Avaya 3641/3645/6120/6140 IP Wireless Handset with Session Initiation Protocol (SIP) Administration Guide

21-603998
Issue 2

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http:/www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone

computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types
Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server. CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud
“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks
The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter One: Introduction 7
- Purpose of this book 7
- Resources 7
  - Documentation 7
  - Software 8
  - Customer support 8
- Send us your comments 8

Chapter Two: Avaya 3641/3645/6120/6140 IP Wireless Handset Overview 9
- Changing the software from H.323/CCMS or UNIStim to SIP 9
- WLAN Quality of Service 10
- WLAN security 11
- Minimum system requirements 12
- System diagram 13
- System components 14
- Avaya 3641/3645/6120/6140 IP Wireless Handset specifications 17
  - Table of specifications 18

Chapter Three: SIP integration factors 21
- Sample DHCP server configuration file 22

Chapter Four: System Configuration 25
- Configuration flow chart 26
- Configuring Avaya Aura® Session Manager and Avaya Aura® Communication Manager 27
- Configuring the access points 27
- Configuring SIP handset files 27
  - Remote configuration files 28
  - The 46xxsettings.txt file 29
  - The handset-specific files 30
- Loading SIP configuration files onto HTTP/TFTP server 32

Chapter Five: Downloading and installing the handset software 33
- Minimum Configuration Process 33

Chapter Six: Configuring each Avaya 3641/3645/6120/6140 IP Wireless Handset 37
- Handset Administration Tool 37
- Remote configuration 37
- The Admin (Administration) menu 37
- Admin Menu Table 39
- Phone configuration 43
- Network Config 48
- Diagnostics 54
- Restore defaults 54
- Demos 55
- WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning 56
- Admin menu default table 60

Chapter Seven: Testing a handset 63

Chapter Eight: Certifying the handsets 65
Conducting a Site Survey 65

Chapter Nine: Using the Avaya 3641/3645/6120/6140 IP Wireless Handset 69
Startup sequence 69
Handset modes 70
The handset display 71
Softkeys 73
Menus 75
Notes on battery packs 76
User-defined preferences 78
Config Menu 78

Chapter Ten: Diagnostic tools 83
Run Site Survey 83
Diagnostics enabled 86
Syslog mode 91
SNMP 93

Chapter Eleven: Software maintenance 95
Upgrading handsets 95
Normal download messages 95
Remotely rebooting handsets 96
Download failure or recovery messages 96

Chapter Twelve: Troubleshooting 97
Access point problems 97
Handset status messages 98

Appendix A: Regulatory domains 109

Appendix B: Remote configuration parameters definition 111

Chapter One: Introduction

This document explains how to configure and maintain Avaya 3641/3645/6120/6140 IP Wireless Handsets using Session Initiation Protocol (SIP) release 1.1.

Purpose of this book

This book describes the procedures used to configure and administer Avaya 3641/3645/6120/6140 IP Wireless Handsets using Session Initiation Protocol (SIP) on Avaya Aura® Session Manager with Avaya Aura® Communications Manager.

Resources

Documentation

The following documents provide additional information.

- Avaya 3641/3645 IP Wireless Handset with Session Initiation Protocol (SIP) User Guide, (21-603938)
- Avaya SVP Server[1] Admin Guide (21-603969)
- Handset Administration Tool (HAT) Admin Guide (21-603968)

These documents are available at http:/support.avaya.com. Select **DOWNLADS & DOCUMENTS.** You will be asked for the product name, enter **IP Wireless Phones** and then select **Documents**.

Other pertinent documentation available from Polycom includes the following:

- *VIEW Certified Products Guide* (1725-36040-001) that is available at http://www.polycom.com/support/voice/wi-fi/view_certified.html
- *VIEW Configuration Guide* 1725-36xxx-001 where xxx indicates a number corresponding to the type of access point(AP) that is available at http://www.polycom.com/support/voice/wi-fi/view_certified.html
- *Deploying Enterprise-Grade Wi-Fi Telephony*
  *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones that is a*vailable at

[1] The Avaya SVP Server is also known as the AVPP or the Avaya Voice Priority Processor.

http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/spectralink_8020_wireless.html

- *Open Application Interface (OAI) Specification* (1725-36196-001) that is available at http://www.polycom.com/forms/spectralink_oai_sw_dl.html

Software

Before configuring the phones, ensure that you have the following software:

- The Avaya Handset Administration Tool software version 3.0.9.x or version 4.0.2.x
- SIP software version 133.009 or later

You may download the software from http:/support.avaya.com. Select **DOWNLADS & DOCUMENTS.** You will be asked for the product name, enter **IP Wireless Phones** and then select **Downloads**. Choose the software version from the list of available downloads.

Customer support

Avaya provides a telephone number to report problems or to ask questions about your product. For a full list of support telephone numbers, refer to http://www.avaya.com/support.

Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to the Avaya documentation team. infodev@avaya.com

Chapter Two: Avaya 3641/3645/6120/6140 IP Wireless Handset Overview

The Avaya 3641/3645/6120/6140 IP Wireless Handsets are Wi-Fi handsets for workplace telephone systems. The handsets operate over a VIEW-certified 802.11a/b/g/n wireless LAN (WLAN) providing users a wireless extension of the SIP call server. By seamlessly integrating into a SIP environment, the system provides high-quality mobile voice communication to the wireless telephone users throughout the workplace. The system gives users the freedom to roam throughout the workplace while providing many of the features and functionality of a wired SIP desk phone.

Note:
The Avaya 3641/3645/6120/6140 IP Wireless Handsets do not provide 802.11n support in their Admin menu structure. However, Polycom VIEW certifies the APs running in ‘n’ mode. When the APs use ‘n’ mode, the handset registers as a ‘b’ client and negotiates a lower rate for its own traffic. This has the effect of slowing down the overall network speed, but this is no different than any legacy ‘b’ client co-existing on an ‘n’ network. Consult the VIEW Certified AP Guide for more information.

In a SIP environment, each handset may have up to six sets of credentials to identify itself as belonging to a particular user. The Avaya Aura® configuration establishes the maximum calls per line. .

Changing the software from H.323/CCMS or UNIStim to SIP

The Avaya 3641/3645 IP Wireless Handsets default software is the CCMS protocol software. The Avaya 6120/6140 IP Wireless Handset default software is the UNIStim protocol software. You will need to change the license to the SIP software in the Admin menu. See the minimum configuration instructions in Chapter 5 for exact instructions.

Note:
Only Avaya 6120/6140 IP Wireless Handsets manufactured after August 2010 are capable of loading SIP software. The manufacturing date can be seen on the label in the battery compartment.

The default admin password for each protocol is as follows:

Avaya SIP	27238 (CRAFT)
CCMS	123456

UNIStim	123456

Note:
The latest wireless telephone and Handset Administration Tool software versions are required to support the features described in this document. See Chapter 3: *Software License and Protocol Management*.

WLAN Quality of Service

You may obtain the WLAN Quality of Service (QoS) using one of three available mechanisms: SpectraLink Voice Priority (SVP), Wi-Fi Standard QoS, or Cisco Compatible Extensions (CCX) version 4. However, you cannot mix these QoS modes within the same WLAN. Therefore, all Wireless Telephones on the network must have the same QoS setting.

SVP

SpectraLink Voice Priority (SVP) is a proprietary method of WLAN QoS, developed by Polycom, to ensure enterprise-grade voice quality, battery life and call capacity for Wireless Telephones. SVP requires the use of the SVP Server, which is an Ethernet LAN device that works in conjunction with Wi-Fi APs to ensure QoS over the WLAN. Voice packets to and from the Wireless Telephones are tunneled through the SVP Server to ensure voice prioritization as they are routed between the handset and SIP call server. See the *Avaya SVP Server Administration Guide* for detailed information about this device.

Wi-Fi Standard QoS

Avaya 3641/3645/6120/6140 IP Wireless Handsets support WMM, WMM Power Save and WMM Admission Control - all QoS standards from the Wi-Fi Alliance based on IEEE 802.11e. The combination of these three standards provides enterprise-class QoS in terms of voice quality, battery life and call capacity. The WLAN must also support and enable each of these QoS mechanisms in order to ensure they are utilized. This option does not require the SVP Server.

CCXv4

The CCX program requires WLAN client devices operating on Cisco APs to use a defined set of industry standards and Cisco-specific features. The Avaya 3641/3645/6120/6140 IP Wireless Handset has been certified by Cisco as CCXv4 compliant. When you select the CCXv4 operating mode on the handset, it automatically initiates the required set of Cisco-specific and industry standard QoS mechanisms. This option does not require the SVP Server.

WLAN security

The handsets support the following security methods:

WPA2 Enterprise

The handsets support WPA2 Enterprise, as defined by the Wi-Fi Alliance. The 802.11i standard based WPA2 provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. The Enterprise version of WPA2 uses 802.1X authentication, which is a port-based network access control mechanism using dynamic encryption keys to protect data privacy. The handsets support two 802.1X authentication methods: EAP-FAST and PEAPv0/MSCHAPv2. Both of these methods require a RADIUS authentication server on the network and accessible to the phone. See the *System Components* section for tested models. For additional details, see Chapter Three: *SIP Integration Factors*.

Normal 802.1X authentication requires the client to renegotiate its key with the authentication server on every AP handoff. This renegotiation is a time-consuming process that negatively affects time-sensitive applications such as voice. Fast AP handoff methods allow for the part of the key derived from the server to be cached in the wireless network, thereby shortening the time to renegotiate a secure handoff. The Wireless Telephone supports two fast AP handoff techniques, Cisco Client Key Management (CCKM) (only available on Cisco APs) or Opportunistic Key Caching (OKC). You must configure one of these methods for support on the WLAN to ensure proper performance of the handset.

WPA and WPA2 Personal

The handset supports WPA and WPA2 Personal, as defined by the Wi-Fi Alliance. Based on the 802.11i standard, WPA2 provides government-grade security by implementing the Advanced Encryption Standard (AES) encryption algorithm. WPA is based on a draft version of the 802.11i standard before it was ratified.WPA uses Temporal Key Integrity Protocol (TKIP) encryption. The Personal version uses WPA2. Pre-Shared Key (PSK) allows the use of manually entered keys or passwords to initiate WPA security.

Cisco Fast Secure Roaming

Cisco’s Fast Secure Roaming (FSR) mechanism uses a combination of standards-based and proprietary security components including Cisco Client Key Management (CCKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR provides strong security measures for authentication, privacy and data integrity along with fast AP handoff on Cisco APs.

WEP

The handset supports Wired Equivalent Privacy (WEP) with both 40-bit and 128-bit encryption.

Minimum system requirements

- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g/n wireless APs. Consult the Polycom *VIEW Configuration Guide* for the appropriate make/model of WLAN. Configuration guides for the Polycom SpectraLink® 8020/8030 Wireless Telephones are considered by Avaya as useable with the Avaya 3641/3645/6120/6140 IP Wireless Handsets.
- To load software and configuration files to the handset over the air, an HTTP or TFTP Server must be available on the network. You must install the current handset software in the proper HTTP or TFTP download directory. If the handset cannot connect to the server, the handset boots with the last known configuration.
- If you use SVP for QoS, you must install and properly configure the SVP Server.
- If you use SVP and/or the Avaya Wireless Application Interface Gateway, ensure that you have the following software versions:

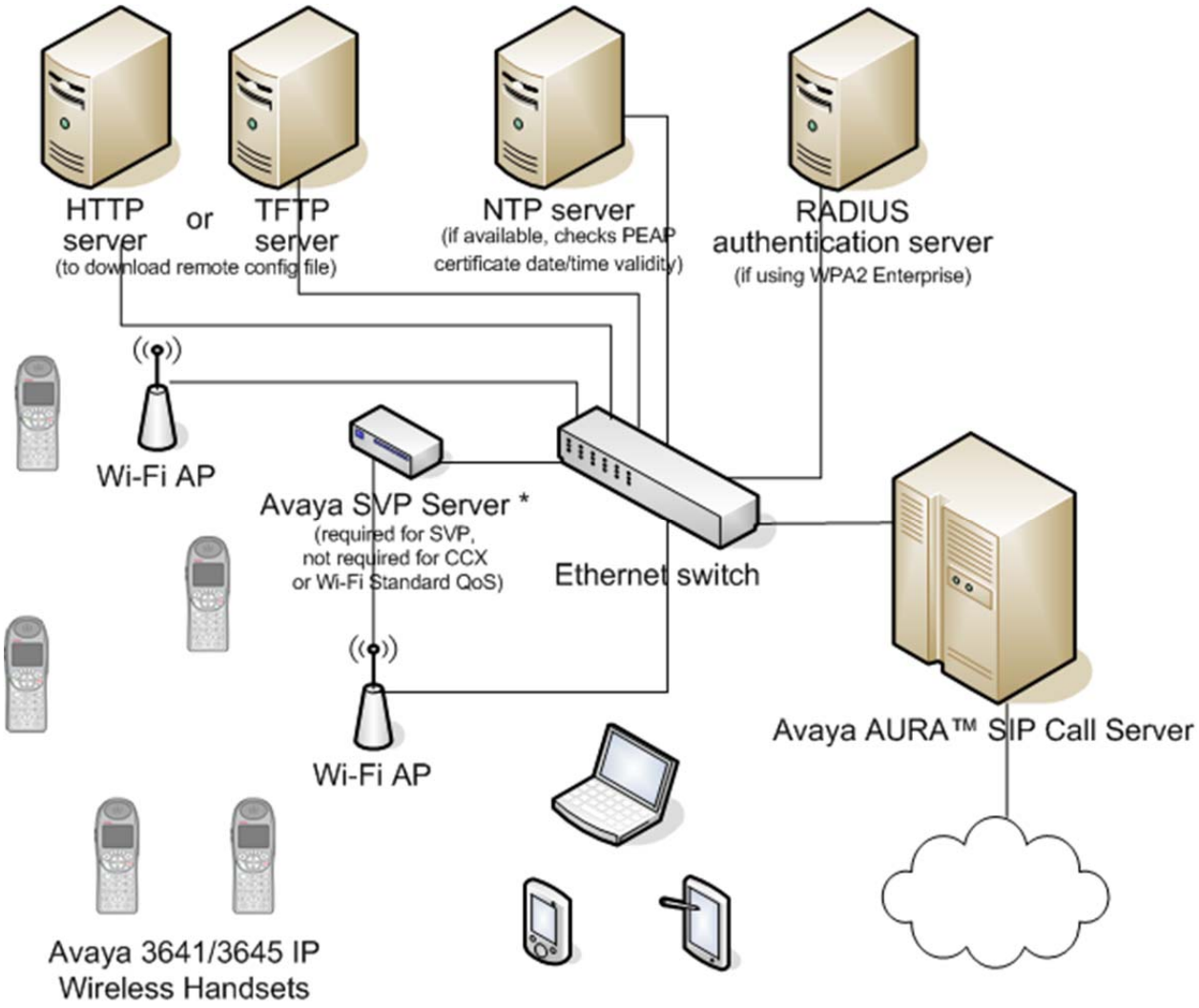
Component	Version
Avaya SVP Server	17x.040 or higher
Avaya Wireless Application Interface Gateway[2]	82.020 or higher

- If you use Wi-Fi Standard QoS, you must configure each AP for such features as WMM-Power Save; WMM-Admission Control; proper EDCA parameters; DSCP mapping for voice and control traffic; call admission control and Proxy ARP. Consult the appropriate *VIEW Configuration Guide* for these settings.
- If you use WPA2-Enterprise, the handsets use the network only when you install and properly configure all portions of the Public Key Infrastructure (PKI).

[2] The Avaya Wireless Application Interface Gateway is also referred to in this document as the “OAI Gateway”, “Open Applications Interface Gateway” or simply “OAI”. The model number on the label is “MOG700.” The Installation document for the Open Applications Interface (OAI) Gateway is available at https://support.avaya.com/css/P8/documents/003745895.

System diagram

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



System components

Avaya 3641/3645/6120/6140 IP Wireless Handset

The Avaya 3641/6120 IP Wireless Handset is a lightweight, durable handset specifically designed for mobile workplace use. The Avaya 3645/6140 IP Wireless Handset has the same features and function, but in a more durable design with and includes push-to-talk and emergency call capability.

Like a wired deskphone, the handset can receive direct calls and transferred calls, transfer calls to other extensions and make outside and long distance calls. The users can use the wireless telephones only within the premises and within the WLAN coverage area.

SVP Server (required when using SVP QoS)

SVP Server is a wired LAN device that is required when using SpectraLink Voice Priority for QoS. This device may be referred to as the Avaya SVP Server, the Avaya Voice Priority Processor or the Nortel WLAN IP Telephony Manager 2245. See the *Avaya SVP Server Admin Guide* for complete information.

Access points

Enterprise-grade Wi-Fi access points provide the connection between the wired LAN and the wireless LAN. To ensure seamless radio coverage, you must position the VIEW certified 802.11a/b/g/n APs in all areas where IP Wireless Handsets will be used. 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 good voice quality. See the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

You must properly configure the APs to support the corresponding QoS and security methods selected for the handset.

Ethernet switch

One or more Ethernet switches interconnect multiple network devices, including the Avaya SVP Server (if used for QoS), the proxy server(s), wired IP phones, HTTP/TFTP Server, RADIUS authentication server (if using WPA2 Enterprise) and WLAN access points. Enterprise Ethernet switches provide the highest performance networks, which can handle combined voice and data traffic, and are required when using the Avaya 3641/3645/6120/6140 IP Wireless Handsets.

Although a single Ethernet switch network is recommended, the handsets and the Avaya SVP Server can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets, as long as the SVP Server and access points and handsets are on the same subnet. However, in such

networks, it is possible for the quality of service (QoS) features of the SVP Server to be compromised, and consequently voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure any quality issues are addressed. See *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones* for additional guidance.

Avaya 3641/3645/6120/6140 IP Wireless Handsets cannot roam with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a Layer-2 tunnel across subnets that enable the handsets to roam. Without this capability, the telephone drops any call in progress when the user moves out of range. The handset must be power cycled in order to resume functionality in the new subnet area.

Ensure that you have attached all your APs to the same subnet for proper operation. The handset can change subnets if you have enabled DHCP and switch on the handset within range of APs on a new subnet. Note that the wireless telephones cannot “roam” across subnets, since their IP addresses do not change while operational.

Avaya Aura® Session Manager and Avaya Aura® Communications Manager

The Avaya Aura® Session Manager and Avaya Aura® Communications Manager provides access to telephony services and connects to another device such as a PBX or gateway and from there, other wired phones and the PSTN.

HTTP server

An HTTP server is required to distribute software to the handsets. In a system with no HTTP server, you may use a TFTP server for this purpose.

TFTP (Trivial File Transfer Protocol) server

You may use a TFTP server to distribute software to the handsets if there is no HTTP server. It may be on a different subnet than the APs and the handsets.

NTP (Network Time Protocol) Server

If you use WPA2 Enterprise security, the handset confirms if the PEAP certificate has a valid date and time with the NTP server on the network, if the server is available. If an NTP Server is not available, the certificate will be assumed valid and operate accordingly. When you use an NTP server, the server provides date and time information to the handset.

Authentication Server (if using WPA2 Enterprise)

You must use a RADIUS authentication server to provide username/password based authentication using RSA certificates for PEAPv0/MSCHAPv2 or PAC files for EAP-FAST.

