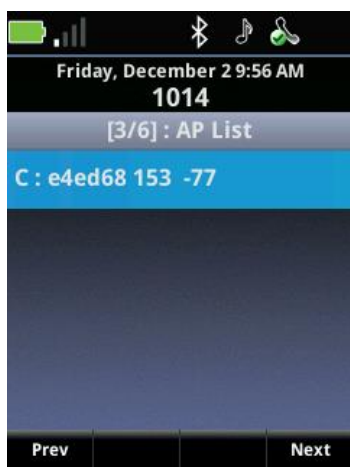
- Other lines: Other local APs

The format of each line is as follows: mmmmch-ssmnem where:

mmmm—Last 6 bytes of the AP's MAC address ch—Channel number

ss—Signal Strength

mnem—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* below.)



The above screen shot shows the phone connected to the AP Radio MAC ending in e4ed68 using channel 153 with RSSI of -77dBm

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 the currently used AP
- Rate**: One or more required rates are not supported by the AP
- 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

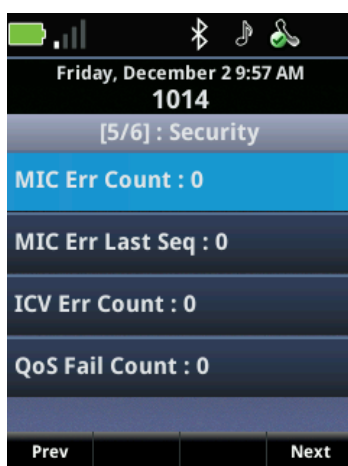
Screen 4 (Association Count/Failure)

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



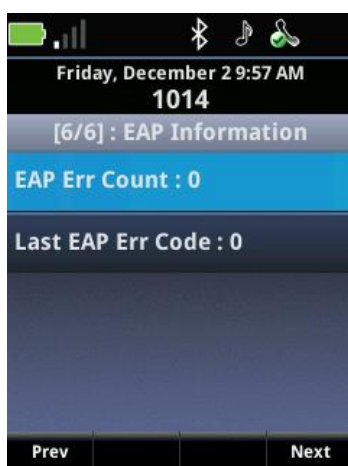
Screen 5 (Security)

- 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
- Line 3: 802.11n: disabled (if shown) or 802.11n: enabled (if not shown)



Chapter 15: Run Site Survey

The Run Site Survey feature is used to evaluate the facility RF coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by displaying RF signal strength, to gain information about an AP, and to scan an area for all APs regardless of the Service Set Identifier (SSID). When Site Survey is run, the 84-Series handset is offline and not able to receive or initiate a call. 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

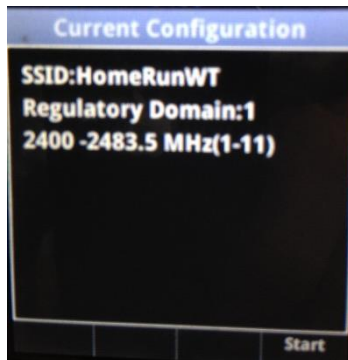
From the Home Screen, select **Settings**, and then select **Advanced Settings** (456)> **Administration Settings**> **Diagnostics**> **Run Site Survey**.

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.

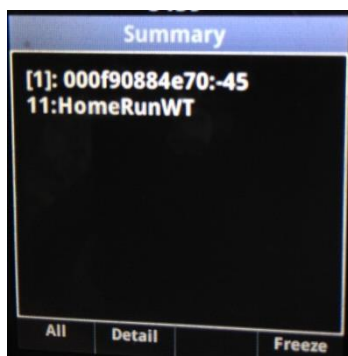


On this screen:

- 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.

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

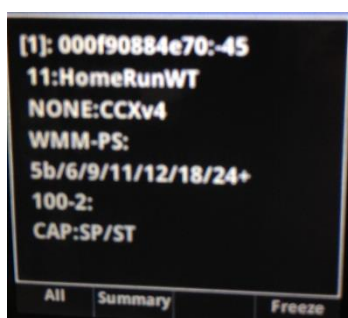


There are two modes of display: Summary and Detail. These modes can be selected pressing the mode desired using either the **Summary** or **Detail** soft key.