You can use the following authentication servers with R3.0:

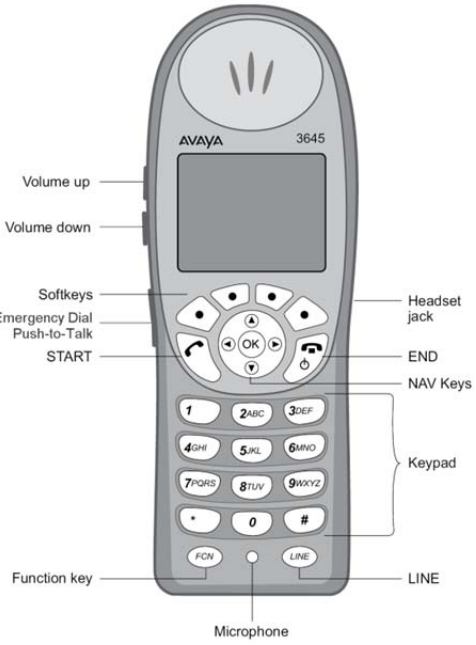
- Juniper Networks Steel-belted Radius Enterprise Edition (formerly Funk), v6.1

- Microsoft Internet Security and Acceleration (ISA) Server 2003
- Cisco Secure Access Control Server (ACS), v4.1
- FreeRADIUS v2.0.1 and 1.1.7

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

Avaya 3641/3645/6120/6140 IP Wireless Handset specifications

Avaya 3641 IP Wireless Handset



Avaya 3645 IP Wireless Handset

Table of specifications

Radio mode (selectable)	(802.11b, 802.11g)	2.4–2.4835 GHz
	(802.11a)	5.150–5.250 GHz 5.250–5.350 GHz 5.470–5.650 GHz 5.470–5.725 GHz 5.725–5.825 GHz 5.725–5.850 GHz
Transmission type	Direct-sequence spread spectrum (DSSS)	
Transmit data rate	up to 54 Mb/s	
WLAN QoS	SpectraLink Voice Priority (SVP) Wi-Fi Standard QoS (using WMM, WMM-Power Save and WMM-Admission Control) CCXv4	
WLAN security	WEP (Wired Equivalent Privacy) Cisco FSR (Fast Secure Roaming) WPA Personal WPA2 Personal WPA2 Enterprise: 802.1X Authentication EAP-FAST PEAPv0/MSCHAPv2: PEAP certificate sizes: 512, 1024, 2048 bit Encryption Ciphers: AES, RSA, RC4 Data Integrity: Hashed Message Authentication Code MD5 (HMAC-MD5) (RFC 2403, 2104) and Secure Hash Algorithm-1 SHA (HMAC-SHA-1) (RFC2404) Fast AP Handoff Opportunistic Key Caching (OKC) Cisco Client Key Management (CCKM)	
FCC certification	Part 15.247	
Other certifications	IP 53 certified for resistance to dust and liquid resistance MIL 810F Proc IV 516.5 for shock resistance Cisco Compatible Extensions (CCX) v4	
Voice encoding	ADPCM (Proprietary) G.711µ-law, G.711a-law and G.729	
Transmit power	Up to 100mW Transmit Power Control (formerly 802.11h), see Appendix A for details.	
Display	Up to five lines of text plus two icon status rows and one row for softkey labels.	
3641/6120 Dimensions	5.7" x 2.0" x 0.9" (14.5 x 5.1 x 2.3 cm)	
3645/6140 Dimensions	5.4" x 2.0" x 0.9" (13.7 x 5.1 x 2.3 cm)	

3641/6120 Weight*	3.9 oz. (110.6 g) with Standard battery pack
3645/6140 Weight*	4.2 oz. (119.1 g) with Standard battery pack
Standard Battery Pack capacity	4 hours talk, 80 hours standby
Extended Battery Pack capacity	6 hours talk, 120 hours standby
Ultra-Extended Battery Pack capacity	8 hours talk, 160 hours standby

Chapter Three: SIP integration factors

CODECs

The Avaya 3641/3645/6120/6140 IP Wireless Handsets are compatible with the G.711µ-law, G.711a-law and G.729 codecs. You can use any of these in a preferred order that is set in the 46xxsettings.txt file.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that dynamically assigns various configuration parameters to the clients. These configuration parameters include 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 handsets use the following DHCP options if DHCP use is enabled:

Option	Meaning
1	Subnet mask
3	Default gateway
6	DNS server
7	Syslog server logging
15	Domain name
42	NTP Server
66	TFTP server
151	Avaya SVP Server
152	Avaya Wireless Application Interface Gateway[3]
242	SSON†
siaddr	Boot server or next server

If values are not received via DHCP, the handsets use the statically defined values.

† If values for the non-SSON options are subsequently found in the SSON data or the config files, the handsets use these values instead of the DHCP supplied values. See the *SSON Option* section below for additional data.

[3] The Avaya Wireless Application Interface Gateway is referred to in the handset menus and elsewhere in this document as the “OAI (Open Application Interface) Gateway”. It is a gateway that manages third party vendor programming such as for nurse call systems or facility directories. The Installation document for the Open Applications Interface (OAI) Gateway is available at https://support.avaya.com/css/P8/documents/003745895.

DNS

Domain Name System (DNS), an industry-standard protocol, locates computers on an IP-based network. IP networks rely on number-based addresses to move information on the network. However, it is easier to remember user-friendly names than number-based addresses, so it is necessary to translate user-friendly names into addresses that the network can recognize. The handset can use DNS for HTTP server IP addresses, SNMP server IP addresses and the Avaya Aura® Session Manager IP address.

SSON Option

The SSON option follows these rules:

- SSON uses DHCP option 242 by default. If a different option setting is used, you must define the setting in the Admin menu. The allowed range is 128 through 254.
- The SSON option number is configurable in the Admin menu.
- The SSON option number is configurable in the HAT tool.
- Multiple SSON values may be set in the DHCP option string. Each parameter shall use the syntax “<name>=<value>”. You must delimit the parameters by commas and no blank spaces outside the quoted strings are invalid.
- If a parameter is present in both DHCP SSON and the 46xxsettings file, the value defined in 46xxsettings file shall supersede the value previously found in DHCP SSON.
- Valid parameters for the DHCP SSON option string include any parameter in the 46xxsettings.txt remote configuration file with the exception of the SIP_FAVORITES parameter that is not valid in SSON.
- The DHCP SSON option string is limited in length to 255 characters. It cannot support all possible parameters at once.

Sample DHCP server configuration file

A sample DHCP server configuration file is illustrated in the following example. Please note that this is only a sample and will not work on your system as written here. In addition, this file is specific to the ISC DHCP server. You must locally program the configuration files according to your site requirements.

dhcpd.cfg

```
# /etc/dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Type "man dhcp-options" at prompt to get help for these options.
#

# Global parameters start at beginning of file.
```

```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
# This means the DHCP server will send DHCPNAK messages to misconfigured
# clients.
authoritative;

# Use local address if you want the DHCP server to listen for DHCP requests
# on a specified address, rather than requests send to all addresses.
local-address 192.168.0.1;

# define the default gateway / router option 3
option routers 192.168.0.1;

# define the DNS server(s) option 6
option domain-name-servers 192.168.0.1;

# define the SYSLOG server option 7
option log-servers 192.168.0.1;

# define the domain name option 15
option domain-name "Avaya.com";

# define the SVP server option code 151 as an IP address.
option svp-server code 151 = ip-address;

# define the OAI server option code 152 as an IP address.
option oai-server code 152 = ip-address;

# This should  be  the  length  in seconds that will be
# assigned to a lease if the client requesting the lease does not ask
# for a specific expiration time.  86400 seconds is 1 day.
default-lease-time 86400;

# This should be the maximum length in seconds that will  be  assigned
# to a lease.
max-lease-time 86400;

# minimum lease time of 10 minutes
min-lease-time 600;

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses in the range 192.168.0.100 to 192.168.0.149,
# and all other clients get addresses in the range 192.168.0.150 to
# 192.168.0.199.

class "AvayaPhones" {
  match if substring (option vendor-class-identifier, 0, 11) = "Avaya";
}

# subnet definition also sets netmask option 1
subnet 192.168.0.0 netmask 255.255.255.0 {

  # DHCP lease pool for Avaya phones
  pool {
    allow members of "AvayaPhones";
    range 192.168.0.100 192.168.0.149;
```

```
  # define the siaddr / next server field as the alternative TFTP server address
  next-server 192.168.0.1;

  # define the NTP server option 42
  option ntp-servers 192.168.0.1;

  # define the primary SSON server address option 242
  option tftp-server-name "192.168.0.1";

  # define the SVP server address option 151 if using SVP QoS
  option svp-server 192.168.0.5; # option 151

  # define the OAI server address option 152
  option oai-server 192.168.0.6; # option 152
}

# DHCP lease pool for other devices
pool {
  deny members of "AvayaPhones";
  range 192.168.0.150 192.168.0.199;
  next-server 192.168.0.1;
  option tftp-server-name "192.168.0.1";
```

Chapter Four: System Configuration

You may configure each handset for site-specific requirements by opening the **Admin** menu and selecting options or entering specific information. Any settings entered in the **Admin** menu must conform to system settings. The **Admin** menu settings affect the only handset that you are configuring.

The IP Wireless Handset user may select several usability options from the Standby menu, described below in the *User-defined Preferences* section. The Avaya Handset Administration Tool is a software utility that enables rapid configuration of handsets by utilizing the USB port on the Dual Charger. See *Avaya Handset Administration Tool (HAT)* for specific instructions. Please see your service representative or contact Avaya customer service for more information about this tool.

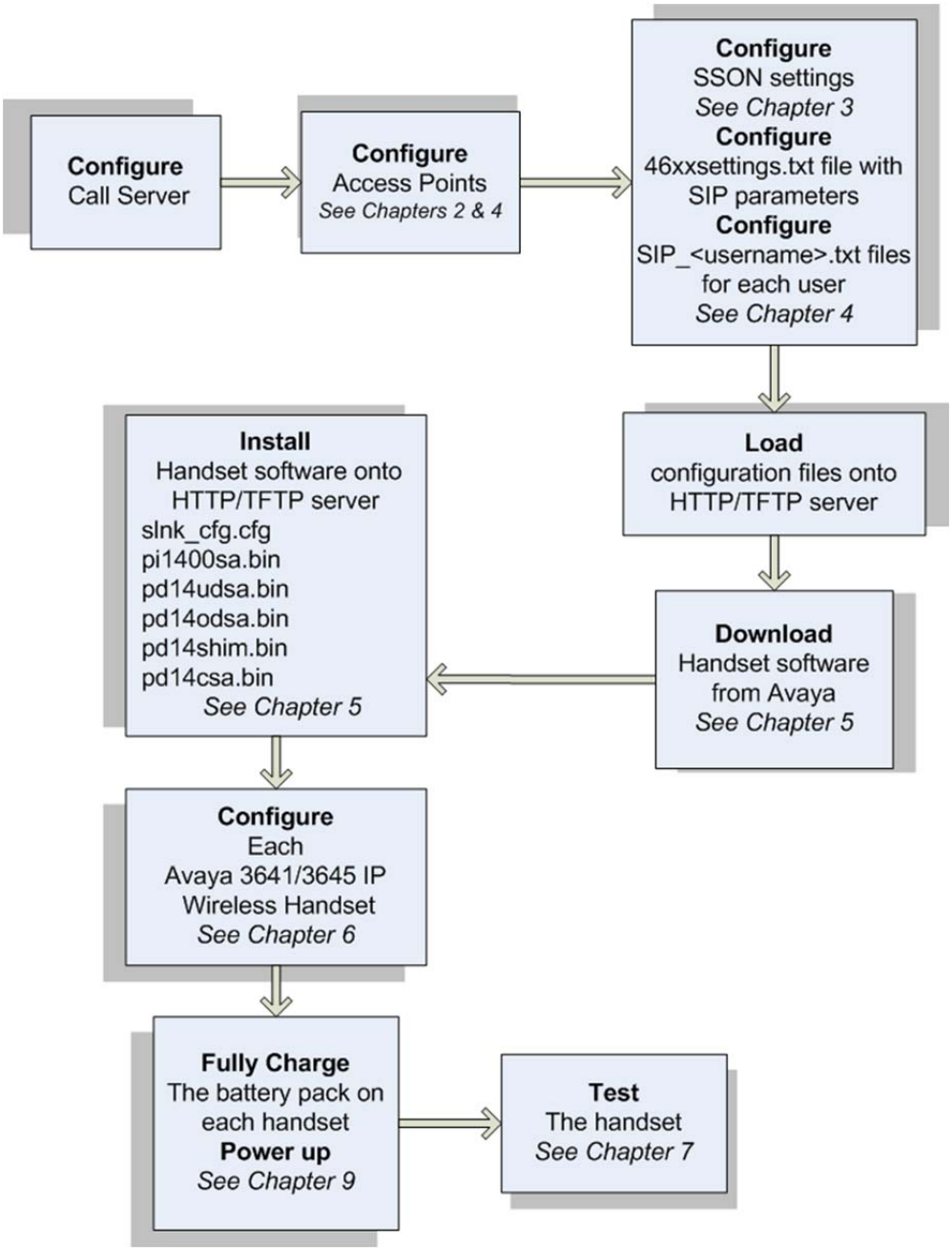
The Avaya 3641/3645/6120/6140 IP Wireless Handset is designed to be initially configured with minimum system requirements using the HAT tool. Thereafter, you can use the Remote Configuration File method to set the remaining parameters. See the *Remote Configuration Files* section below for more information.

When WPA2 Enterprise security is used, you can provision PAC files for EAP-FAST wirelessly or by using the HAT. For PEAP, certificates can be enrolled either using HAT or via the Remote Configuration File. For details, see *WPA2 Enterprise PEAP Certification Enrollment and EAP-FAST Manual PAC Provisioning*.

Other settings that must be configured include, but are not limited to, WLAN QoS, DSCP tagging, and DHCP. If you do not select these parameters, the handset uses the default settings. However, certain settings, for example: SID and related security settings and Regulatory Domain parameters, do not have default values and you must configure these parameters. . For more information, see *Remote Configuration Files*.

Configuration flow chart

(Each step is explained in the following pages)



Configuring Avaya Aura® Session Manager and Avaya Aura® Communication Manager

Refer to the Avaya Aura® documentation. Review the proxy information in this document for configuration requirements. You must configure an extension and related information for each handset you deploy.

The 3641/3645/6120/6140 IP Wireless Handset with SIP software provides basic SIP functionality with Avaya Aura®. Do not enable features on the Avaya Aura® Call server that has a similar functionality as local handset features, as doing so may lead to conflicts or inconsistent behavior.

Example: Do not configure “ACM Coverage Answer Group” or “Terminating Extension Group” because it might conflict with local Call Forward from the handset’s FCN menu.

Configuring the access points

See your access point documentation. You must enable WMM on the access point if the QoS method is WMM. Polycom VIEW certified access points are listed in the *Polycom VIEW Certified Products Guide.* Configuration Guides for each certified product can be found on the Polycom website. See the *Resources* section at the beginning of this document for link information.

Configuring SIP handset files

During normal handset setup in the SIP environment, the handsets download two files during startup. The handsets obtain these files from either the default HTTP directory (specified in the HTTPDIR parameter) or the root directory of the TFTP server. During the power-up sequence, every handset downloads the 46xxsettings.txt file. This file contains generic system information. The handset then downloads the second file, the SIP_<username>.txt file. This file is unique for each handset. The SIP_<username> file contains specific information for each handset such as username, password, and line appearances. Both of these files must be written specifically for the facility where the handsets will operate.

Note that if the handset cannot find one or both of these files, the handset will initialize using previously stored parameters.

A sample 46xxsettings.txt file is available on the Avaya website. You may use the sample file as a starting point and edit it according to your system requirements.

Remote configuration files

The two file types, generic and specific, are identical in format. Normally, system information is programmed in the 46xxsettings.txt file and only user-specific information is programmed in the SIP_<username>.txt file. However, system parameters can be in the user file if an override is necessary. Any information in the specific file that conflicts with the information in the generic file will take precedence over the information in the generic file. See Appendix B for more information about parameter precedence.

Authentication information will be accepted from both files. For ease of administration, it is recommended both file types be utilized in the way described.

Guidelines

- The generic filename may be 46xxsettings.txt and this is the default filename expected by the software. A different filename may be assigned as long as the GET statement in the slnk_cfg.cfg command is programmed to find it. If there is no GET statement, the software looks for a 46xxsettings.txt file.
- Each specific filename must have the form of SIP_xxxx.txt, where xxxx is the username assigned to each individual user by the system administrator. The username is entered into the handset at the login prompt or specified by the parameter SIP_USERNAME1 in a remote configuration file. See Chapter 6: *Configure Each Avaya 3641/3645/6120/6140 IP Wireless Handset*, section *The Admin Menu*, subsection *SIP Registration*.
- Username parameters are: numbers only, no spaces, no punctuation, 1-13 characters. See the sample 46xxsettings.txt file for complete information on allowed characters.
- Information in the specific file should contain data specific to each user such as authentication credentials and line appearance data.
- Lines may appear in any order although maintenance may be simplified by preserving the order in the supplied example file. Lines in the WLAN section of the 364x section should remain in the same order as they appear in the sample file as some later parameters depend on earlier parameters.

Program each of the files according to the following instructions.

The 46xxsettings.txt file

The settings file contains the parameters that you can use to customize the Avaya IP Wireless Handset for your enterprise. Contact your service representative for a sample of this file or if you need additional assistance.

Note:
Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Wireless Handset can use Avaya-provided default values and operate without the settings file if you have no settings that you want to customize. Note that you can also change these settings with DHCP.

Note:
Use one settings file for all your Avaya IP Wireless Handset. The settings file includes the 3641/3645/6120/6140 IP Wireless Handsets covered in this document. The settings file also includes parameters for other IP Deskphones as covered in their respective administrator guides.

The settings that pertain to the 3641/3645/6120/6140 IP Wireless Handsets can include the following types of statements, one per line. Any invalid statement is ignored. The statement types are:

- SET statements of the form **SET *parameter_name value***. If the desired value contains a blank or a comma, the entire value must by placed within double quotes.
- GOTO statements, of the form **GOTO *tag***. GOTO statements cause the handset to continue interpreting the configuration file after a line that begins with a "**# tag**" statement. If no such line exists in the upgrade or settings file after the GOTO, the phone ignores anything in the file after the GOTO.
- Tags are lines that begin with a # tag; tag is an unquoted string and cannot contain a space or comma.
- IF statements, of the form **IF $*name SEQ string* GOTO *tag***, where name is one of the system parameters shown in the table below. Conditionals cause the GOTO command to be processed if the (string equivalent) value of name is equal to string. Note that the string comparison ignores case, so "Abc" matches "ABC" or "abc". If no such name exists, the entire conditional is ignored.
- Format of SET statements: the string must be included in double quotes if it includes spaces or commas. Any string may be in double quotes, so 1 and "1" are equivalent as are "abc" and abc..

Any line which does not match one of the previous statement types is ignored and, therefore, can be treated as a comment. By convention, in the settings files distributed by Avaya, any line intended to be ignored by the phone or read as a comment starts with "##".

Settings file system parameters that can be tested in an IF statement

GROUP	The value is whatever the user sets in the Admin menus/HAT for Phone Group– number from 0-999 (default is 0)

See the self-documenting sample 46xxsettings.txt file for complete information about the settings. Use the information in Chapter 5 for Admin menu settings and the table in Appendix B for further information about SIP parameters.

The handset-specific files

The handset-specific configuration file provides specific information for the handset to identify itself and communicate with other handsets. Each handset must have its own file with a unique filename.

Note:
Each handset must have a specific filename with the form of SIP_[username].txt where [username] is as assigned to each individual user by the system administrator (e.g. sip_3001.txt or sip_JohnDoe.txt). Username requirements are: numbers only, no spaces, no punctuation, 1-13 characters.

The **** SIP SETTINGS **** section of the 46xxsettings.txt file contains sample parameter information. Use this section to start your custom user files.

Note:
The specific file should contain data specific to each user such as authentication credentials and line appearance data. See the *SIP Registration* section in Chapter 6: *Configure Each Avaya 3641/3645/6120/6140 IP Wireless Handset*.

Gather information

Gather the following information:

- Usernames and corresponding passwords
- Extension numbers for up to 5 lines per user
- Caller ID for each of the 5 lines (optional)
- Other parameters as shown in the sample file
- Favorites to be programmed in the generic file. A total of 15 Favorites are allowed.

Create username file

Program a file for each username. The following parameters must be present in the username file:

SIP_USERNAME (1-6): the first set is required (SIP_USERNAME1 and SIP_PASSWORD1) unless they are to be entered at handset startup in the login screen or are already added in HAT or Admin menus. Usernames 2-6 are optional

and are used to provide more credentials for authentication when more than one line is defined.

SIP_PASSWORD (1-6): as above.

SIP_LINE (1-5): up to five lines may be identified.

SIP_LINE_CALLID (1-5): a different caller ID may be set for each line.

SIP_FAVORITES: up to 15 Favorites are allowed. These should be specified in the generic configuration file or the phone specific file but not both, as an entry in the phone specific file will override the same entry in the generic file.

Sample file

The following sample file has all six usernames and passwords defined. It has all five lines defined and each line has a defined caller ID. Three Favorites are defined. See the 46xxsettings.txt file for information on allowed characters and other parameter possibilities.

The name of the file is SIP_USERNAME1.txt.

```
SET SIP_USERNAME1 "4711"
SET SIP_PASSWORD1 "1174"
SET SIP_USERNAME2 "4712"
SET SIP_PASSWORD2 "2174"
SET SIP_USERNAME3 "4713"
SET SIP_PASSWORD3 "3174"
SET SIP_USERNAME4 "4714"
SET SIP_PASSWORD4 "4174"
SET SIP_USERNAME5 "4715"
SET SIP_PASSWORD5 "5174"
SET SIP_USERNAME6 "4716"
SET SIP_PASSWORD6 "6174"
##
SET SIP_LINE1 "4711"
SET SIP_LINE2 "4711"
SET SIP_LINE3 "4711"
SET SIP_LINE4 "4712"
SET SIP_LINE5 "4713"
##
SET SIP_LINE_CALLID1 "4711 Miller"
SET SIP_LINE_CALLID2 "4711 Miller"
SET SIP_LINE_CALLID3 "4711 Miller"
SET SIP_LINE_CALLID4 "4712 Smith"
SET SIP_LINE_CALLID5 "4713 Johnson"
##
SET SIP_FAVORITES 1231;"Favorite1",1232;"Favorite2"
```

Loading SIP configuration files onto HTTP/TFTP server

Move the46xxsettings.txt file and each SIP_[username].txt file to the server designated for handset support. If using a TFTP server, the files must be in the root directory. If using an HTTP server, the exact location of the files must be specified in the HTTP Server Directory Path setting. See the Admin menu options for more information.

Ensure the HTTP/TFTP server is started.

Chapter Five: Downloading and installing the handset software

All Avaya 3641/3645/6120/6140 IP Wireless Handsets are shipped with a software load that allows them to associate to a wireless LAN and download functional software from a HTTP/TFTP server once properly configured. For the handsets to perform properly, you must configure the handsets properly and must allow the handsets to download appropriate software from the HTTP/TFTP server as outlined in the following paragraphs.

The following process details the steps to configure Avaya 3641/3645/6120/6140 IP Wireless Handsets and download software via over-the-air file transfer.

Note:
You may need to charge the handset first. See Chapter 9: *Using the 3641/3645/6120/6140 Handset*.

Minimum Configuration Process

The handset requires minimum configuration in order to associate with an access point (AP). Once the handset gains access to the network, the remaining configuration parameters can be automatically obtained through the 46xxsetting.txt file. See the *Remote Configuration Files* section below. If the Remote Config file is not used, you may use the HAT tool to set all parameters in each handset, or by manually opening the Admin menu on each handset and entering the configuration information. The options are listed in the following paragraph in decreasing order of efficiency:

- HAT plus Remote Config: Use the HAT tool to set minimum parameters in each handset and then turn on the handset and allow it to download remaining parameters from the 46xxsettings file.
- Manual plus Remote Config: Manually configure the minimum settings in each handset and then turn on the handset and allow it to download remaining parameters from the 46xxsettings file.
- All HAT: use the HAT tool to set all parameters in each handset.

The option you choose depends upon a number of factors including the number of handsets you need to configure, the availability of the 46xxsettings file, and the installation of the HAT utility.

Configuration sequence

1. Download the latest Avaya 3641/3645/6120/6140 IP Wireless Handset IP software from http://support.avaya.com.
2. Load the latest version of the SIP software and place it on the designated server and ensure the server is started. The slnk_cfg.cfg is downloaded first by the phone, and defines the SIP code files that will be subsequently downloaded. Ensure that you use the slnk_cfg.cfg file that comes with the latest version of the SIP code and do not change the order of the files within slnk_cfg.cfg.

   The following six files are included in the typical SIP software package.

Description	Filename
Configuration file	slnk_cfg.cfg
PHINTL (language translation)	pi1400sa.bin
USB downloader	pd14udsa.bin
Over-The-Air Downloader (OTADL)	pd14odsa.bin
OTADL Shim	pd14shsa.bin
Functional (telephony protocol)	pd14csa.bin

Note:
See the next chapter Chapter 6: *Configure Each Avaya 3641/3645/6120/6140 IP Wireless Handset* for complete information on configuring the handsets as described in steps 3 through 5 below.

3. [Conditional] If using the 46xxsettings file for remote configuration, set the parameters in the file. See previous chapter, Chapter 4: *System Configuration*, and *Appendix B* for detailed information. Ensure the slnk_cfg.cfg GET statement points to the correct filename if it is different than 46xxsettings.txt.
4. Verify the license type is set to SIP (license 56) in the Admin menu. If not, manually change the license protocol on each handset. If any parameters have been changed, run Restore Defaults after changing the license type. See Chapter 6 for exact instructions.
5. Depending on which configuration method you have chosen, set parameters on each handset.
   a. HAT plus Remote: Set minimum parameters for associating to the WLAN:
      - QoS method: Configure the QoS handset mode to match the AP and site QoS plan. Follow the VIEW Configuration Guide for the appropriate make/model of WLAN.
      - SSID.
      - Security method: Configure handset security settings to match AP configuration and RADIUS server settings. If WPA2-Enterprise

security is used, you must install credentials onto the handset. For EAP-FAST, you must provision the PAC file and for PEAP you must enroll the handset with a certificate (initial configuration requires use of the HAT). See the *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section in this guide for details.

- Any security sub-options required for initial access to network.
- Regulatory domain.
- Radio band.
- DHCP or static IP addresses.

b. Manual plus Remote: Set minimum parameters for associating to the WLAN as above.

c. HAT: Set all parameters for associating to the WLAN as above.

See the next chapter, Chapter Six: *Configure Each Avaya 3641/3645/6120/6140 IP Wireless Handset* for detailed configuration instructions.

6. Restart the handset.
7. The handset then downloads the SIP code. The status bar starts incrementing across the display for each function that is being performed in the download process. Upon completion of the update process, the handset restarts with the new software.

During the second download cycle, the handset receives code from the HTTP/TFTP server for system configuration and for its own settings. Once this second cycle is complete, the handset is ready to use.

Note:
For future software upgrades, update the files that are stored on the HTTP/TFTP server. Each time you power on the handset, the handset checks with the HTTP/TFTP server to ensure that the handset has the proper software version.

Chapter Six: Configuring each Avaya 3641/3645/6120/6140 IP Wireless Handset

To configure the Avaya 3641/3645/6120/6140 IP Wireless Handset, carry out the following steps:

Power up the handset and download the software. If the handset code needs to be updated, the SIP code will now download to the handset. The status bar will increment fully across the display for each function that is being performed in the download process. Upon completion of the update process, the handset will re-boot with the new software.

During the second download cycle, the handset receives code from the designated server for system configuration and for its own settings. Once this second cycle is complete, the handset is ready for use.

Handset Administration Tool

The Handset Administration Tool is a software utility to automate the configuration of multiple Avaya 3641/3645/6120/6140 IP Wireless Handsets and perform various administration tasks. For complete data, please see *Avaya 3641/3645/6120/6140 IP Wireless Handsets Administration Tool*.

Remote configuration

After you configure the initial settings either manually or thorough the HAT, the handset can obtain the remaining parameters from the 46xxsettings.txt file and its SIP_<username> .txt file.

The Admin (Administration) menu

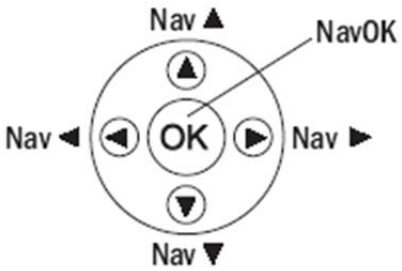
The **Admin** menu contains configuration options that are stored locally on each handset. Each handset is independent, and if you do not want to apply the default settings, the **Admin** options must be set in each handset requiring different settings. Default settings can be found later in this document. The handset **Admin** menu can be accessed in one of two ways:

- Power off the handset, press and hold the **START** key. While holding the **START** key, press and release the **END** key. When the Admin menu appears, release the **START** key.
- Press and release the **END** key. Press and hold the **START** key. When the Admin menu appears, release the **START** key.

Note:
If an admin password has been set, the display will require its entry before opening the **Admin** menu. The default password is 27238 (“CRAFT”). If no password is set, the display will proceed directly into the **Admin** menu.

Navigation

The navigation keys just below the softkeys are used to navigate through and select menu options. These are referred to as **Nav▲**, **Nav▼**, **Nav◄**, **Nav►**, and **NavOK**.



Toggle options

Some menu items have only two options, which operate on a toggle basis. The current setting is shown below the menu heading on the info line. The other available setting is highlighted in the menu list. Press **NavOK** to activate the highlighted setting.

For example, when predial is disabled, the info line displays **Predial Disabled** and the highlighted menu item is the **Enable Predial** option. Press **NavOK** to enable predial. The info line will change to display **Predial Enabled**.

In another example, when the info line displays **Currently Speaker**, the highlighted menu option is **Ring in Headset**. Press **NavOK** to select **Ring in Headset**, The ring will now sound in the headset and the info line will change to **Currently Headset**.

Data entry and editing

An asterisk (*) next to an option on the display indicates that the option is selected. Use the **Nav** keys and the softkeys to navigate and select desired options.

Enter numbers by pressing the buttons on the keypad. The blinking underscore identifies the current cursor position. When entering alphanumeric strings, the **CAPS**/**caps** softkey displays and you can press the softkey to toggle the case. Enter letters by repeatedly pressing the corresponding key until the desired letter displays on the screen. Use the **CAPS** softkey to change the case as needed.

To edit during entry of data, delete the character to the left of the cursor by pressing the **Del** softkey. To replace an entry, delete the entry by pressing the **Clr** softkey and then enter the new data. To edit an existing entry, use **Nav◄** and **Nav►** to move the cursor

position, and then press the **Del** softkey to delete the character to the left. Insert new data by pressing the buttons on the keypad.

Alphanumeric entries:

Key	CAPS	Caps
1	1	1
2	2 a b c	2 A B C
3	3 d e f	3 D E F
4	4 g h I	4 G H I
5	5 j k l	5 J K L
6	6 m n o	6 M N O
7	7 p q r s	7 P Q R S
8	8 t u v	8 T U V
9	9 w x y z	9 W X Y Z
0	0	0
*****	* . ! $ % & ’ ( ) + , : ; / \ = @ ~ - _	
#	<space>	

Admin Menu Table

The following table lists the **Admin** menu items. The default settings have an * prior to the option. Detailed descriptions of each option appear below the table.

1st level	2nd level	3rd level	4th level	5th level
Phone Config	Language	*English Français Deutsch Español Italiano		
	Telephony Protocol	*Type 033 Type 056		
	PTT/Emerg. Button	Emergency Dial	Emergency # [Enable/Disable]	
			Emergency Number	[Enter Number] [Enter Name]
		Push-to-talk	PTT [Enable/*Disable]	
			Allowed Channels	*Channel 1 *Channel 2 *…. *Channel 24

1st level	2nd level	3rd level	4th level	5th level
			Name Channels	[list]
			Priority Channel	Priority Channel On/*Off
				Name Channel
	Time Zone	[list] *GMT		
	Daylight Savings	*DST No Adjust DST Auto (USA) DST Auto (AUS) DST Auto (EURO)		
	Protected Spd-dial	Enter Number	Enter Name	Assign Speed-Dial
	Password *Enable/Disable			
	[If Password is enabled] Change Password			
	Phone Group			
	SIP Registration	Login Reg 2 Reg 3 Reg 4 Reg 5 Reg 6	[for each option] Username Password	
	Clear SIP Regist.			
	*Enable OAI Disable OAI			
	Location Service	Enable RTLS *Disable RTLS		
		Transmit Interval	15 seconds 30 seconds 1 minute 5 minutes *10 minutes	
		Location Server IP	Enter IP	
		ELP Port	Enter Port *8552	
Network Config	IP Addresses	*Use DHCP		
		Static IP	Phone IP	

1st level	2nd level	3rd level	4th level	5th level
			Default Gateway Subnet Mask	
			File Servers	TFTP Server IP HTTP Server IP HTTP Port HTTPDir Path
			Syslog Server IP DNS Server IP DNS Domain Time Server IP SVP Server IP OAI Server IP	
	SS ID	[enter]		
	WLAN Settings			

3rd level	4th level	5th level	6th level	7th level
*Custom	Security	*None		
		WEP	Authentication	*Open System Shared Key
			WEP [Enable/*Disable]	
			Key Information	Default Key Key Length Key 1-4
		WPA2-PSK	*Passphrase Pre-Shared Key	
		WPA-PSK	*Passphrase Pre-Shared Key	
		Cisco FSR	Username Password	
		WPA2-Enterprise	Authentication	*EAP-FAST PEAP
			Fast Handoff	*CCKM OKC
			Username	
			Password	
			Delete [Cert./PAC]	
	QoS	*SVP	DSCP tags	WT in call (*46) WT standby

3rd level	4th level	5th level	6th level	7th level
				(*34) Other (*0)
		Wi-Fi Standard	DSCP tags	Voice (*46) Control (*34) Other (*0)
			Admission Cntrl	*Mandatory Optional
CCX	WPA2-Enterprise	Authentication	*EAP-FAST PEAP	
		Fast Handoff	*CCKM	
		Username		
		Password		
		Delete [Cert./PAC]	[Yes/No]	
	QoS	DSCP tags	Voice (*46)	
			Control (*34)	
			Other (*0)	

1st level	2nd level	3rd level	4th level	5th level
Network Config	Reg. Domain	01 02 03 04 05 06 07 08		
		→	[802.11 Config]	
			a →	[802.11a]† 5.150–5.250 5.250–5.350 DFS 5.470–5.650 DFS 5.470–5.725 DFS 5.725–5.825 5.725-5.850
			‡b & b/g mixed g only	

1st level	2nd level	3rd level	4th level	5th level
			→	[Transmit Power] 5mW (7dBm) 10mW (10dBm) 20mW (13dBm) *30mW (15dBm) 40mW (16dBm) 50mW (17dBm) 100mW (20dBm)
Diagnostics	Run Site Survey Enable Diagnostics Disable Diagnostics			
	Syslog Mode	*Disabled Errors Events Full		
	Halt on Error/ *Restart on Error			
Restore Defaults				
Demos	Graphics Demo			

* default setting

† Only those 802.11a bands that are available in the selected domain will be listed. See Appendix A for complete information.

‡ Sub-bands have not been established for the b and b/g mixed or the g-only mode at this writing. The software has been configured to to accommodate these ranges once established. Until added, if you select either of these two modes, the Transmit Power options are displayed.

Note:
Modifications of settings under **WLAN Settings** = "**CCX**" may get reflected in the corresponding settings under **WLAN Settings** = "**Custom**" or vice versa. If you change the configuration from "**CCX**" to "**Custom**" or vice versa, you must double-check all settings.

Phone configuration

Language

The **Language** option is available on both the **Admin** and **Config** menus. Select the desired language from the list. The default language is **English**.

Telephony Protocol

You can select the VoIP protocol that your site is licensed to download and run using the Telephony Protocol. The SIP protocol used for the Avaya 3641/3645/6120/6140 IP Wireless Handsets requires license option selection **56**. Any other protocol will cause the handset to malfunction.

Note:
You may need to change the protocol from the default (**Type 033**) to the SIP protocol which is **Type 056**. If any parameters have been changed, run **Restore Defaults** before configuring settings under the new protocol.

PTT/Emerg. Button

This option appears only on the Avaya 3645/6140 IP Wireless Handset. You can configure the Push-to-talk button on the left side of the handset to either standard PTT functionality or to dial the specified emergency call number when pressed twice within two seconds. In the standard PTT functionality, you push and hold the button to transmit a PTT broadcast. These are mutually exclusive options. Both are disabled by default.

When you use the Handset Administration Tool to configure this option, ensure that you disable the PTT option in the **PTT Admin tab** under **Handset type** before enabling the **Emergency Dial** option in the **Phone Config** tab. When you enable **PTT**, the **Emergency Dial** option will not be available and is grayed out.

Push-to-talk [Disable/Enable] – If enabled, the PTT options will appear on the **Config** menu for the end user to subscribe to allowed channels, etc. If disabled, the PTT options will not appear on the **Config** menu and the Emergency Dial option may be enabled.

PTT is disabled by default. When enabled, all 24 PTT channels are allowed by default. To toggle the allowed status of any channel, select **Allowed Channels**, scroll to the channel to be disallowed and press **NavOK**. Allowed channels are displayed with an asterisk (*) in the left column. Only those channels allowed in the **Admin** menu will appear on the Config menu where they can be subscribed to by the end user. The priority channel, labeled by default as channel 25, may be set and made available to all PTT handsets. When you make a PTT broadcast on the priority channel, the broadcast overrides any active PTT transmission on all other channels.

Note:
When using the HAT, the administrator can select a default PTT channel for the user. However, the user can override the administrator’s choice and change the default channel to any enabled channel, except the priority channel. If a default channel is not set, the user must select a channel from the enabled channel list before transmitting.

Emergency Dial – the **Emergency Dial** option allows you to enable or disable the feature. When enabled, the handset will dial the number programmed into the **Emergency Number** option when the panic button is pressed twice within two seconds.

Caution!
If you use the emergency dial feature, only a telephone call is setup; however the ferature is inoperable if the wireless system or the call server fails for any reason. Do not rely on it as your sole method of emergency notification.

Note:
Follow your dial plan rules when entering the emergency number to be dialed. For example,,if an outside number is to be dialed and a prefix is required to obtain an outside line, enter the prefix as part of the emergency number.

Note:
Once you enter an emergency number, you can only modifiy the number..You can clear the number only by restoring the handset to defaults.

Time Zone

Worldwide time zone options are available. Greenwich Mean Time (GMT) is the default.

Daylight Savings

You can adjust the handset for daylight savings time.

Protected Speed-dial

The protected speed-dial number is a number that is programmed to be called in emergencies. The number appears as the first item on the speed-dial list and is specially marked with a greater-than symbol (>) as the first character in its name. Only one such number can be programmed. Enter the number to be dialed and the name, for example, Security, and scroll to assign to one key press. The choices for this key press are 1-9, 0, *, or #. The carat represents the volume up and down buttons. This number must be programmed in every handset. This setting cannot be modified by the user. This feature is not available in a handset where the user has disabled **Pre-dial** in the **Config** menu.

Password Enable/Disable/Change

The password option controls access to the **Admin** menu. It is enabled by default with the password 27238. The **Password** option operates as a toggle between **Enabled** and **Disabled**. The info line will display the current state. Press **NavOK** to change the password protection state. You must enter the default or previously set password to modify the password requirement and to verify the change. **Change Password** option appears only if you have enabled the password..The password is disabled by default. You must set the password in each handset for which controlled access is desired. The password may be up to 18 characters in length. Only numbers and letters are allowed.