The Summary screen shows.

- Line 1 AP Radio MAC and RSSI
- Line 2 channel and SSID (as configured in 84-Series .cfg files)
- Up to four APs are displayed.

Press the Detail softkey:

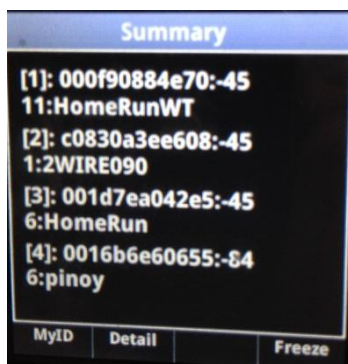


The 84-Series configured SSID Detail screen shows. Use the arrow keys to step through the APs.

- Line 1: Radio MAC and RSSI
- Line 2: channel and SSID
- Line 3: SSID security info
- Line 4: WMM info

- Line 5: data rates (5.5Mbps is Basic while others are supported)
- Line 6: Beacon rate (102.4ms), with DTIM = 2
- Line 7: Capability info: SM=spectrum management enabled, SP=short preamble, ST=short timeslot, PR=privacy bit enabled, CA=channel agility

Press the All softkey:



The All SSID summary screen shows:

- Line 1: AP radio MAC and RSSI
- Line 2: channel and SSID
- Line 3: 2nd AP Radio and RSSI
- Line 4: channel and SSID
- Line 5: 3rd AP radio MAC and RSSI
- Line 6: channel and SSID
- Line 7: 4th AP radio MAC and RSSI
- Line 8: channel and SSID



DTIM

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.

Update Interval

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.

Chapter 16: Access Point Issues

Most, but not all, handset audio issues are associated with AP range, RF signal strength, positioning, and capacity. Performing a site survey as described in Run Site Survey on page 4-57 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. If the call is dropped there is no recovery and the call is lost. If audio stops or gets choppy when the user moves out of range, this can be remedied by moving back in range.

Capacity

In areas of heavy use, the call capacity of a particular AP may be full. If this happens, audio gets poor and the user may 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

A highly reflective environment (metallic) will cause a multi-path environment. The RF transmissions will reflect or bounce off metallic objects which cause packet corruption, high retry rates, Missed and/or Dropped packets. Diversity in the AP using two or more antennas (often separated by a few feet if possible) will go far to alleviate multi-path environments. It can also help to lower the AP (out of the ceiling rafters, AC ducting, electrical wiring) so there is a more direct line of site between the AP and 84-Series handset.

Part V: Appendices

Appendix A: Setting up an FTP Server

Read this section if you have never set up a provisioning server before.

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. This application (version 0.9.xx) has been tested with the Spectralink Software.



Tip: Choosing a Provisioning Protocol

By default, Spectralink sets FTP as the provisioning protocol on all Spectralink phones. This guide focuses on the FTP provisioning protocol. Other supported protocols include TFTP, HTTP, and HTTPS.

To set up an FTP server using FileZilla Server:

- 1 Download and install the latest version of [FileZilla Server](#).
- 2 After installation, a *Connect to Server* pop-up displays on your computer. 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, *administrator*.
- 6 Select the **Password** checkbox and enter a password.
For example, *admin123*. The phone will use this password to log in.



Admin Tip: Provisioning computer requirement

“administrator” must be used as the username and *“admin123”* as the password when setting up the initial provisioning computer. The central provisioning server may use a different user name and password.

- 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** Determine the IP address of the FTP server by entering *cmd* in the Run dialog on your Start menu, and *ipconfig* in the command prompt.

The IP Address of the FTP server is shown.

Appendix B: Upgrading Spectralink 84-Series Software

You can upgrade the software that is running on the Spectralink 84-Series handsets in your organization. The updater, Spectralink software executable, and configuration files can all be updated on the central provisioning server.

Upgrading Your Phones

Please read the Release Notes before performing the upgrade.