Note:
You can defined the admin password in the HAT, in the Admin menu or by using the PROCPSWD configuration setting in the 46xxsettings.txt file. HAT and admin menus allow a wider range of passwords than remote configuration. If you decide to set the PROCPSWD parameter, it is limited to a maximum of seven (7) digits. Only numbers may be used. See the PROCPSWD parameter at the end of this document for more information.

Phone Group

The Phone Group can be denoted by an integer from 0 to 999. The default is 0. This value can be used by the remote config files for specifying some parameters only for some groups. See the 46xxsettings.txt file for more information.

SIP Registration

You can configure individual handsets to correspond with the SIP configuration information in the HTTP/TFTP server. If both HTTP and TFTP IP addresses are present, the handset attempts to download files from the HTTP server(s) first and only tries TFTP if the file(s) are not found on the HTTP server. The handset is then automatically identified at startup. If username and password information is not configured in the **Admin** menu, then this information will be requested at startup.

In either case, the username must agree with a corresponding configuration file. See Chapter 4 *System Configuration* section *Configure SIP Handset Files.*

You can specify a username and password for automatically acquiring SIP configuration information using **Login**. If you have not specified any username, the SIP handset requests username and password at startup and the system ignores any additional registrations that you have specified.

The username should correspond to the primary (line 1) dial number assigned to the user. The username and password should also correspond to the authentication credentials as created by your system administrator for your primary line registration. You can erase the usernames or passwords by selecting the item, then pressing the **Bksp** softkey and then the **Save** softkey.

Reg 2, through **Reg 6** allow you to specify additional authentication usernames and passwords that might be required by your handset for any additional line appearances (registrations) that may appear in the specific user's configuration file. This information will be ignored if a **Login** username is not provided.

OAI Enable/Disable

The Avaya Wireless Application Interface Gateway or Open Application Interface (OAI) enables third-party computer applications to display alphanumeric messages on the handset display and accept input from the handset keypad. Refer to the *Installation* document for the Open Applications Interface (OAI) Gateway at https://support.avaya.com/css/P8/documents/003745895 for information about installing and administering the Avaya Wireless Application Interface Gateway.

If you have an Avaya Wireless Application Interface Gateway installed in your system, you may optionally enable OAI in each handset. You may select whether the handset should attempt to connect to the Avaya Wireless Application Interface Gateway by choosing either the **Enable** or **Disable** options in this menu.

If OAI is enabled, and an IP address (called the **OAI Server IP**) is available to the handset through either DHCP or Static IP configuration, the handset communicates with the Gateway at power-on, and periodically while it is powered-on. If you don't have an Avaya Wireless Application Interface Gateway installed at your site, you should disable the OAI feature to preserve network bandwidth and battery life.

Location Service

You can enable or disable the Ekahau Real-Time Location System (RTLS), select a transmit interval, or enter a static IP address for the Ekahau Positioning Engine (EPE) using the Location service. Location services capability is provided by the EPE 4.0 using Ekahau Location Protocol (ELP). See Ekahau's user documentation for more information.

RTLS [Enable/Disable] The RTLS is disabled by default. Press **NavOK** to toggle to the alternate setting. When RTLS is enabled, the handset will display the RTLS icon in the top center of the screen.

The ring indicator icon will take precedence over the RTLS icon, i.e. the new icon will not be visible while the handset is ringing. When ringing has ceased and the ring indicator becomes inactive, the RTLS icon will again appear (regardless of hook state).

Transmit interval allows selection of **15 seconds**, **30 seconds**, **1 minute**, **5 minutes**, or **10 minutes** for maximum time between transmit intervals. Default transmit interval is 10 minutes. Press **NavOK** to select the desired transmit interval.

Note:
To optimize battery life, the interval between sending out ELP updates will vary based on handset state. It is expected that ELP updates will occur at most every two to six seconds and at least every few minutes. If you want improved tracking capability, set the transmit interval for a shorter time between ELP updates. Increasing the frequency of transmissions will decrease battery life.

Location Server IP allows the user to statically enter the IP address of the EPE. Enter the IP address and press **NavOK** to save.

Note:
Ekahau clients are not expected to find the EPE automatically. Regardless of the handset's selection of DHCP or static IP, the EPE IP address must be statically entered in the Ekahau Admin menus or HAT.

ELP Port allows the user to select the port number to which ELP updates are sent to at the Location Server IP address. It must match the value configured in the Ekahau Positioning Engine for proper functionality. The ELP port number must be greater than zero and less than 65536. Default is 8552. Enter the port number and press **NavOK** to save.

Network Config

IP Addresses

There are two modes in which the handset can operate: DHCP-enabled or Static IP. Select the mode for operation from the IP Address menu:

Use DHCP mode will use Dynamic Host Configuration Protocol to assign an IP Address each time the handset is turned on. If DHCP is enabled, the handset also receives all other IP Address configurations from the DHCP server. If a needed parameter is not supplied by DHCP and there is a static value, the static value will be used.

You can use the **Static IP** to manually set a fixed IP Address. If you have selected Static IP, the handset will prompt for the IP addresses for each configurable network component. When entering addresses, enter the digits only, including leading zeroes.

Regardless of the mode in which the handset is operating, the following components are required and must be configured as part of the SIP system:

Phone IP: The IP address of the handset. This is automatically assigned if DHCP is used. If using Static IP configuration, you must obtain a unique IP address for each handset from your network administrator.

Default Gateway and Subnet Mask are used to identify subnets, when using a complex network, which includes routers. Both of these must be configured either with an IP address under Static IP. These must not set to 000.000.000.000 or 255.255.255.255 or with DHCP for the handset to contact any network components on a different subnet. If configured on the DHCP server, use option 3 for the Default Gateway and option 1 for the Subnet Mask. Contact the network administrator for the proper settings for the network.

Note:
You cannot use Avaya 3641/3645/6120/6140 IP Wireless Handsets with uninterrupted service between subnets unless specific LAN components are present. Certain AP/Ethernet switch combinations establish a Layer-2 tunnel across subnets that enable the handsets to roam. Without this capability, any call in progress is dropped when the user moves out of range and the handset must restart in order to to resume functionality in the new subnet area.

Ensure that all your APs are attached to the same subnet for proper operation. The handset can change subnets if DHCP is enabled and the handset is powered off and then powered on when within range of APs on the new subnet. Note that you cannot “ roam” with wireless handsets across subnets, since the handsets cannot change IP addresses while they are operational.

Note:
See *Best Practices for Deploying Enterprise-Grade Wi-Fi Telephony* for detailed configuration information.

File Servers: The file server holds software images for updating the handsets and contains the handset files. If the HTTP server IP or TFTP server IP is configured (not set

to 0.0.0.0 or 255.255.255.255) with either Static IP configuration or using DHCP option 66 (HTTP/TFTP server), or the boot server/next server (siaddr) field, the handset will check for newer software each time it is powered on or comes back into range of your network. This check takes only seconds and ensures that all handsets in your network are kept up-to-date with the same version of software. In a SIP environment, an HTTP server is usually employed for this purpose.

TFTP Server IP: The IP address of a TFTP server on your network, A TFTP server is not required if the files are on an HTTP server.

HTTP Server IP address: A single IP address for the HTTP server on your network. An HTTP server is not required if the files are on a TFTP server.

HTTP Port: An integer from 0-65535 and will default to 80

HTTP Server Directory Path: A string from 1-127 characters that identifies the location of the configuration files.

Syslog Server IP: The IP address of the syslog server. See Chapter Ten: *Diagnostic Tools* for more information.

DNS IP address: The IP address of the DNS server.

DNS domain: A string from 1-127 characters.

Time Server IP: The IP address of the time server.

SVP Server IP: The IP address of the Avaya SVP Server. If using Static IP configuration, this is the IP address of the Avaya SVP Server. Note that the Avaya SVP Server must be statically configured to have a permanent IP address. If DHCP is being used, the handset will try the following, in order: the DHCP option 151, then a DNS lookup of “SLNKSVP2” if the DHCP options 6 (DNS server) and 15 (Domain Name) are configured.

OAI Server IP: The IP address of the SpectraLink 8000 OAI Gateway. If using Static IP configuration, this is the IP address of the SpectraLink 8000 OAI Gateway. If DHCP is being used, the handset will try the DHCP option 152.

SSID

Enter the SSID.

WLAN Settings

Select between Custom and CCX modes. The Custom mode allows explicit control of all of the security and QoS settings. Using CCX mode automatically enables the CCXv4 features and functions, with only the 802.1X mechanism needing to be selected.

Custom – Security

Note:
Handset security setting should exactly match the settings in your APs. Consult the *VIEW Configuration Guide* for the APs installed in your facility for information on which of the security methods are certified.

Note:
Encryption keys, Username and Password displayed as you enter them. For security reasons, these items will not display when a user returns to the Admin menu.

***NONE** disables any 802.11 encryption or security authentication mechanisms.

WEP (Wired Equivalent Privacy) is a wireless encryption protocol that encrypts data frames on the wireless medium allowing for greater security in the wireless network. If WEP is required at this site, you must configure each handset to correspond with the encryption protocol set up in the APs. Select the entries from the options below to enable the handset to acquire the system.

Authentication

Select either **Open System** or **Shared Key**.

WEP Enable/Disable
Select either **Enable WEP** or **Disable WEP**.

Key Information

Default Key: Enter the key number specified for use by the handsets. This will be **1** through **4**.

Key Length: Select either **40-bit** or **128-bit** depending on the key length specified for use at this location.

Key 1-4: Scroll to the key option that corresponds to the **Default Key** that was entered above. Enter the encryption key as a sequence of hexadecimal characters. (Use the **2** and **3** keys to access hexadecimal digits A through F.

WPA2-PSK: The security features of WPA2 (Wi-Fi Protected Access) using PSK are available and may be used if supported by the APs in the facility. Select either **Passphrase** and enter a passphrase between eight and 63 characters in length or **Pre-Shared Key** and enter the 256-bit key code.

WPA-PSK: The security features of WPA (Wi-Fi Protected Access) using PSK (pre-shared key) are available and may be used if supported by the APs in the facility. Select either **Passphrase** and enter a passphrase between eight and 63 characters in length or **Pre-Shared Key** and enter the 256-bit key code.

Cisco FSR: (Fast Secure Roaming) FSR is designed to minimize call interruptions for Avaya 3641/3645/6120/6140 IP Wireless Handset users as they roam throughout a facility. Cisco FSR requires specific configuration of the Cisco APs in your site. See your Cisco representative for detailed documentation on configuring the APs and other required security services on the wired network. To configure Cisco FSR on a handset, you must enter a Radius Server username and password into each handset.

Username

Enter a username that matches an entry on the RADIUS server. Usernames are alphanumeric strings, and can be entered using the alphanumeric string entry technique.

Password

Enter the password that corresponds to this username.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server. See the *System Components* section for tested models.

Fast Handoff allows the use of either ***CCKM** or **OKC**. These mechanisms allow a phone to quickly and securely roam between APs with a minimum disruption of audio.

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]** option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC on the phone is deleted. If the RADIUS server has enabled “anonymous in-band PAC provisioning”, then the phone automatically re-acquires these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning, the credential on the phone is deleted and a new one needs to be downloaded through the HAT or over the air. See additional details in *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section later in this chapter.

Custom – QoS

SVP mode uses the SVP Server to provide enterprise-grade QoS.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the wireless telephone. Default values are given, but may be overwritten: **WT in call = 46, WT standby = 34, Other = 0**. Once the packets reach the SVP Server, packets are re-tagged using the SVP Server DSCP settings. See the Avaya SVP Server Admin Guide for more information.

Wi-Fi Standard QoS mode uses standards-based traffic controls for QoS, instead of the SVP Server.

DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the wireless telephone. Default values are given but may be overwritten: **Voice = 46, Control = 34, Other = 0**.

Admission Cntrl is used to enable and disable the use of WMM Admission Control by the handset for the AC_VO and AC_VI access categories. If the WLAN is using WMM Admission Control, the handset should be set to ***Mandatory**. If the WLAN is not using WMM Admission Control, the handset should be set to ***Optional**. See the

Best Practices Guide for Deploying Avaya 3641/3645 IP Wireless Handsets for a detailed explanation of the use of WMM Admission Control.

CCX

CCX settings configure the handset for operation as a CCX V4 certified client.

WPA2-Enterprise

The **Authentication** setting can select either ***EAP-FAST** or **PEAP** as the authentication method for RADIUS server. See the System Components section for tested models.

Note that for **Fast Handoff**, the only selection available is ***CCKM.**

Username: Enter a username that matches an entry on your RADIUS server. Alphanumeric strings can be entered using the alphanumeric string entry technique.

Password: Enter the password that corresponds to this username.

The **Delete [PAC/Cert.]**: Option removes expired credentials from the phone. When the authentication method is EAP-FAST the PAC on the phone is deleted. If the RADIUS server has enabled “anonymous in-band PAC provisioning”, then the phone automatically re-acquires these credentials from the RADIUS server over the air. When the authentication method is PEAP or EAP-FAST manual provisioning, the credential on the phone is deleted and a new one needs to be downloaded through the HAT or over the air. See additional details in *WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning* section later in this chapter.

QoS – DSCP tags are used to change the priority settings for various classes of packets as they are transmitted to the network from the Wireless Telephone. Default values are given but may be overwritten: **Voice = 46, Control = 34, Other = 0**.

Regulatory Domain/802.11 and Config/Transmit Power

Regulatory domain, 802.11 configuration and transmit power are interdependent. See Appendix A: *Regulatory Domains* for regulatory domain setting specifications. Check with local authorities for the latest status of national regulations for both 2.4 and 5 GHz wireless LANs. A regulatory domain must be selected in order for the handset to operate. There is no default setting.

FCC requirements dictate that the menu for changing the regulatory domain be available by password, which in our case is the **LINE** key. Press **LINE** and then navigate to the desired domain. Press **NavOK** to set the domain.

01 - North America

02 – Europe

03 – Japan

04 – Singapore

05 – Korea

06 – Taiwan

07 – Hong Kong

08 – Mexico, India

802.11 config

Once the regulatory domain is set, the **802.11 Config** modes are displayed. Only one may be chosen. **802.11(b & b/g mixed)** is the default. Press **NavOK** to set the mode. If the mode has subbands, the **Subband** list is displayed. If the mode does not have subbands, the **Transmit Powe**r list is displayed.

Note:
Use **g only** mode if all of your infrastructure and client devices will use only 802.11g. The handsets will operate up to 54 Mb/s in this mode. If any 802.11b capable clients or infrastructure are used in your wireless LAN then do not use **g only** mode, instead use **802.11b and b/g mixed** mode for optimum performance.

Use **b & b/g mixed** if some of your infrastructure components are compatible with 802.11b. The handsets will operate up to 11 Mb/s.

Subbands have not been established for the **b and b/g mixed** or the **g only** mode at the time of writing this document. Provisions are made in the software to accommodate these ranges once established. Newly added subbands may not appear in the preceding **Admin** menu table..

Subband

Once a mode is set, the subband list will display, if applicable. Only those ranges which are allowed in the set regulatory domain and that pertain to the set mode are displayed. Note that for 802.11a the bands labeled **DFS** will vary depending on the set regulatory domain. Multiple subbands may be set. Navigate to the desired subband and set with **NavOK.** The **Transmit Power** menu will open. Once the **Transmit Power** setting is done, you will be returned to the subband list.

To deselect a subband, navigate to it and press **NavOK**.

Once the subband settings are as desired, press the **Done** softkey to exit to the **Network Setup** menu.

Transmit power

For subbands: The **Transmit Power** list opens when **NavOK** is pressed from the **Subband** menu. A transmit power setting is required for each subband. Only one level may be set per subband. Only those power levels which apply to the regulatory domain and 802.11 mode are listed. Navigate to the desired level and press **NavOK** to set and return to the subband list. Another subband may be selected which repeats the process.

If the highlighted power transmit level is legal on all of the subbands for the set mode, an **All** softkey will appear. Press the **All** softkey to apply that level to all subbands and return to the subband menu where all subbands will now be selected. **All** overrides any previously set power transmit levels.

Without subbands: When the 802.11 mode has no subbands, the **Transmit Power** list is displayed when **NavOK** is pressed to set the mode. Only those power levels which apply to the domain and 802.11 mode are listed. Navigate to the desired level and press **NavOK**. This sets the transmit power level and exits the **Regulatory Domain** menus. The **Network Setup** menu will again display.

Note that the power setting selected specifies the maximum for that band/subband. When Transmit Power Control (TPC) is enabled in the infrastructure, the AP may instruct the handset to use a lower value to match its own transmit power.

Diagnostics

Run Site Survey

The **Site Survey** mode is activated by selecting this option. The site survey starts running immediately upon selecting this option. See Chapter 10: *Diagnostic Tools* for more information about site survey.

Diagnostics Mode

Diagnostics can be enabled or disabled. See Chapter 10: *Diagnostic Tools*, section *Diagnostics Enabled* for a detailed explanation of the **Diagnostics** mode options.

Syslog Mode

See Chapter 10: *Diagnostic Tools*, section *Syslog Mode* for a detailed explanation of the **Syslog** mode options.

Error Handling Mode

The Error Handling mode determines how the handset behaves when an error occurs. The **Halt on Error** option will cause the handset to stop operating if an error message is received. Unless the error is a fatal one, normal operation may be resumed by restarting the handset. The **Restart on Error** option will cause the handset to make every effort to reboot quietly and quickly to standby mode. In either scenario, a call in progress will be lost. **Restart On Error** should be used unless specific error conditions are being investigated.

Error detail may be shown on the display, captured by the syslog server and may also be available for downloading with the Handset Administration Tool. An error memory dump can be taken and sent to Customer Service for escalation and analysis.

Restore defaults

The Restore Defaults option will set all user and administrative parameters except Telephony Protocol to their factory defaults.

Demos

The **Graphics Demo** option starts a demonstration of the handset's OAI graphical capabilities immediately upon selection.

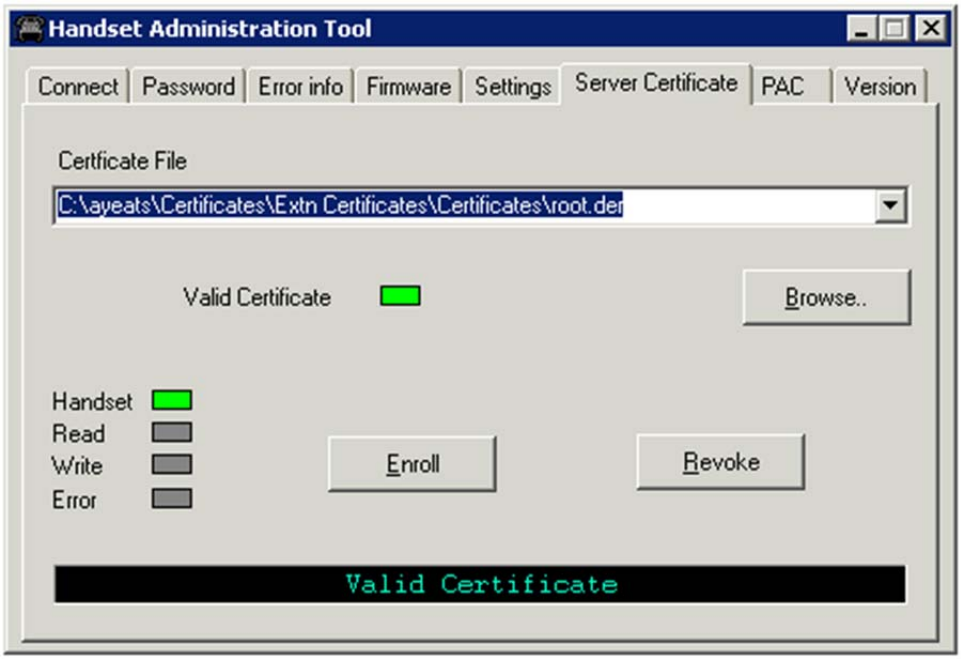
WPA2 Enterprise PEAP Certificate Enrollment and EAP-FAST Manual PAC Provisioning

The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate or manually provisioning PAC files.

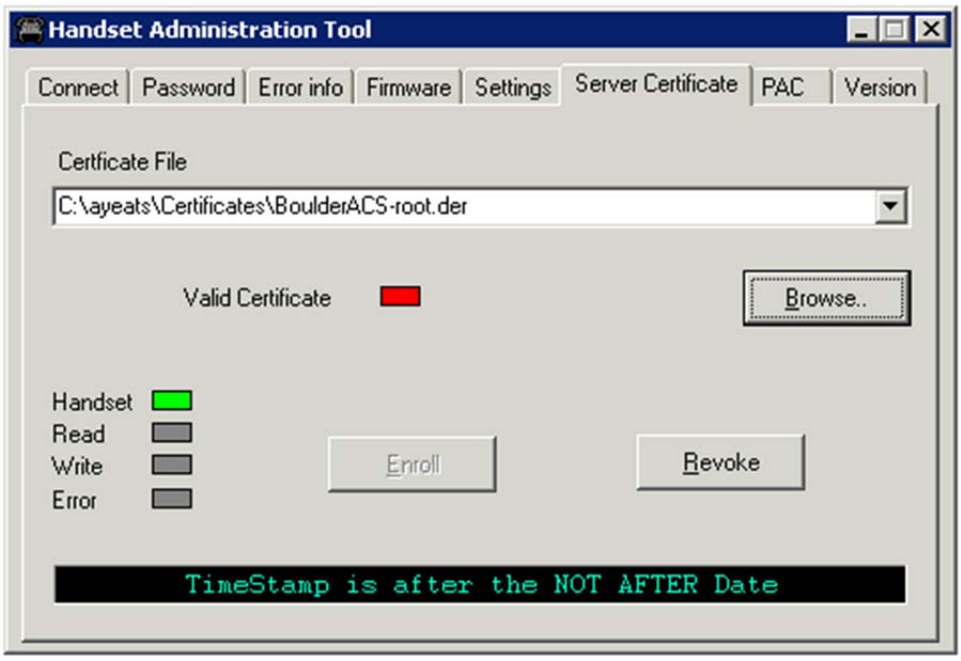
PEAP

The Handset Administration Tool (HAT) is used for enrolling a handset with a PEAP certificate in DER format. Only the DER certification format is supported. All other certificate formats need to be converted into the DER format prior to enrolling the handset. Choose the **Certificate** tab and use the file browser to identify the certificate to be loaded. Once chosen, HAT will perform a rudimentary check on the file to make sure the format is DER and that the certificate date is valid. If these tests pass, HAT will indicate that the certificate is valid and enable the **Enroll** button. Click **Enroll** to install the certificate onto the handset.

The screen below shows a valid certificate that has been identified with the file browser.



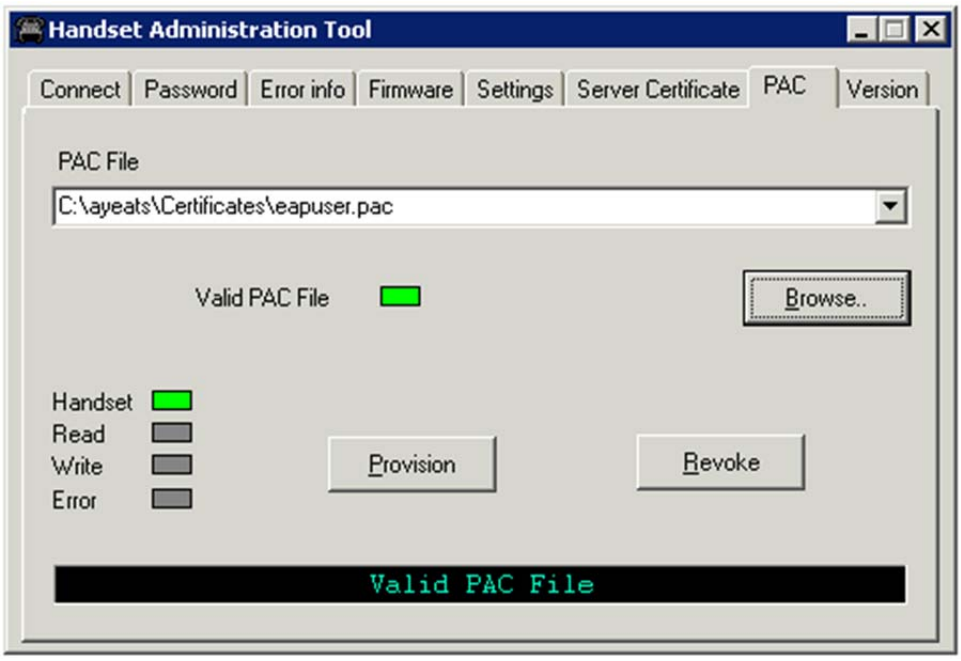
The screen below shows a certificate chosen with the file browser, but found to be invalid because it has expired.



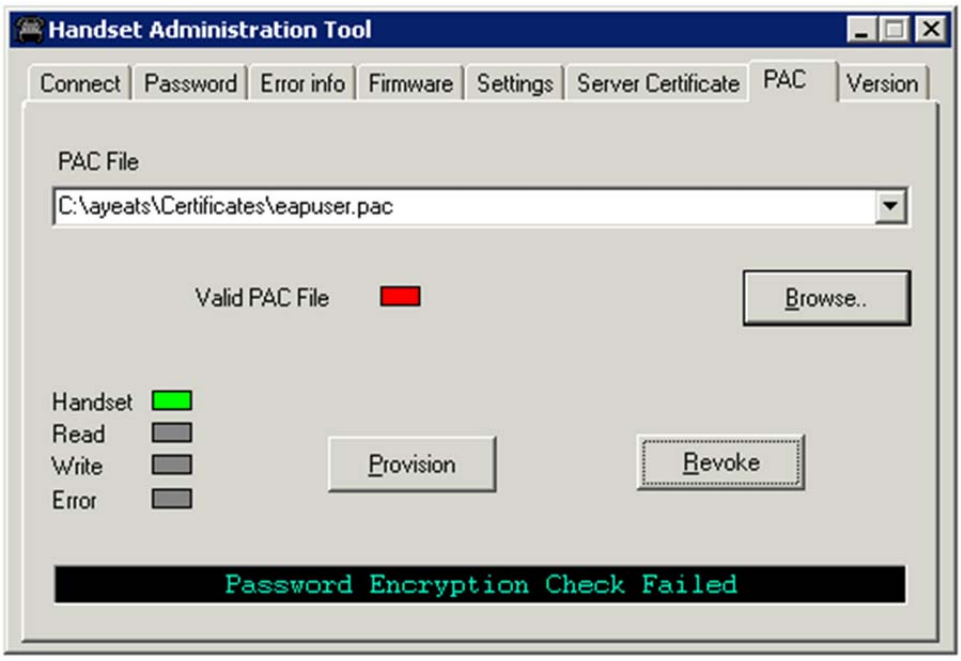
EAP-FAST

For EAP-FAST, HAT is also used for manually provisioning a handset with a Protected Access Credential (PAC). Choose the PAC file with the file browser. The user will be prompted to enter the password used to generate the PAC as part of its validation process. Once the PAC is considered to be valid, the **Provision** button will be available for installing the PAC onto the handset.

The screen below shows a valid PAC identified with the file browser after a valid password has been entered.



The two screens below show the result of entering the wrong password.



If anonymous in-band PAC provisioning is enabled on the RADIUS server, then it is not necessary to download PAC files through HAT. The phone will automatically re-acquire credentials from the RADIUS server over the air.

Admin menu default table

When you select the **Restore Defaults** option, administrative parameters are reset to their factory defaults as shown in the table below. The **Telephony Protocol** setting will not change. User parameters will be reset per the user-defined preferences default settings table. See in Chapter 9 section *User-Defined Preferences* *Default settings tables*.

Menu option	Setting	Sub-option	Sub-sub-option	Default
Phone Config	Language			English
	PTT/Emerg. Button	Emergency Dial		Disabled
		PTT		Disabled
		[if enabled]	Allowed Channels	[all]
			Name Channels	[None set]
			Priority Channel	Disabled
	Time Zone			GMT
	Daylight Saving			DST No Adjust
	Protected Speed-dial			[none set]
	Password			Enabled
	Change Password			[n/a]
	Phone Group			0
	SIP Registration			[None set]
	Clear Regist.			[n/a]
	OAI			Disabled
	Location Service			
		RTLS		Disabled
		Transmit Interval		10 minutes
		Location Server IP		[None set]
		ELP Port		8552
Network Config	IP Addresses			Use DHCP
	SSID*			[None set]
	WLAN Settings	Custom/Security		None
		Custom/QoS	WEP Key Length	40 bit
			QoS (Mode)	SVP

Menu option	Setting	Sub-option	Sub-sub-option	Default
			QoS (DSCP tabs)	WT in call = 46 WT standby = 34 Other = 0
		Cisco FSR	Username Password	[none set]
	Reg. Domain*			[none set]
		802.11 mode		b & b/g mixed
		Transmit Power		30 mW (15 dBm)
Diagnostics	Run Site Survey			[n/a]
	Diagnostics			Disabled
	Syslog Mode			Disabled
	[Error Handling Mode]			Restart on Error

*Minimum requirements for functionality after Restore Defaults:
Set SSID to an available AP and set Regulatory Domain to 01.

Chapter Seven: Testing a handset

Note:
It may be necessary to charge the handset before performing this test. If so, place the handset into the charger for a minimum of two hours before using it.

Verify proper registration and operation of each handset by performing the following tests on each handset in an active wireless area.

1. Power on the handset by pressing the **END** key. A series of messages will be displayed as the handset connects to the system. The handset should display the user extension.
2. Place a call and listen to the audio quality. End the call by pressing the **END** key.
3. Place a call to the handset and verify ring, answer, clear transmit, and clear receive audio.
4. Use the softkeys to verify all softkey programmed features on the handset.
5. Press the **END** key. Any active line indicators should turn off and the extension number display will return.

If any of these steps fails to operate as described, refer to Chapter 11 *Troubleshooting* for corrective action.

Chapter Eight: Certifying the handsets

Test the handsets according to the sequence given in the Testing a handset before determining that the installation is complete. Also, conduct a **Site Survey** mode test according to the directions given in the previous *Diagnostic Tools* section.

The installation may need some adjustments. Note any areas where coverage is conflicting or inadequate. Note any system difficulties and work with your wireless LAN and/or LAN system administrator to determine the cause and possible remedy. See Chapter 12: *Troubleshooting* for clues to possible sources of difficulties. If you make any changes to the system, re-test the device in the same vicinity to determine if the difficulty is resolved.

The installer should not leave the site before performing installation verification.

You must perform these tests in typical operating conditions, especially if heavy loads occur. Testing sequence and procedure is different for every installation. Generally, you should organize the test according to area and volume, placing numerous calls to others who can listen while you perform coverage tests. Note any areas with excessive static or clarity problems and report it to an Avaya service engineer.

The coverage test will also require you to put the handset in **Site Survey** mode and walk the entire coverage area to verify all APs.

Conducting a Site Survey

Conduct a site survey of the installation, by walking the site looking for interfering 802.11 systems, adequate coverage and channel assignment, and correct AP configuration. The site survey discussed here does not replace an RF site survey conducted by professionals who specialize in WLAN design and voice optimization implementations. Avaya offers professional services including RF site surveys.

Note:
The handset's site survey mode is not a replacement for a professional site analysis and must be used only for testing, limited site validation, and troubleshooting.

Note:
The handset's site survey mode does not include functionality to allow for analysis or troubleshooting of 802.11n specific WLAN features.

1. Referring to Chapter 8 *Diagnostic Tools*, section *Run Site Survey*, put a handset into **Site Survey** in the **Any**/**Smry** ESSID mode. Walk throughout the site checking for any expected APs or other ESSIDs.

2. Then, walk the site again, in **MyID**/**Smry** ESSID mode, this time checking that every location has adequate coverage and has good channel allocation.

Note:
There should be at least one AP stronger than -the minimum specified in the following tables.

Note:
At any point, the strongest AP shown should be on a different channel than the next best choice.

The handset configured for 802.11b requires:

- -70 dBm when all 802.11b data rates are available (with only 1 Mbps set Required)
- -65 dBm when only 2 Mbps is set Required and other higher rates enabled
- -64 dBm when only 5.5 Mbps is set Required with 11 Mbps set enabled
- -60 dBm when 11 Mbps is set required and other 802.11b rates disable or enabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s

- The critical factor is the highest data rate that is set to Required or Mandatory. Other 802.11b data rates can be set enabled or disabled. The highest data rate set to Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

The handset configured for 802.11g requires:

- -60 dBm when all 802.11g data are available (with only 6 Mbps set Required)
- -45 dBm when 54 Mbps is set Required and other 802.11g rates Required, Enabled or Disable

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11g	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set to Required or Mandatory. Other 802.11g data rates can be set to Required, Enabled or Disabled. The highest data rate set to Required or Mandatory

determines the RF power available to the wireless telephone for proper operation.

- -45 dBm when 54 Mbps is set Required and other 802.11g rates Required, Enabled or Disable

The handset configured for 802.11a requires:

- -60 dBm when all 802.11a data are available (with only 6 Mbps set Required)
- -45 dBm when 54 bps is set Required and other data rates Required, Enabled or Disabled

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

- The critical factor is the highest data rate set to Required or Mandatory. Other 802.11a data rates can be set enabled or disabled. The highest data rate set to Required or Mandatory determines the RF power available to the wireless telephone for proper operation.

3. Finally, use the single AP (**MyID**/**Detl**) display to check each AP, to ensure it is configured for the proper data rates, beacon interval, 802.11 options enabled, QoS method, and security method.

Make any necessary adjustments to AP locations and configurations and repeat steps 1 through 3 until the site survey shows adequate coverage and correct configuration at every location.

The installation is not complete until these certification steps have been performed. Do not hand out handsets at a site that has not been certified.

Chapter Nine: Using the Avaya 3641/3645/6120/6140 IP Wireless Handset

The handset's battery pack must be fully charged before its first use. Place the handset into the charger for a minimum of two hours before using it.

For complete operational instructions see Avaya 3641/3645/6120/6140 IP Wireless Handset and Accessories User Guide for SIP.

Startup sequence

The Avaya 3641/3645/6120/6140 IP Wireless Handset goes through an initialization sequence at startup. The line icons 1-9 display and count down as the handset steps through this sequence. The countdown sequence is usually very rapid. If there is difficulty at any step that prevents initialization from continuing, an error message will display and the related icon(s) will stay on. See the error table at the back of this document for instructions on how to handle error messages that occur during initialization.

Icon	The icon(s) shown in bold turns off when:
12345678**9**	The handset has located, authenticated, and associated with at least one AP, and is proceeding to bring up higher-layer networking functions.
1234567**8**	The handset is either configured for Static IP or, if configured for DHCP, the DHCP discovery process has started.
123456**7**	If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.
12345**6**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. Indicates one of the following possibilities: 1. Static IP configuration 2. SVP Server address found in DHCP option 151 response 3. SVP Server address found via DNS lookup
1234**5**	All networking functions are complete (notably, DHCP), and the handset is proceeding with establishing the SRP link to the Avaya SVP Server.
123**4**	Note: Used for SVP QoS only and not present when using Wi-Fi Standard QoS or CCXv4. The SRP link is established; all network stack initialization is complete, proceeding with application-specific initialization.

Icon	The icon(s) shown in bold turns off when:
12**3**	SIP application startup is completed. Icon 3 is extinguished if a generic SIP config file is found.
1**2**	Icon 2 is extinguished if a handset specific SIP config file is found.
(no icons) **Registering**	Handset is attempting to register each of the specified line contacts.
(no icons) **EXT. XXXXX**	Handset has registered with at least one contact on one proxy server. Initialization is complete. The handset is in standby mode ready to receive and place calls. The line one contact is displayed.

During the last three steps of this process, the handset contacts the file server and downloads general SIP information, downloads specific information pertaining to the handset, registers with the SIP server, and verifies handset credentials. Once this process is complete, the handset is ready to use.

If the username and password have not been defined in the Admin menu or previously via the Remote Config file, you will be prompted to enter both of these items before the extension number can display. The user name must correspond to the configuration file that contains user-specific information. If the file is not found, an error message will appear and the handset will restart. See Chapter 4: *System Configuration* section *Configure SIP Handset Files*.

Handset modes

Standby mode (on-hook)

In standby mode, the handset is ready for an incoming call or for the user to place an outgoing call. The extension number is shown on the display and there is no dial tone. In this mode, the handset conserves battery power and wireless LAN bandwidth.

When an incoming call arrives, the handset rings; the handset enters the active mode and remains in this mode until the call has ended. The call is answered by pressing the **START** key or the **Answ** or **Spkr** softkey. The handset will ring according to user preference as specified in the standby menus. The ringing can be silenced by pressing the **END** key. If you do not wish to accept the call, some SIP call servers support the ability to press the **Rej** softkey. If supported, the SIP call server will redirect the call as configured by the system administrator.

Active mode (off-hook)

The handset is in the active mode when it is off hook or an incoming call is answered.

When an incoming call occurs during an active call, the handset will play the second call ringing sound until the call is answered, the caller hangs up, or the call transfers to voicemail. If the **END** key is pressed, the first call is terminated and the handset reverts to a full ring.

The active mode utilizes the most bandwidth and battery power. To conserve battery resources, return the handset to the standby mode when a call is completed by pressing the **END** key.

Push-to-talk (PTT) mode

The Avaya 3645/6140 IP Wireless Handsets utilize channels for incoming and outgoing radio communication. While PTT is active, the handset is in PTT mode. It can receive regular phone calls in this mode. When a regular phone call is answered, the handset enters active mode.

Configuration menu mode

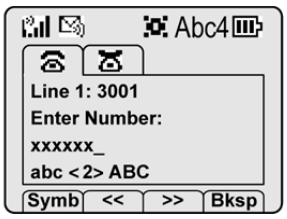
When user preferences are being configured in the Config menu, the handset is on but is not active. If the handset is idle 20 seconds while in the Config menu, it will return to the standby state. Calls can be received but cannot be answered unless you exit the Config menu. If the handset receives an incoming call while in the Config menu, an incoming call ringing icon is displayed and the handset starts ringing as soon as it returns to the standby state.

Messaging mode

If text messaging functions have been programmed through the OAI server, as in a nurse call system, the handset is able to receive text messages. While these messages are being accessed, the handset is in messaging mode. Incoming calls will ring with the second call ringing sound.

The handset display

When active, the handset screen displays either a call status screen or one of several menu screens. The call status screen has the following format:



This example screenshot shows two call tabs indicating that two calls are in progress. The un-selected call tab indicates that we have put another call on hold. The call-status icon for the selected call indicates that this call is being dialed. The text indicates the selected call is on line 1, extension 3001. Enter Number indicates that the handset is

ready to be dialed. Once this call is connected, the connected party's information will appear on the third line, and the fourth line contains help or error messages, as appropriate. The softkeys during this action offer text editing functions.