Admin Tip: Which software version to use?

You will need to be sure that you are running the 4.4.x or 4.6.x Lync software release if your handsets are Lync-compatible and you are using a Lync server for telephony functions, instant messaging, presence and/or calendaring. Handsets variants sold without Lync support shall will not run Lync software releases.

Starting with 4.4.0, even numbered releases support Lync, odd numbered releases do not.

Spectralink 84-Series handset models 8441 and 8453 are shipped from the factory with software release 4.3.0 (or later) for basic SIP and 4.4.0 (or later even numbered releases) for SIP with Lync already installed. These models cannot run earlier code versions (as the older releases do not support these handsets' personal alarm capabilities).



Spectralink recommends: Upgrade your software

Wherever possible, Spectralink recommends upgrading to upgrade to the latest available software that supports your handset type.

Software release 4.2.1 and earlier contained multiple software images with filenames that were based on the hardware id of the 84-Series handsets. With release 4.3.x or 4.4.x and later, the release has been simplified to contain a single software image that supports all hardware models (the 8440, 8441, 8450, 8452, and 8453 models). The filename is slnk84xx.sip.ld for a SIP release or slnk84xx.lync.ld for the SIP with Lync release.

However the introduction of the single filename requires a transition step when updating 8440/8450/8452 handsets running software 4.2.1 or earlier, because the previous older software does not know about this new filename.

Handsets running 4.2.1 or earlier will look for a filename using the following algorithm:

First they will look for a file based on the model's hardware ID. For example, an 8440 phone will look for a file named 3111-36150-001 pre-pended to the value of APP_FILE_PATH (typically set as "sip.ld").

If that file can't be found, then it looks for APP_FILE_PATH as a standalone file (sip.ld or lync.ld).

If the APP_FILE_PATH parameter is not available, it will use whatever software is already loaded in the phone.

Therefore we must direct the phone to the new unified filename at the start and it will thereafter know how to find it.

To upgrade phones running 4.2.1 (or earlier) to Spectralink 84-Series software 4.3.x/4.4.x or later:

- 1 Back up your existing application and configuration files.
- 2 Download the latest software version that corresponds to your handset model. (Lync or SIP) from the support.spectralink.com website.
- 3 Log into the central provisioning server
- 4 Unzip the software. Ensure you do not overwrite any files that you need to keep.
- 5 Copy your .cfg files back to the root directory.
- 6 There are two methods to have the existing phones load 4.3.0/4.4.x or later firmware:
 - a Rename the new release firmware image (i.e. slnk84xx.sip.ld or slnk84xx.lync.ld) to the hardware model of the phones installed at your site. The following list indicates how to rename the files based on your phone model. If your site contains several 84-Series handset models, simply copy the slnk84xx.sip.ld or slnk84xx.lync.ld file as many times as needed and rename each copy to match the required file name:
 - » 8440 - rename to 3111-36150-001.sip.ld
 - » 8450 - rename to 3111-36152-001.sip.ld
 - » 8452 - rename to 3111-36154-001.sip.ld
 - b Or change the value of the APP_FILE_PATH parameter in the config files to slnk84xx.sip.ld or slnk84xx.lync.ld.
- 7 Reboot the 84-Series handset or update configuration using the keypad.
 - a Configuration file changes and enhancements are explained in the Release Notes that accompany the software.



Admin Tip

The phones can be configured to periodically poll the provisioning server for changed configuration files or application executables. If a change is detected, the

phone may reboot to download the change. Contact a Deployment Specialist for assistance in setting up this option.

To upgrade phones to Spectralink 84-Series software 4.2.0

- 1** Back up your existing application and configuration files.
- 2** Log into the central provisioning server and download the 4.2.0 software from the website.
- 3** Unzip the software. Ensure you do not overwrite any files that you need to keep.
- 4** Copy your .cfg files back to the root directory.
- 5** Check your top level files and ensure the APP_FILE_PATH="sip.ld" parameter is in the 000000000000.cfg or <MACaddress>.cfg file.
- 6** Reboot the 84-Series handset or update configuration using the keypad.
Configuration file changes and enhancements are explained in the Release Notes that accompany the software.