System icons

Indicator	Function
	The signal-strength icon indicates the strength of the signal and can assist the user in determining if the handset is moving out-of-range.
	The battery icon indicates the amount of charge remaining in the battery pack. When only one level remains, the battery pack needs to be charged.
	The voicemail icon is activated when a new voicemail message is received if the feature is supported by the phone emulation.
	The missed call icon is displayed when a call is not answered. Such calls can be viewed in the Missed Log. It is active only when Call Logging has been enabled by the system administrator.
	The speakerphone icon displays when the speakerphone is active.
	Up and down arrows are displayed when the menu has additional options above or below. Left or right arrows are displayed during editing when the cursor may be moved left or right.
	The Push-to-talk (PTT) ring icon. A PTT call is coming in.
	The priority PTT ring icon. A call is coming in on the priority PTT channel. This call will override any other.
	Location Service icon: indicates the Ekahau Real-Time Location System (RTLS) is enabled.
Locked	Locked indicates that the keypad is locked to prevent accidental activation. Use the **Unlk** softkey plus the # key to unlock it.
[No Service message]	If warning tones are not disabled, an alarm will sound and a descriptive message displays when the handset cannot receive or place calls. You may be outside of the covered area. Walk back into the covered area. The in-service tone indicates service is reestablished.
	The download icon indicates that the handset is downloading code. This icon only appears while the handset is running the over-the-air downloader. It appears to the right of the Signal Strength icon in the same location as the Voicemail icon.
	The download failure icon indicates that the handset has failed to download code because the code is incompatible with the handset hardware. Contact your system administrator should this icon appear.
MUTED	The muted icon indicates the current call is locally muted.
XXXX	During character entry, Indicates current data entry symbol mode.

Call status icons

Indicator	Function

Indicator	Function
☎	On-hook icon, Solid when in standby mode to indicate that at least one call is on hold. Flashing when incoming call is ringing.
☎	Off-hook icon. Solid when a call is being dialed.
☎	Hold icon. Call is on hold
✕	Transfer icon. Call is in the process of being transferred
⇆	Audio flowing icon. Audio is flowing both ways on a call.
=	No audio icon. No audio is flowing. Call is terminating or far end hold with audio disable.

NavOK functions

The **NavOK** key acts as a fifth softkey with implicit functionality as follows:

State	NavOK key function
Dialing	Place phone call.
Answering	Answer a second phone call (same or different line)
Holding	Resume audio.
Displaying menu	Select the highlighted menu option.
Displaying call status	Resume audio on the currently selected call and place previous call on hold. If the selected call is ringing, the call will be answered.
Entering login name or login password	Save name or password and proceed with startup.

Softkeys

Softkey	Name	Displayed during…	Press to…
<<	Cursor backward	Entering a dial number.	Move the cursor back one position.
>>	Cursor forward	Entering a dial number.	Move the cursor forward in alphanumeric mode, if the cursor is at the end of the line, adds a space character.
Answ	Answer	Incoming call on the selected line.	Answer the call (equivalent to **START** key).
Bksp	Backspace character	Entering a dial number.	Delete the character prior to the cursor position.
Back	Back one screen	Displaying a menu.	Exit the menu.
End	End Call	An active call on the selected line.	Terminate the call without going back to standby mode.
Favr	Favorites	Prior to entering the first character of a dial number when off hook.	Activate the Favorites menu.

Softkey	Name	Displayed during…	Press to…
Logs	Call Logs	Standby mode	Open the Call Log menu.
Hold	Hold	In an active call.	Place the call on hold. The line status shows when the call is on hold or when audio is flowing.
Msg	Message	Initial dial screen when new line is selected and a dial tone is active prior to entering first character of the number to be dialed[4].	Initiate a call to the specified message center contact address for retrieval or administration of voicemail.
Mute	Toggle muting	In an active call.	Toggle audio transmission to the far end. The line status shows when not muted or when muted.
OK	OK	Power up registration if username is not configured in **Admin** menu.	Send the username and password to the SIP server for authorization to register the handset.
Redl	Redial	Prior to entering the first character of a dial number.	Redial the last number that was dialed.
Rej	Reject	Incoming call on the selected line.	Reject the incoming call. The SIP server will then redirect the call elsewhere.
Resm	Resume	In an active call and you have placed the call on hold or in standby mode if any call is on hold.	Resume a call that was previously placed on hold or that went on hold when another line was activated.
Save	Save	Entering a dial number as a forward destination.	Save the dial number as the forwarding destination for the selected line.
Symb	Symbols	Entering a username or password. Entering the digits of a number.	Select the set of symbols available on the keypad while entering data.

[4] Appears only if MSGNUM is configured. A message center contact address must be defined for the proxy used by the selected line.

Menus

Line menu

You can activate a call using the Line menu on a selected line or view the status of lines.

Pressing the **LINE** key from the active mode displays a menu of line appearances as programmed in the HTTP/TFTP configuration file. The **LINE** key can be pressed while the handset is in the standby mode to activate the handset and to activate a new call on the selected line.

The currently selected line is indicated by an asterisk (*****). Lines for which the corresponding proxy server has outstanding new mail are flagged with plus (**+**) characters. The proxy server IP address is displayed on the info line. Lines that should be registered to a proxy but have failed registration for any reason are displayed in faded text and are not selectable from the menu.

Exit the **LINE** display by pressing a line number key to start a new call on the selected line and put any other call on hold, or by pressing the **END** key to exit without starting a new call. Press the **More** softkey to page through additional items on the Line menu.

Symbol menu

The symbol menu allows you to change the set of characters available for data entry through multiple key presses of the dial pad keys.

While dialing a number or entering login information, press the **Symb** softkey to view a menu of possible sets of characters that can be entered using multiple key presses of the dial pad keys. Normally, a simple numeric mode is selected; selecting other symbol modes allows convenient access to the complete printable US ASCII character set. The following table shows what characters are available through repeated key presses in various symbol modes.

Key	Numeric	Alpha-Numeric	Numeric-Alpha	Punctuation
1	1	1 ; : / \ ! ‘	1	@ : 1
2	2	a b c 2 A B C	2 A B C a b c	; , 2
3	3	d e f 3 D E F	3 D E F d e f	& | ` ~ 3
4	4	g h I 4 G H I	4 G H I g h i	( ) 4
5	5	j k l 5 J K L	5 J K L j k l	< > 5
6	6	m n o 6 M N O	6 M N O m n o	{ } 6
7	7	p q r s 7 P Q R S	7 P Q R S p q r s	[ ] 7
8	8	t u v 8 T U V	8 T U V t u v	‘ “ \ 8
9	9	w x y z 9 W X Y Z	9 W X Y Z w x y z	^ _ 9
0	0	@ - _ 0 = , < >	0 - _	[space] 0
*	.*.	. $ * & % + ( )	* .	* . = + / -
#	# @	[space] , ( ) |	# [space]	# ! ? $ %

Favorites menu

While dialing, you can use the favorites menu that provides access to a predefined list of dial numbers. The predefined list can include either complete dial numbers for named parties or partial numbers that need additional data entry. For example, if a PBX feature access code for call forwarding is defined in the favorites list but you need to add the forwarding destination information before sending the call to the PBX to activate the feature.

While in a dialing state, press the **Favr** softkey to display a menu of pre-defined numbers or names that can be dialed (as programmed in the Remote configuration file.) When an item is selected from the list, the screen displays the dial number. You may edit or add digits to the displayed number if necessary before pressing the **NavOK** key or **START** to place the call.

FCN menu

The FCN menu is accessible while in the active mode and provides these features:

Transfer

Do Not Disturb

Set/Clear Forward

<OAI>

<OAI>

<OAI>

Items on the FCN menu are accessible through navigation and selection keys or through short-cut keys as displayed with the menu items. OAI functions are automatically added as items at the end of this menu when defined on an OAI server.

Notes on battery packs

- Avaya offers the following battery types with increasing capacity: Standard, Extended and Ultra-Extended.
- ***Battery pack life will vary depending on handset model and features and system infrastructure.***
- Batteries are shipped with a partial charge. You must fully charge the batteries before using them in phone operation.
- Maximum battery pack performance is achieved after a few charge/discharge cycles.
- If multiple battery packs are supplied with your handset, you must charge each battery fully upon receipt to prolong battery life. battery packs will slowly lose charge if unused. To maintain battery potential, charge unused battery packs occasionally or alternate battery pack use.

- After a length of time battery packs will lose the ability to maintain a charge and to perform at maximum capacity and will need to be replaced. This behavior is normal for all batteries.
- You must charge the battery overnight while the handset is turned off.
- If the handset does not charge, clean battery pack, charger and handset contacts with an alcohol swab.
- When the handset is properly seated, the backlight comes on briefly to indicate charging has begun.
- Any battery which exhibits swelling, cracking or other abnormality should be disposed of promptly and properly.

User-defined preferences

The Avaya 3641/3645/6120/6140 IP Wireless Handset features a configuration menu ("Config menu") that is available to the user to configure user preferences and display handset information. The Config menu is opened by pressing the **Cfg** softkey from standby mode. See the *Avaya 3641/3645/6120/6140 IP Wireless Handset and Accessories User Guide*.

Config Menu

Config menu	2nd level	3rd level	4th level	5th level	6th level
Lock Keys					
User Profiles	Silent Vibrate Loud Soft Custom				
		Set as Active			
		Ring Settings	Telephone Ring Message Alert 1 Message Alert 2		
				Ring Cadence	Off PBX Continuous Short Pulse Long Pulse
				Ring Tone	Tones 1-10
				Ring Volume	Volume ■■■■■■■
				Vibrate Cadence	Off PBX Continuous Short Pulse Long Pulse
				Ring Delay	No Delay 5 Second Delay 10 Second Delay

Config menu	2nd level	3rd level	4th level	5th level	6th level
		Noise Mode[5]	Normal High Severe		
		Ring in Headset Ring in Speaker			
		Warnings Disable/Enable			
		Key Tones Disable/Enable			
		PTT Disable/Enable			
Phone Settings	Keypad Autolock	Disable 5 Seconds 10 Seconds 20 Seconds			
	Language	*English Français Deutsch Español Italiano			
	Display Contrast	Set Contrast			
	Use Hearing Aid Use No Hearing Aid				
	Play Startup Song Inhibit Song				
	Predial Disable/Enable				
	SNMP Settings†				

[5] High and Severe noise modes increase microphone, speaker, and ring volume settings above Normal mode baseline. All measures are approximate.

	Microphone	In-ear speaker	Ring volume
High	+12dB	+6dB	+3dB
Severe	+18dB	+12dB	+6dB

Config menu	2nd level	3rd level	4th level	5th level	6th level
Push-to-talk *	Default Channel	Channel 1 …. Channel 24			
	Subscribed Channels	Channel 1 Channel 2 Channel 3 …. Channel 24			
	PTT Audio Volume	Audio Volume ■■■■■■■			
	PTT Tone Volume	Tone Volume ■■■■■■■			
	PTT Vibrate Disable/Enable				
System Info	Phone IP Address				
	Alias IP Address				
	SVP IP Address				
	OAI IP Address				
	Software Version				
	Emergency Dial *	Emergency Number Emergency Name			

* **Push-to-talk** and **Emergency Dial** only appear if enabled.

† The SNMP option is designed for system administrator use when troubleshooting.

If the administrator selects SNMP there is a 3rd level menu which is a prompt to enter the admin password if the admin password is enabled. This is the same as the password in the Admin menu. The default password is 27238 (“CRAFT”). If the admin password is disabled the password entry menu is skipped. Upon successful entry of the admin password (or if the password is disabled) there is a 4th level menu selection that allows entry of the SNMP IP address or SNMP Community string.

You can also configure the SNMP parameters remotely through Avaya Aura® System Manager.

See Chapter 10: *Diagnostic Tools* for more information.

Default global settings

Options on the **Config** menu may be reset to their default values by the **Restore Defaults** option in the **Admin** menu. These are the default global settings that affect every Profile:

Menu option	Default
Language	English
Lock Keys	Unlocked
Display Contrast	Medium
Use Hearing Aid	Disabled
Play Startup Song	Enabled
Predial	Enabled

Default Profile settings

The profile options on the standby menu may be reset to their default values by the **Restore Defaults** option in the **Admin** menu. These are the default settings:

Setting/profile	Silent	Vibrate	Soft	Loud	Custom
Headset/Speaker	Speaker	Speaker	Speaker	Speaker	Speaker
Key Tones	Off	Off	On	On	On
Warning Tones	Off	Off	Off	Off	Off
Push-to-talk	Off	Off	On	On	On
PTT Vibrate	Disabled	Disabled	Disabled	Disabled	Disabled
Emergency Dial	On	On	On	On	On
Ring Cadence	Off	Off	PBX	PBX	PBX
Ring Tone	Tone 1	Tone 1	Tone 1	Tone 1	Tone 1
Ring Volume	1	1	3	7	5
Vibrate Cadence	Off	PBX	Off	Off	PBX
Ring Delay	0	0	0	0	5
Noise Mode	Normal	Normal	Normal	Normal	Normal

Push-to-talk must be enabled by the system administrator before it can be activated by the user. If it is not enabled, then it will not appear on the Config menu and will not be “On” for any profile.

PTT Vibrate is available only when Push-to-talk has been enabled by the system administrator.

The system administrator must enable the Emergency Dial. If enabled, it will be “On” and available for use in every profile.

Chapter Ten: Diagnostic tools

Three diagnostic tools, **Run Site Survey**, **Diagnostics Enabled** and **Syslog Mode** are provided to assist the LAN administrator in evaluating the functioning of the Avaya 3641/3645/6120/6140 IP Wireless Handset and the system surrounding it. Diagnostic Tools are enabled from the **Admin** menu.

The **Halt on Error** option in the Admin menu is a diagnostic tool that will cause the handset to stop operating if an error message is received. Error details may be shown on the display, captured by the syslog server, and may also be available for downloading with the Handset Administration Tool. Unless the error is a fatal one, normal operation may be resumed by restarting the handset.

Run Site Survey

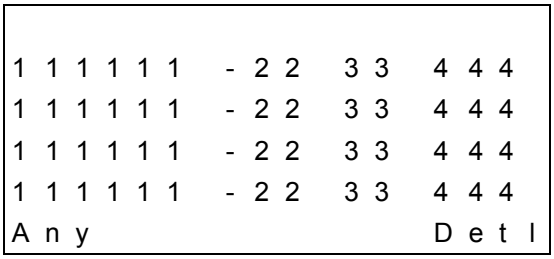
Site survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs regardless of SSID. The information available 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

Start the site survey by selecting **Run Site Survey** from the **Admin** menu. The mode starts immediately.

When the test is started, it is by default in “single SSID” mode. When the **Any** soft key is pressed (softkey A) all APs, regardless of SSID, are displayed and the softkey changes to say **MyID**. Pressing the **MyID** soft key will revert to the “single SSID” mode and change the softkey back to **Any**.

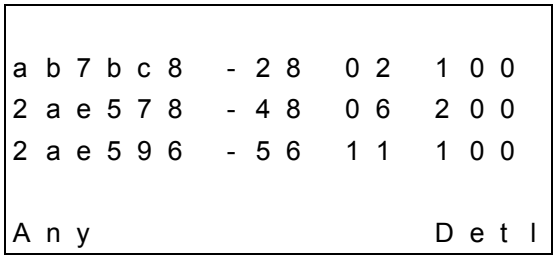
The display would look like the following for the single AP mode.



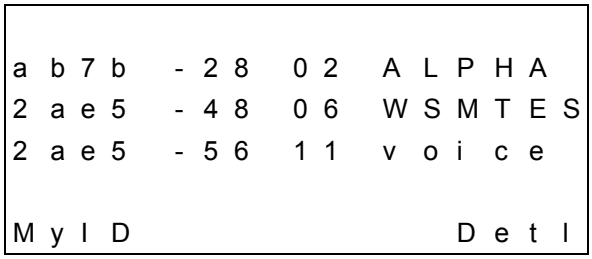
Where:

- 111111 – the last three octets of the on-air MAC address for a discovered AP.
- 22 – the signal strength for the specified AP.
- 33 – the channel number of the specified AP.
- 444 – the beacon interval configured on the specified AP.
- Any/MyID – softkey to toggle between “single SSID” and “any SSID” mode.
- Detl/Smry – softkey to toggle between the multiple AP (summary) display, and the single (detail) displays for each AP.

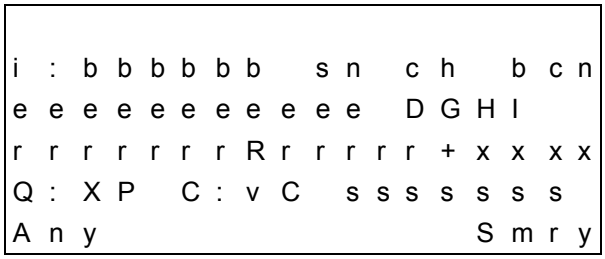
The following screen shows how the display would look when there are three APs configured with an SSID that matches that of the handset. The first has a signal strength of –28 dBm, is configured on channel 2, with a beacon interval of 100 ms. The second has a signal strength of –48 dBm, is configured on channel 6, with a beacon interval of 200 ms. The third has a signal strength of –56 dBm, is configured on channel 11 with a beacon interval of 100 ms.



When the **Any** SSID mode is selected, the summary display contains the first six characters of the APs SSID instead of the beacon interval as in the example below.



In **Detl** (detail) mode the display would appear as follows. The left/right arrow keys will move between AP indices.



Where:

- i – index of selected AP (value will be from 0 to 3 inclusive)
- bbbbbb – the last three octets of the BSSID for a discovered AP

- sn – signal strength in –dBm
- ch – channel
- bcn – beacon interval
- eeeeeeeeeee – SSID (up to first 11 characters)
- DGHI – standards supported i.e. 802.11d, 802.11g, etc. in addition to 802.11a and 802.11b.
- rrrrrrrr – rates supported. Basic rates will have a “b” following the rate
- + – more rates are supported than those displayed
- xxxx – WMM or UPSD if those QoS methods are supported
- Q:XP
- X is a hexadecimal representation of the access categories configured with admission control mandatory (ACM). Bit3 = voice, Bit2 = video, Bit1 = background, Bit0 = best effort. For example, if an AP advertises voice and video as ACM then X=c. If all the ACs are set as ACM then X=f. If AP does not have WMM support, this character space will be blank.
- P is displayed when the AP advertises WMM-PS. If the AP does not advertise WMM-PS then this character space will be blank.
- C:vC
- v is a decimal number indicating the CCX version advertised by the AP.
- C is displayed when AP advertises CCKM. If the AP does not advertise CCKM then this character space will be blank.
- ssssssss – Security modes: “None”, “WEP”, “WPA-PSK”, “WPA2-PSK”, “WPA2-Ent”
- Any/MyID – softkey to toggle between “single SSID” and “any SSID” modes
- Detl/Smry – softkey to toggle between the multiple AP display (summary), and the single AP display (detail)

Numbers racing across the handset display indicate AP information is being obtained. A **Waiting** message indicates the system is not configured properly and the handset cannot find any APs.

Solving coverage issues

Coverage issues are best resolved by adding and/or relocating APs.

Overlap issues may be resolved by reassigning channels to the APs or by relocating them. See Chapter 12: *Troubleshooting*, section *Access Point Problems* for more information.

Diagnostics enabled

Diagnostics is used to evaluate the overall quality of the link between the handset, AP, and infrastructure side equipment, such as IP PBX, Avaya SVP Server, and gateways. Unlike **Site Survey**, **Diagnostics** is used while the functional code is running, and during a call.

When you enable **Diagnostics** in the **Admin** menu, the handset can display diagnostic screens when it is in active mode. However, navigation among calls cannot be done as the **Nav** keys are used to display diagnostic screens.

You can initiate the display of information when in a call, by pressing the **Nav**◄ or **Nav**► key. Only one of the six diagnostic screens listed below can be shown at a time. Pressing the **Nav** keys multiple times will cycle through the various diagnostics screens and the normal off-hook (IP-PBX) display. The numeric icon at the top of the display indicates the screen number is being displayed.

For example: The first time you press the **Nav** key, the icon for **1** is shown, and the first of six diagnostics screens are displayed. The next time it you press the Nav key, the icon for **2** is displayed and the next of six diagnostics screens are displayed. The counters will be cycled through in this fashion until there are no more counters to be displayed. After all the diagnostics screens have been displayed, the screen returns to the normal off-hook IP-PBX screen.

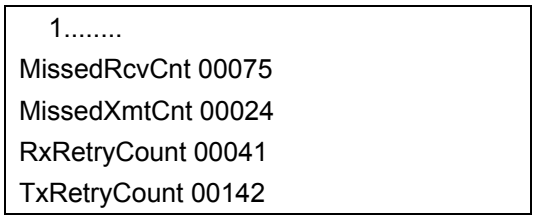
The text portion of each debug display is read from the language translation file, and therefore may be translated to the language the phone would otherwise use. The examples in this document reflect the debug displays as shown in English.

The debug displays refresh once per second, although the information displayed may take longer to update.

Unless otherwise noted, all numbers are displayed as 16-bit unsigned integers, which will wrap from 65535 to 0.

The information provided by **Diagnostics** includes:

Diagnostic display #1:



- MissedRcvCnt: The number of 10 ms audio frames for which audio was not present when the phone tried to play it. The phone therefore used its ClearTalk algorithm to fill in the missing audio. Note this is NOT the same as the missed audio payloads reported in the Syslog audio statistics messages.

- MissedXmtCnt: The number of transmit packets dropped for not receiving an ACK from the AP after all retries are exhausted.
- RxRetryCount: The number of packets received with the retry bit set.
- TxRetryCount: The number of packets transmitted or attempted that required at least one retry.

Diagnostic display #2

```
   .2.......
Jitter      07500
LastRate    00054
GatewyType  NoA2
TxPower(dBm) 00015
```

- Jitter: Audio jitter in microseconds (us.) This is calculated in the same way as the jitter reported in the audio statistics Syslog message.
- LastRate: The highest transmit date rate in megabits per second (Mbps) at which the phone has successfully transmitted a packet and received an ACK in the last second.
- GatewyType: The gateway type (if any) that the phone is checked in to. This will be one of the following:
    - 2Mb: SVP server operating at 2 Mbps max speed.
    - 11Mb: SVP server operating at 11 Mbps max speed.
    - NoA2: No gateway in use (used with Wifi Qos.)
- TxPower(dBm): Current transmit power in dBm. A table of dBm values and the associated power in milliwatts is shown below:

dbM	mW
7	5
10	10
13	20
15	30
16	40
17	50
20	100

Diagnostic display #3:

```
   ..3......
9970 060 -67 c011
7020 064 -71 Weak
a340 116 -72 Weak
```

```
b2e0 153 -72 Rate
```

The third debug display shows the status and signal strength of the current AP and up to three other candidate APs. The first line shows the current AP, and the next three lines show up to three candidates, if there are that many. If there are fewer than three candidates, extra lines will be blank.

Each line has four fields:

1: Last 4 (hexadecimal) digits of the AP's MAC address.

2: The channel being used by that AP.

3: The signal strength of that AP.

4: For the current AP, the Association Identifier (AID) with the highest two bits set. To extract the actual AID, subtract 0xc000.

For the candidates,a reason code telling why the current AP was a better candidate.

The reason codes are as follows: The numbers in brackets are the associated handoff codes)

- Unkn: Unknown
- Weak: The AP's signal strength was weaker than the current AP, or not enough stronger to justify roaming. {0, 1, 2, 6, 12, 13}
- Rate: The data rates required by the AP were not supported by the phone. {5}
- Full: The AP was already handling as much voice traffic as it could support, and had no additional bandwidth for this call. {7}
- AthT: Authorization timeout. {8}
- AscT: Association timeout. {9}
- AthF: Authorization failed. {10}
- AscF: Association failed. {11}
- SecT: Security timeout. {29, 30, 31, 32, 33, 34, 35}
- SecF: Security failed. {37, 39}
- Cnfg: Configuration failure. (19, 38, 41, 45}
- CCX: AP does not support CCX (52}
- CCKM: AP does not support CCKM {53}
- WMM: APp does not support WMM {54}

Diagnostic display #4:

```
   ...4.....
AssocCount   00002
ReAssocCount 00000
```

```
Assocfailure 00000
Assocfailure 00000
```

- AssocCount: The number of times the phone has associated since starting the functional code. This number will always be at least one (the initial association) and higher numbers reflect hard handoffs (where the phone completely lost the AP. Note that hard handoffs in standby are normal, only hard handoffs while in call reflect problems.
- ReAssocCount: The number of times the phone has re-associated since starting the functional code. This is equivalent to the number of soft handoffs.
- AssocFailure: The number of times the phone has failed to associate, defined as the number of times the phone attempts to associate minus the number of times it has successfully associated.
- ReassocFail: The count of re-association failures, again this is tries minus successes.

Diagnostic display #5:

```
    ....5....
Sec-ErrCount 00000
LstSeqErrSeq 00000
QosFailCnt   00000
```

- Sec-ErrCount: The number of radio packets that have failed to decrypt properly.
- LstSeqErrSeq: The 802.11 sequence number of the last radio packet (if any) that failed to decrypt properly.
- QosFailCnt: The number of times the QOS admission control negotiation (TSPECS) has failed.

Diagnostic display #6:

```
    .....6...
EapErrCnt    00000
LstEapErCode 00000
```

- EapErrCnt: The number of EAP (Extensible Authentication Protocol) errors which have happened since the phone was powered up.
- If the EapErrCnt is non-zero, the second line will show a reason code for the last EAP error. These error codes are:
    - 0: No EAP error.
    - 1: Unknown EAP error.

- 2: EAP type mismatch.
- 3000: Invalid certificate presented by EAP-AS.
- 4000: General TLS alert.
- 5000: Credentials produced by client are invalid.

Syslog mode

A syslog server must be present on the network in order for the handset to send the log messages and save the messages. The syslog server will be found with DHCP option 7 if the handset is using DHCP. If static addresses are configured, the syslog server's IP address can be configured statically in the **Admin** menu. Alternatively, you may set LOGSRVR in SSON or the 46xxsettings.txt file.

Note:
If the syslog server address is blank (**000.000.000.000** or **255.255.255.255**) or the handset is using DHCP and no option 7 is received from the DHCP server, the handset will not send any syslog messages.

Admin menu options:

- ***Disabled** – turns syslog off.
- **Errors** – causes the handset to log only events that we consider to be an error (see below).
- **Events** – logs all errors plus some other interesting events (see below).
- **Full** – logs all the above plus a running stream of other quality information (see below).

Messages are formatted like the following example:

```
JAN 21 12:51:26 172.29.76.67:11133>Jan 21 19:50:46.00 0090.7a05.18f6
(172.029.076.067) [0000] Successful Handoff to 0013.5f59.9970 (-68 dBm)
from 0000.0000.0000 (-0 dBm), Reason 24, other APs:0013.5f59.9970 (-68
dBm) 0, TxPO:15 dBm, TxPN:15 dBm
```

The message may be divided into three parts, a header added by the logger program, a header added by the handset, and the message itself.

The header added by the logger program is the first part of the message.

```
<JAN 21 12:51:26 172.29.76.67:11133>
```

The information in this header includes the date and time from the logging computer's internal clock, as well as the IP address of the device sending the message. The additional information from p-Logger (11133) is the UDP source port number from the handset.

The handset header in above example is:

```
Jan 21 19:50:46.00 0090.7a05.18f6 (172.029.076.067) [0000]
```

The handset header contains the date and time, but this time from the handset's clock, followed by the Phone's MAC (Media Access Control) address, the phone's IP address in parentheses, and a message number in brackets.

If the handset is not configured to use the SNTP (Simple Network Time Protocol) to determine the correct date and time, it will set its clock to midnight, January 1, 2001 on power up.

The message number starts at 0 on power up, and increments for every Syslog message sent. Note that the message number is in hexadecimal.

The remainder of the Syslog message is the message itself, and can be any text, and often includes data as well as the text.

Syslog Messages

The table below lists the Syslog messages and which level of logging will produce them:

Message type	Errors	Events	Full
SW ERROR	Yes	Yes	Yes
CHARGER-Placed in charger	No	Yes	Yes
CHARGER-Removed from charger	No	Yes	Yes
CHARGER-Vbat: 4187mV	No	Yes	Yes
CHARGER-Charge complete	No	Yes	Yes
Handoff report	No	Yes	Yes
Failed Handoff	Yes	Yes	Yes
In-Call Syslog Messages			
Call Start	No	Yes	Yes
Call End	No	Yes	Yes
AStat	No	Yes	Yes
AThresh	Yes	Yes	Yes
NStat	No	Yes	Yes
NThresh	Yes	Yes	Yes
Rare Syslog Messages			
CHARGER Battery temp out of range	No	Yes	Yes
CHARGER Battery temp out of range in unit	No	Yes	Yes
Download aborted, code incompatible	Yes	Yes	Yes
DCA initiated radio reset	No	Yes	Yes
LockUpRecovery	Yes	Yes	Yes
Probe Recovery	No	Yes	Yes
DCA unknown MgmtAction	Yes	Yes	Yes
txMissedIrptPatchCnt	No	Yes	Yes
SIP Specific Syslog Messages			
Number of methods in header exceed maximum size	Yes	Yes	Yes
SIP <method> request received from <ipaddr>	No	Yes	Yes
SIP <method> request sent to <ipaddr>	No	Yes	Yes

Message type	Errors	Events	Full
SIP <code> response received from <ipaddr>	No	Yes	Yes
SIP <code> response sent to <ipaddr>	No	Yes	Yes
Call established to <ipaddr>	No	Yes	Yes
Call terminated to <ipaddr>	No	Yes	Yes
Invalid SIP <method> request received from <ipaddr>, rc <code>	Yes	Yes	Yes
Invalid SIP <code> response received from <ipaddr>, rc <code>	Yes	Yes	Yes
Invalid value for <parm> in SSON data	Yes	Yes	Yes
Invalid value for <parm> in generic config file	Yes	Yes	Yes
Invalid value for <parm> in specific config file	Yes	Yes	Yes
Value too long for <parm> in SSON data	Yes	Yes	Yes
Value too long for <parm> in generic config file	Yes	Yes	Yes
Value too long for <parm> in specific config file	Yes	Yes	Yes
Download aborted code incompatible. Error=####	Yes	Yes	Yes
DCA unknown MgmtAction category code=###	Yes	Yes	Yes
CHARGER-Battery temp out of range	Yes	Yes	Yes

SNMP

An SNMP remote application may issue SNMP Get commands to the handset. The handset supports only Get commands..SNMP Set and Trap commands are not supported. An SNMP address and community string must be configured on the handset for SNMP commands to be processed.

- SNMP IP address – The handset responds only to SNMP Get commands originating from devices with this IP address Multiple comma separated IP addresses may be entered in the DHCP SSON option or 46xxsettings.txt file. A single IP address may be entered from the User Menus. If an IP address isentered from the User Menus, any previously configured IP addresses are erased.
- SNMP Community String – The handset will respond only to SNMP Get commands if the community string set on the handset matches the community string in the Get command. Ensure the community string is set to the same value on the handset and the remote SNMP application. The string can be 1-32 characters.

Remotely Configuring SNMP

You can configure both the SNMP IP address and community string remotely through Avaya Aura® System Manager. For more information, see *Device Settings Groups* in the *Administering Avaya Aura® Session Manager* (03-603324) documentation, available on the Avaya Web site www.avaya.com/support.

Note:

If the source IP address of the SNMP Get command does not match one of the SNMP addresses configured in the handset, or the SNMP community string in the SNMP Get command does not match the community string in the handset, the handset will not respond to the SNMP command.

The handset supports portions of the standard RFC1213 and IEEE802.11 MIBs and the proprietary AVAYA-364x MIB. The supported MIBs are included with the handset software package. For information on specific MIB parameters refer to the descriptions in the MIBs.

Chapter Eleven: Software maintenance

The Avaya 3641/3645/6120/6140 IP Wireless Handsets use proprietary software programs specified and maintained by Avaya. The software versions that are running on the handsets can be displayed during power on by holding down the **END** button. **Software Version** is also an option on the Config menu.

Avaya Customer Service or an authorized dealer will provide information about software updates and how to obtain the software (for example, downloading from a website).

After software updates are obtained, they must be transferred to the appropriate HTTP/TFTP server located on the LAN to update the code used by the wireless handset.

The handset allows over-the-air transfer of software updates from the designated server to the handsets. The download function in the wireless handset checks its software version every time you power on the handset, when the designated server is active. If there is a different version available, the handset immediately begins to download the update.

Upgrading handsets

After you obtain the software updates, you must transfer the updates to the appropriate location in the LAN to update the code used by the handsets. In case of supplying a list of HTTP server addresses via SSON or config files, ensure that you transfer the update to all servers to avoid inadvertently downgrading code in case of a server outage.

Avaya 3641/3645/6120/6140 IP Wireless Handsets allow over-the-air transfer of software updates from the designated TFTP or HTTP server to the handsets. The downloader function in the handset checks its software version every time the handset is turned on. If there is any discrepancy the handset immediately begins to download the update.

Normal download messages

When the handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions, and downloading. The normal message progression is:

Message	Description
Checking Code	The handset is contacting the HTTP/TFTP server to determine if it has a newer version of software that should be downloaded.
Erasing Memory	The handset has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.

Message	Description
Updating Code	The handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.

When the update is complete, the handset displays the extension number, and is ready for use.

Remotely rebooting handsets

You can configure both the SNMP IP address and community string remotely through Avaya Aura® System Manager. For more information, see *Rebooting of selected AST devices* in the Administering Avaya Aura® Session Manager (03-603324) documentation, available on the Avaya Web site www.avaya.com/support.

Note:

The Avaya 3641/3645/6120/6140 IP Wireless Handsets for SIP are not Avaya AST devices. The Avaya 641/3645 IP Wireless Handsets for SIP support only those functionalities that are mentioned in this Administrator Guide.

Download failure or recovery messages

The following display messages indicate a failure or recovery situation during the download process.

Message	Description
Server Busy	The handset is attempting to download from a HTTP/TFTP server that is busy downloading to other phones and refusing additional downloads. The handset will automatically retry the download every few seconds.
TFTP ERROR(x):yy	A failure has occurred during the HTTP/TFTP download of one of the files. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = HTTP/TFTP server did not find the requested file. 02 = Access violation (reported from HTTP/TFTP server). 07 = HTTP/TFTP server reported "No such user" error. Check the HTTP/TFTP server configuration. 16 = No HTTP/TFTP server address. Check the HTTP/TFTP server configuration. 81 = File put into memory did not CRC. The handset will attempt to download the file again. FF = Timeout error. HTTP/TFTP server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the handset. This operation will retry.
Waiting	The handset has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again.

Chapter Twelve: Troubleshooting

In certain scenarios, transmission problems may occur due to any number of factors originating from the wireless LAN. Avaya 3641/3645/6120/6140 IP Wireless Handsets can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting handsets, consider the following problem sources to determine the best method of approaching any specific situation.

Access point problems

Handset audio problems are related to AP range, positioning, and capacity. Performing a site survey as described in this document can isolate the AP causing these types of problems. 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 wireless LAN APs. Service is restored if the user moves back within range. If a call drops because a user moves out-of-range, the handset will recover the call if the user moves back into range within a few seconds.

Capacity

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

Transmission obstructions

Prior to system installation, the best location for APs for optimum transmission coverage should have been determined. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after system installation. This loss of service can be restored by moving out of the obstructed area or by adding/rearranging APs.

Handset status messages

Avaya 3641/3645/6120/6140 IP Wireless Handset status messages provide information about the Avaya 3641/3645/6120/6140 IP Wireless Handset's communication with the AP and host telephone system. The following table summarizes, in alphabetical order, the status messages.

Message	Description	Action
	Download failure icon	Update handset code in the HTTP/TFTP server and power cycle the handset.
3 chirps (audio)	Handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning, the call will hand off to the best AP once it becomes available.
802.1X Failure Xxxxxxxxxxxx XXX	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect because the user credentials are restricted based on the user account properties. In the case of EAP-FAST, the PAC ID may not match the username. The second line of the error message contains the twelve digits of the AP MAC address and three digits that indicate the error code as defined in RFC2759.	Verify and resolve if the user account has any restrictions such as password expired, account restricted/ disabled, or in case of EAP-FAST, the handset PAC and username matching the authentication server.
Address Mismatch	Handset software download files are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.
Assoc Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset association was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive association response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Auth Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset authentication was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.

Message	Description	Action
Auth Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive authentication response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per *VIEW Configuration Guide*. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software license types. Handset software does not match current handset license selection.	Download new software from the Avaya website per *Software Maintenance*.
Bad Config	Some needed configuration parameter has not been set.	Check all required handset configuration parameters for valid settings.
Bad SSID	The handset has not had an SSID entered.	Statically configure an SSID in the **Admin** menu.
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.
Bad SIP TFTP IP	A bad unicast address has been entered for the HTTP/TFTP server in static entry mode.	Re-enter the correct IP address in the administrative menus for static IP addresses.
(battery icon), Battery Low, beep (audio)	Low battery.	In call: the battery icon displays and a soft beep will be heard when the user is on the handset and the battery charge is low. User has 15–30 minutes of battery life left. Not in call: The battery icon displays whenever the battery charge is low The message Battery Low and a beep indicate a critically low battery charge when user is not on the handset. The handset will not work until the battery pack is charged.
Battery Failure	The battery pack is not functioning.	Replace the battery pack with a new or confirmed SpectraLink battery pack. Only SpectraLink battery packs will work.
Battery Failed	Battery pack is damaged or incompatible with handset.	Replace the battery pack with a new or confirmed SpectraLink battery pack. Only SpectraLink battery packs will work.
Can't Renew DHCP yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server is not responding to initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.

Message	Description	Action
Cert Expired	When WPA2-Enterprise with PEAP authentication is selected, the handset failed to connect due to an expired certificate on the handset or authentication server.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at “valid to” field from “validity” data in certificates. If any of the certificates have expired replace them with new certificates.
Cert Invalid	When WPA2-Enterprise with PEAP authentication is selected, the Wireless Telephone failed to connect to the network because the certificate start date is in the future.	Verify that the NTP server is properly configured with the correct time. Verify that the certificates loaded on the handset and authentication server have valid start/end dates by looking at “valid from” field from “validity” data in certificates. If any of the certificates have expired replace them with new certificates.
Charging …	The handset is charging in the desktop charger.	No action needed.
Charge Complete	The handset is now fully charged.	No action needed.
Charger Error	The handset has detected a problem with the charging circuitry.	Allow the charger and battery to cool. If the problem persists, try a new or confirmed battery. If the problem still persists, contact technical support and report the error.
Checking Code	Handset is contacting the HTTP/TFTP server to determine if it has a newer version of software that should be downloaded.	None, this message should only last for approximately one second. If message remains displayed, power off and contact customer support for a replacement phone.
Checking DHCP IP	The handset is retrieving DHCP information from the DHCP server.	None. This is informational only.
CRC Code Error	The software which has been HTTP/TFTP downloaded has a bad redundancy code check.	Try the download again; it is possible the software was corrupted during download. If the error repeats, check that the download image on the HTTP/TFTP server is not corrupted.
Code Mismatch!	The software loaded into the handset is incorrect for this model handset.	Verify the License Management value is correct. Replace the software image on the HTTP/TFTP server with software that is correct for the handset model.

Message	Description	Action
Config reboot	Appears when the handset reboots after the remote configuration if a parameter changed that requires the handset to reboot (for instance, it the ESSID or the Security method is changed, the handset has to reboot to start using the new values). This message appears for a few seconds while the handset is rebooting	Informative only. No action required.
DCA Timeout	The handset has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, then on again. If error persists, contact Avaya Technical Support and report the error.
DHCP Error (1-5)	DHCP Error 1.	The handset cannot locate a DHCP server. It will try every four seconds until a server is located.
	DHCP Error 2.	The handset has not received a response from the server for a request for an IP address. It will retry until a server is found.
	DHCP Error 3.	The server refuses to lease the handset an IP address. It will keep trying.
	DHCP Error 4.	The server offered the handset a lease that is too short. The minimum lease time is 10 minutes but Avaya Engineers recommend at least one-hour minimum lease time. The handset will stop trying. Reconfigure the server and power cycle the handset.
	DHCP Error 5.	Failure during WEP Key rotation process (proprietary feature).
DHCP Lease Exp yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP is not responding to renewal attempts (at least one renewal succeeded).	The handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The handset will attempt to negotiate a new lease, which will either work, or it will change to one of the above DHCP errors (1 through 4).
DHCP NACK error yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server explicitly refused renewal.	The DHCP lease currently in use by the handset is no longer valid, which forces the handset to restart. This problem should resolve itself after the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	Handset software download files are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.