Appendix C: 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**.



Spectralink recommends: Change default password

Spectralink recommends that you change the administrative password from the default value.



Settings: Limitations of the Web Configuration Utility

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.



Caution: Overrides

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

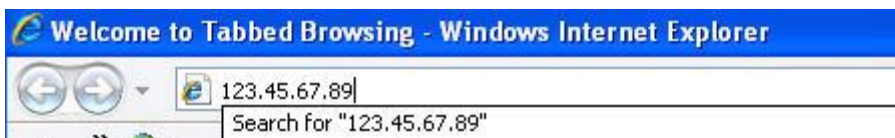
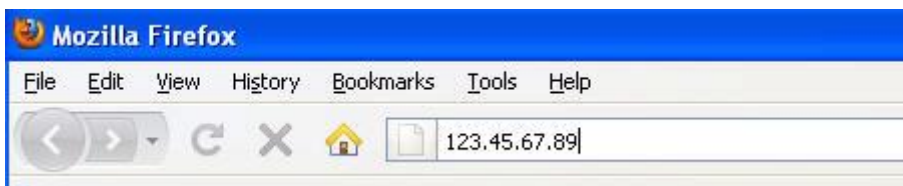
If the provisioning server permits file uploads, override settings created using the Web Configuration Utility will be saved in a file called <MACaddress>-web.cfg.

Configuration Using 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 Open one of the supported Web browsers.

For a list of supported Web browsers, see the latest *Spectralink Web Configuration Utility User Guide*.

- 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 **Admin**.
By default, the administrative password is **456**.

A Web page similar to the one shown below displays.

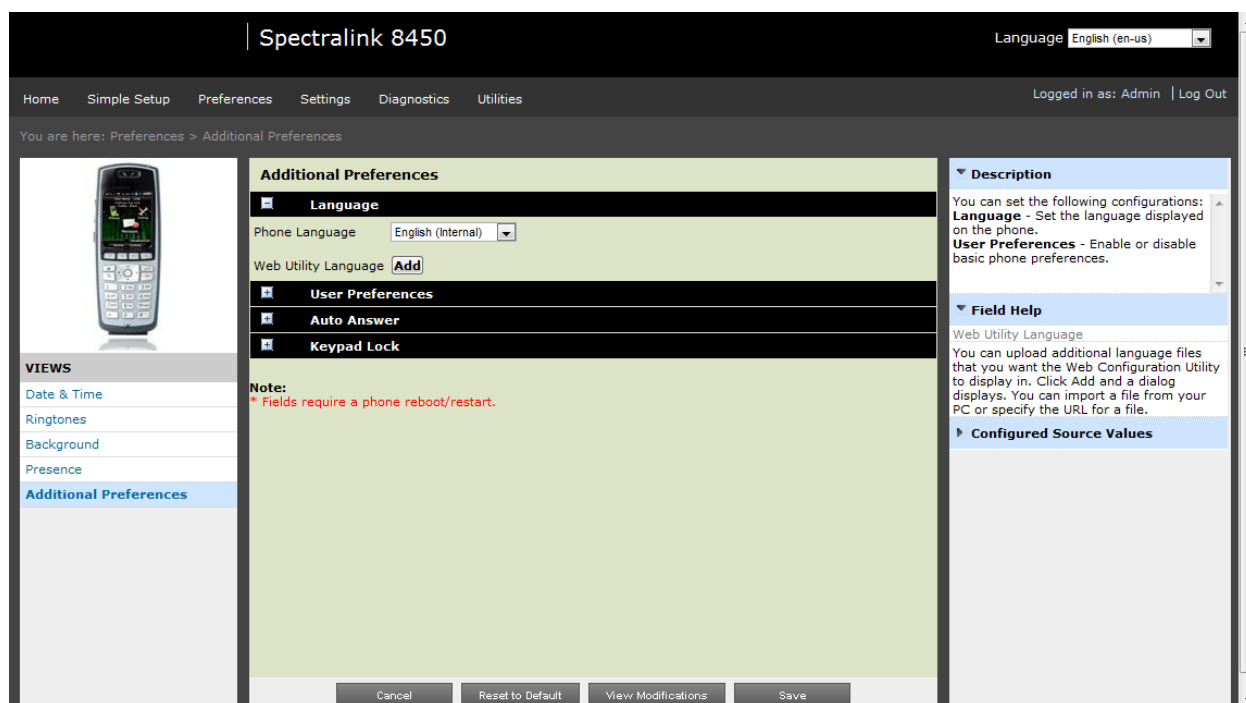


5 Make the desired configuration changes to the handset's configuration.

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 84-Series handset configuration files using the Web Configuration Utility.

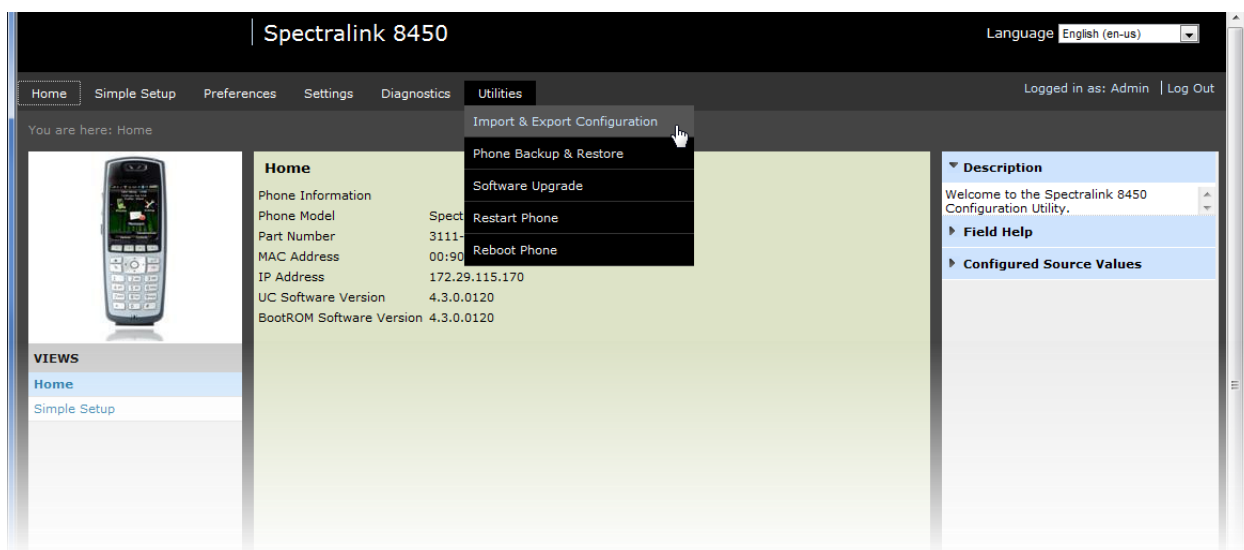


Caution: Security

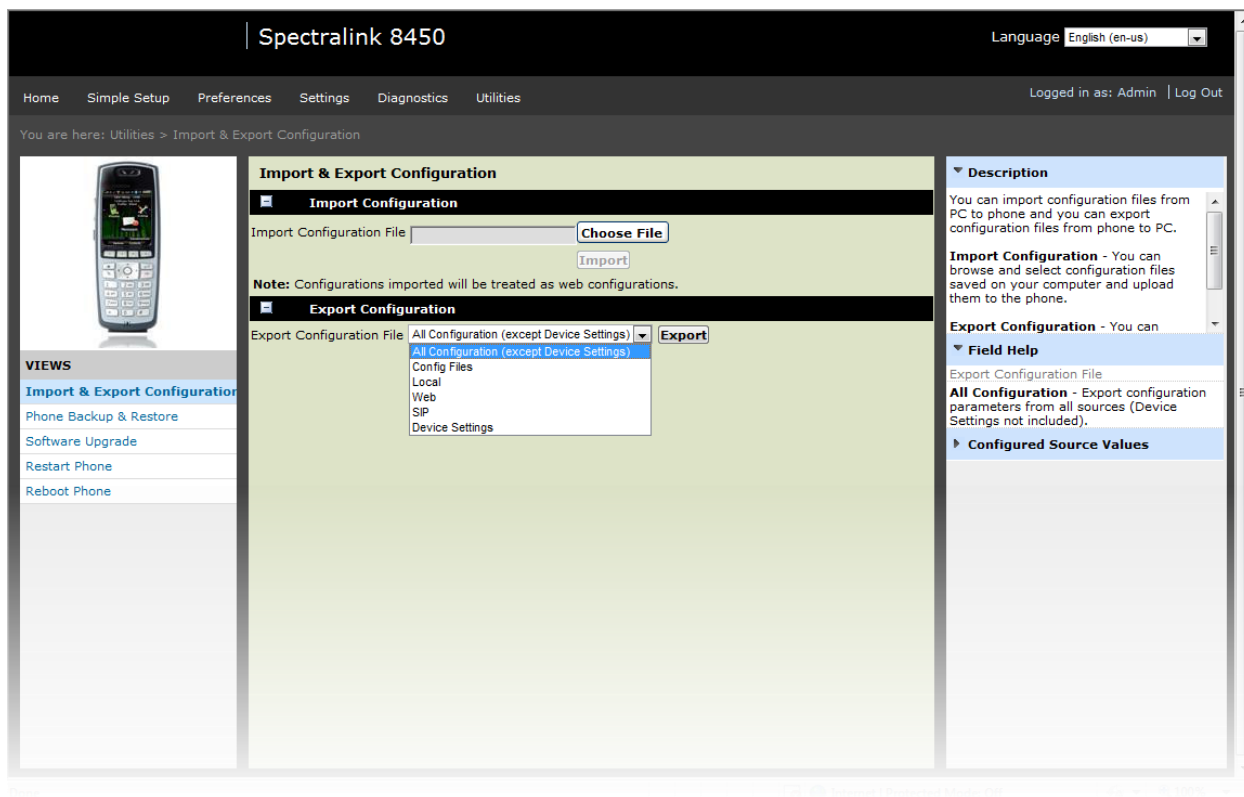
Passwords and security keys from the device settings are not exported. These parameters are listed at the top of the exported file, so they can be found quickly for editing.

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 Open 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.



- 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.

Save the file in the desired location.

Appendix D: Software Copyrights and Open Source Information

Software Copyright

Portions of the software contained in this product are:

Copyright © 1998, 1999, 2000 Thai Open Source Software Center Ltd. and Clark Cooper

Copyright © 1998 by the Massachusetts Institute of Technology

Copyright © 1998-2008 The OpenSSL Project

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved

Copyright © 1995-2002 Jean-Loup Gailly and Mark Adler

Copyright © 1996-2008, Daniel Stenberg, <daniel@haxx.se>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

OFFER for Source for GPL and LGPL Software

You may have received a Spectralink 84-Series handset from Spectralink that contains—in part—some free software (software licensed in a way that allows you the freedom to run, copy, distribute, change, and improve the software).

A complete list of all open source software included in the Spectralink 84-Series handset, as well as related license and copyright information, is available at <http://support.spectralink.com>.

You may also obtain the same information by contacting Spectralink by regular mail or email at the addresses listed at the bottom of this notice.

For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the contact information provided below, for a charge of no more than our cost of physically distributing, the items listed in “Spectralink OFFER of Source for GPL and LGPL Software” , which is available at <http://support.spectralink.com>.

Contact Information for Requesting Source Code

Spectralink Open Source Manager

2560 55th Street

Boulder, CO 80301

OpenSource@Spectralink.com

Appendix E: Spectralink Certificates

Spectralink CA certificates can be obtained from:

<http://pki.spectralink.com/aia/Spectralink%20Issuing%20CA.crt>

<http://pki.spectralink.com/aia/Spectralink%20Root%20CA.crt>

END OF DOCUMENT