Message	Description	Action
DO NOT POWER OFF	The handset is in a critical section of the software update.	None. Do not remove the battery pack or attempt to power off the phone while this message is displayed. Doing so may render the handset inoperable.
Duplicate IP	The handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the handset.	Operation will retry but may eventually report the error "int. error: 0F" Power cycle the handset.
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory.	None. When the progress bar fills the display line the erase operation is complete. Do not turn the handset off during this operation.
Files Too Big	Handset software download files are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via Admin menu (or re-program with Configuration Cradle).
Initializing …	The handset is performing power-on initialization.	None. This is informational only.
Initializing SIP	The handset is performing a power-on initialization of the SIP application. The phone is initializing its data structures and attempting to access the SIP HTTP/TFTP server and download the SIP configuration files.	None. This is informational only.
Internal Err. # #	The handset has detected a fault from which it cannot recover.	Record the error code so it can be reported. Turn the handset off then on again. If error persists, try registering a different handset to this telephone port. If error still persists, contact Avaya Technical Support and report the error.
Invalid Usr/Pwd	When WPA2-Enterprise or Cisco FSR is selected, the handset failed to connect due to incorrect device credentials or unavailability of authentication server. If the error is because of the incorrect device credentials then the username or password doesn't match with those configured on the authentication server.	Verify that the required credentials {username, password} are created on the authentication server and should match the handset. This may also happen when the authentication server is not reachable while doing the EAP authentication. Make sure the authentication server is active and reachable from the WLAN access points/controller at all times.

Message	Description	Action
Multiple GW Res	More than one Avaya SVP Server has responded.	Caused by two or more handsets sharing the same IP address. Assign unique IP addresses to each handset.
Multiple SVP Reg yyy.yyy.yyy.yyy	y…y = SVP IP address Handset received responses from multiple SVP Servers; displays IP address of one responding SVP Server.	This can happen if the handset has been reconfigured to use a different SVP server and then powered on before the previous server has had time to determine that the handset is no longer connected to it. The problem should go away after about 30 seconds.
Must Upgrade SW!	Handset software is incompatible with hardware.	Download new software from the Avaya website per *Software Maintenance*.
Net Busy xxxxxxxxxxxx	x…x = AP MAC address. Handset cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.	Try the call again later.
No 802.11a Sub-bands Enabled	'a' radio selected but no sub-bands are enabled	Configure 'a' radio sub-bands from **Admin** menus
No 802.11 Sub-bands Enabled	'b/g radio selected but no sub-bands are enabled	Configure 'b/g' radio sub-bands from **Admin** menus
No APs Heard	The handset is unable to hear beacons/probes from any AP in the network in site survey mode.	Verify that network is properly configured and the handset is able to hear beacons from the AP.
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to WLAN or use Static IP configuration in the handset.
No ESSID	Attempted to run Site Survey application without an ESSID set.	Let handset come completely up. Statically configure an ESSID in the **Admin** menu.
No Func Code	Handset software download files are incorrect or corrupted.	Reconfigure the handset to gain access to the WLAN and download new code.
No Host IP	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid host IP address (the handset’s IP address) has been entered.	Enter a valid IP address in the configuration settings or change to “use DHCP.”
No IP Address	Invalid IP.	Check the IP address of the handset and reconfigure if required.
No Net Access	Cannot authenticate / associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found No APs	This indicates that the handset cannot find any access points and has no additional information to display as to why. Possible problems are enumerated below. No radio link.	 Verify that the AP is turned on.

Message	Description	Action
	No ESSID: Auto-learn not supported (or) incorrect ESSID. AP does not support appropriate data rates. Out of range.	Verify the ESSID of the wireless LAN and enter or Autolearn it again if required. Check the AP configuration against Configuration Guide for AP. Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of this handset.
	Incorrect Security settings.	Verify that all the Security settings in the handset match those in the APs.
No Net Found xxxxxxxxxxxx yy	x…x = AP MAC address. yy = AP signal strength. Handset cannot find a suitable AP; displays MAC and signal strength of "best" non-suitable AP found.	Check AP and handset network settings such as ESSID, Security, Reg domain and Tx power. Ensure APs are configured per *VIEW Configuration Guide* for AP. Try Site Survey mode to determine a more specific cause.
No Net Found No CCX APs	The Wireless Telephone is configured for CCX compatible operation, but cannot find an access point that is advertising CCX capability.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No CCKM APs	The Wireless Telephone is configured to use CCKM for fast and secure handoffs, but cannot find an access point that is configured appropriately.	Check the AP configuration against *VIEW Configuration Guide* for AP.
No Net Found No WMM APs	The Wireless Telephone is configured to use Wi-Fi Standard QoS, but cannot find an AP configured appropriately.	Check the AP configuration against *VIEW Configuration Guide*.
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from proxy server.	Verify that proxy server IP address and port are properly configured.
No Reg Domain	Regulatory Domain Not Set.	Configure the Regulatory Domain of the handset.
No Server IP	In the case of static IP configuration, the handset failed to find the call server IP.	Verify that call server info is properly configured on the handset.
No SVP IP	The handset is configured for "Static IP" (as opposed to "use DHCP"), and no valid Avaya SVP Server address has been entered.	Enter a valid Avaya SVP Server IP address in the configuration setting or change to "use DHCP."

Message	Description	Action
No SVP Response yyy.yyy.yyy.yyy	y…y = SVP Server IP address. Handset has lost contact with the SVP Server.	This may be caused by bad radio reception or a problem with the Avaya SVP Server. The handset will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset will restart. Report this problem to the system administrator if it keeps happening.
No SVP Server	Handset can't locate Avaya SVP Server. Avaya SVP Server is not working. No LAN connection at the Avaya SVP Server.	IP address configuration of Avaya SVP Server is wrong or missing. Check error status screen on Avaya SVP Server. Verify Avaya SVP Server connection to LAN.
No SVP Server No DNS Entry	Handset unable to perform DNS lookup for SVP Server, server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option 151.
No SVP Server No DNS IP	Handset unable to perform DNS lookup for SVP Server, no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been identified.	Check that the handset license type has a corresponding entry in the slnk_cfg.cfg file. Check that the correct files are listed under the handset license type entry.
No TFTP Response	The handset could not get the HTTP/TFTP server to respond.	The handset will continue to boot without checking if its current code is the latest available. Check that the HTTP/TFTP server is operational. If the Wireless Telephone is using DHCP, check that the DHCP options are set correctly.
No WPA PassPhrase	This error only appears when the Admin menus are exited. The handset is configured for WPA-PSK or WPA2-PSK and no pass phrase or shared key has been entered.	Enter the pass phrase or pre-shared key and restart the handset
Not Installed!	A required software component is missing.	Check that all required software files are on the HTTP/TFTP server, if over-the-air downloading is being used. If the error repeats, contact Avaya Technical Support.
Press END	The far end of a call has hung up.	Hang up the near end.
Press END to quit	The handset is waiting to acquire bandwidth required for voice communication.	Press **END** or wait until bandwidth is available.

Message	Description	Action
Prom Bad Length	The handset software downloaded files that are incorrect or corrupted.	Download new software from the Avaya website per *Software Maintenance*.
Registering	The handset has completed initialization of the SIP application and is attempting to register lines to the SIP proxy servers.	If registrations are failing, the phone can stay in this state for a considerable length of time. After the phone leaves this state, press the **LINE** key to view what lines have failed to register. Ensure usernames and passwords have been entered in administrative menus for registrations that have failed and that proxy information is correct in the SIP configuration files.
RTP Open Failed	The handset attempted to open an RTP port for audio but was unsuccessful.	Verify that Avaya SVP Server capacity has not been exceeded.
Select License	The correct protocol has not been selected from the license set.	Using the **Admin** menu, select one license from the set to allow the phone to download the appropriate software.
Server Busy	Handset is attempting to download from a HTTP/TFTP server that is busy downloading to other devices and refusing additional downloads.	None, the handset will automatically retry the download every few seconds.
SIP Login	Prompt for login information – username and password.	At power-on initialization, no username was detected in the **Admin** menu items for SIP registrations. Enter a valid username and password for an existing SIP configuration file.
Skt Open Fail	Socket open fail. Occurs when the handset attempts to open a connection to the proxy server but fails.	Verify that Avaya SVP Server capacity has not been exceeded.
Service Rej.	The Avaya SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the Avaya SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
Storing Config	Handset is storing changes to handset configuration.	None. Informational only. The handset may display this briefly following a configuration change or software download.
SVP Service Rej.	The Avaya SVP Server has rejected a request from the handset.	The handset will restart and attempt to re-register with the SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy	y…y = SVP Server IP Address. SVP Server has reached call capacity.	All call paths are in use, try the call again in a few minutes.
System Locked (with Busy Tone)	Avaya SVP Server is locked.	Try call again later, system has been locked for maintenance.

Message	Description	Action
TFTP ERROR(x):yy	A failure has occurred during a HTTP/TFTP software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are: 01 = HTTP/TFTP server did not find the requested file. 02 = Access violation (reported from HTTP/TFTP server). 07 = HTTP/TFTP server reported "No such user" error. 16 = No HTTP/TFTP server address. 81 = File put into memory did not CRC. FF = Timeout error. HTTP/TFTP server did not respond within a specified period of time.	Error code 01, 02, 07, or 16 - check the HTTP/TFTP server configuration. Error code 81, the handset will attempt to download the file again. For other messages, power off the handset, then turn it on again to retry the download. If the error repeats, note it and contact Avaya Customer Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Avaya.
Unknown xx:yy:zz	A phrase is missing from the phintl language file.	Download new software from the Avaya website per Chapter 11: *Software Maintenance*.
Updating …	The handset is internally updating its software images.	None. The handset may do this briefly after a download. This is informational only.
Updating Code…	Handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.	None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the handset off during this operation.
Wait for bandwidth	The phone is waiting for bandwidth sufficient for voice communication.	No action required. You will have the option of pressing **END** to abort the phone call.
Waiting…	Handset has attempted some operation several times and failed.	None. The handset is waiting for a specified period of time before attempting that operation again.
Wrong Code Type	The software loaded into the handset is incorrect for this model phone.	Replace the software image on the HTTP/TFTP server with software that is correct for the handset model.

Appendix A: Regulatory domains

This table details the specifications for regulatory domain settings. Avaya recommends that you check with local authorities for the latest status of their national regulations for both 2.4 and 5 GHz wireless LANs.

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
01	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	US Canada Brazil
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
02	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Europe Australia New Zealand UAE
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
03	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Japan
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
04	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Singapore
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
05	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Korea
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.6500 GHz	100 – 124	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		

Domain Identifier	802.11 Mode	Band	Channels	DFS Required?	Max. Power Limit (peak power)	Countries
06	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Taiwan
	a	5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8500 GHz	149 – 165†	No		
07	g only b & b/g mixed		1 – 13	n/a	100mW (+20dBm)	Hong Kong
	a	5.1500 – 5.2500 GHz	36 – 48	No	50mW (+17dBm)	
		5.2500 – 5.3500 GHz	52 – 64	Yes	100mW (+20dBm)	
		5.4700 – 5.7250 GHz	100 – 140	Yes		
		5.7250 – 5.8250 GHz	149 – 161	No		
08	g only b & b/g mixed		1 – 11	n/a	100mW (+20dBm)	Mexico India
	a	5.1500 – 5.2500 GHz	36 – 48	No		
		5.2500 – 5.3500 GHz	52 – 64	Yes		
		5.7250 – 5.8500 GHz	149 – 161	No		

† Channel 165 is not currently supported on the handset when the UNI-3 (5.7250 – 5.8250) band is enabled for 802.11a.

Appendix B: Remote configuration parameters definition

The following table describes the parameters that can be used in the remote configuration file. This file is typically named 46xxsettings.txt and includes a 364x endpoint section. Parameters below followed by an asterisk are those that are common with at least one other Avaya phone. The 364x endpoint section contains parameters that are specific to the Avaya 3641/3645/6120/6140 IP Wireless Handsets.

Note that double quotes can be used around the entire value that a parameter is set to, with the exception of the SIP_FAVORITES parameter. They can also be used to denote the NULL string (“”). They cannot be used any other way except on the SIP_FAVORITES parameter. See the sample file for more information.

Persistency

The handset saves configuration information in its memory and uses the information if the value is not available otherwise. This persistence is true for all the parameters.

In order to remove a parameter that was previously set and no longer needed, one must set it to the null string (“”) in the configuration file. The null string can be used to clear out any parameter that is a string or an IP address. Other parameters, such as a port address, have to be deliberately set back to the default to get rid of a particular definition. For parameters that are enabled or disabled, just removing them from the configuration file does not disable them if they were previously enabled, you must deliberately set them to 0 to disable them (for instance, the OAI_ENABLE parameter).

In some installations, it is advisable to set all user specific values, such as lines, to the null string rather than leaving them un-configured.

Precedence and how the handset initializes and uses the supplied parameters

If the handset is configured to use DHCP, it initializes using the values supplied by DHCP (non-SSON data). Note that these values supplied by non-SSON DHCP are used by the handset, but they are not stored in persistent storage on the handset. If any of the requested parameters are not supplied by non-SSON DHCP, values for those same parameters in persistent storage (if any) will be used. Then the handset parses the SSON data and any values specified in this data are saved in persistent storage on the handset (overwriting any previously saved data). The handset will start using the new values immediately as long as these are values that do not require a config reboot.

If the handset is not configured to use DHCP, it initializes using values from persistent storage on the handset.

Next, the handset reads in the generic config file if possible. Any values specified in this generic config file are saved in persistent storage on the handset (overwriting any previously saved data). The handset will start using the new values immediately as long as these are values that do not require a config reboot.

Then the handset reads in the handset specific config file if possible. Any values specified in this handset specific config file are saved in persistent storage on the handset (overwriting any previously saved data). The handset will start using the new values immediately as long as these are values that do not require a config reboot.

If any of the parameters that can cause a config reboot (see table) were modified by the SSON data or either of the config files, the handset will now reboot and initialize using the values supplied by DHCP (if configured to use DHCP) and the latest values of all other parameters.

Config reboot

If a parameter is changed via SSON data or one of the config files and the handset cannot begin to use that parameter without rebooting (see table below for these parameters), the handset will reboot when it finishes reading in and processing the SSON data and config files. The handset will not prompt the user for login info and it will not re-read the config files, it just reboots and starts using all the new configuration values.

The handset does not reboot if none of these indicated parameters have changed. It does not reboot for changes in other parameters (those that are not indicated in the table as parameters that cause a reboot).

Note:
Certain phone parameters allow values that the installed PBX may not support. The PBX restrictions should be taken into account when configuring the handsets using these SIP parameters. For instance, a PBX may support up to 13 digits for a username value where the phone itself has broader options. In this case, you must limit your options to those supported by the PBX. Other such situations may exist in your facility. Be sure to configure values that all components used by the phones can recognize.

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
SYSLANG*[4]	English, Francais, Deutsch, Espanol, Italiano	English		no	Admin menus, HAT, SSON, config files
GMTOFFSET*	"0:00"[5]	00:00		yes	Admin menus, HAT, SSON, config files
DSTADJUST	none, usa, aus, euro	none		yes	Admin menus, HAT, SSON, config files
PROCPSWD*	1-7 digits or NULL[6] (no password)	27238		no	Admin menus, HAT, SSON, config files
TFTPSRVR	ip addr or NULL[6]	not set	static	no	Admin menus, HAT, DHCP Option 66, SSON, config files, dhcp
LOGSRVR*	ip addr or NULL[6]	not set	static	yes	Admin menus, HAT, DHCP Option 7, SSON, config files, dhcp

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
SNTPSRVR*	ip addr[7] or NULL[6]	not set	static	yes	Admin menus, HAT, DHCP Option 42, SSON, config files, dhcp
SVPSRVR	ip addr or NULL[6]	not set	static	yes	Admin menus, HAT, DHCP Option 151, SSON, config files, dhcp
OAISRVR	ip addr or NULL[6]	not set	static	yes	Admin menus, HAT, DHCP Option 152, SSON, config files, dhcp
DNSSRVR*	ip addr or NULL[6]	not set	static	no	Admin menus, HAT, DHCP Option 6, SSON, config files, dhcp
DOMAIN* (for dns)	1-63 chars, no spaces or NULL[6]	Null	static	no	Admin menus, HAT, DHCP Option 15, SSON, config files, dhcp
HTTPSRVR*	ip addr/DNS name list or NULL[6] - up to 255 chars	not set	static	no	Admin menus, HAT, SSON, config files[8]
HTTPPORT*	number from 0-65535	80	static	no	Admin menus, HAT, SSON, config files
HTTPDIR*	0-127 chars, no spaces or NULL[6]	none	static	no	Admin menus, HAT, SSON, config files
WLAN_ESSID	1-32 chars[6]	not set		yes	Admin menus, HAT, SSON, config files
WLAN_USE_CCX	0,1 (0=custom, 1=use CCX)	0		yes	Admin menus, HAT, SSON, config files
WLAN_SECURITY	none, wep, wpa2psk, wpapsk, fsr, wpa2e	none		yes	Admin menus, HAT, SSON, config files
WEP_AUTHENTICATION	openSystem, sharedKey	open system	wep	yes	Admin menus, HAT, SSON, config files
WEP_DEFAULT_KEY	1-4	1	wep	yes	Admin menus, HAT, SSON, config files
WEP_KEY_LEN	40bit, 128bit	40bit	wep	yes	Admin menus, HAT, SSON, config files
WEP_KEY1	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes	Admin menus, HAT, SSON, config files
WEP_KEY2	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes	Admin menus, HAT, SSON, config files
WEP_KEY3	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes	Admin menus, HAT, SSON, config files

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
WEP_KEY4	10 hex digits for 40 bit keys, 26 hex digits for 128 bit keys or NULL[6]	not set	wep	yes	Admin menus, HAT, SSON, config files
WPA_TYPE	passphrase, psk	passphrase	wpa2psk, wpapsk	yes	Admin menus, HAT, SSON, config files
WPA_PASSPHRASE	1-63 chars or NULL[6]. Illegal characters: ASCII 34("), ASCII 63 (?),ASCII 96 (`).	not set	wpa2psk, wpapsk	yes	Admin menus, HAT, SSON, config files
WPA_PSK	64 hex chars or NULL[6]	not set	wpa2psk, wpapsk	yes	Admin menus, HAT, SSON, config files
WPA2E_AUTH	eapfast, peap	eapfast	wpa2e	yes	Admin menus, HAT, SSON, config files
WPA2E_FAST_HANDOFF	cckm, okc	cckm	wpa2e	yes	Admin menus, HAT, SSON, config files
WLAN_SEC_USERNAME	1-32 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	fsr, wpa2e	yes	Admin menus, HAT, SSON, config files
WLAN_SEC_PASSWORD	1-32 chars or NULL[6]. Valid chars:A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set	fsr, wpa2e	yes	Admin menus, HAT, SSON, config files
WLAN_QOS_TYPE	svp, wifiStandard	svp		yes	Admin menus, HAT, SSON, config files
WMM_ACCESS_CONTROL	mandatory, optional	mandatory	qos= wifi standard	yes	Admin menus, HAT, SSON, config files
DSCPAUD*	0-63	46		yes	Admin menus, HAT, SSON, config files
DSCPSIG*	0-63	34		yes	Admin menus, HAT, SSON, config files
DSCP_OTHER	0-63	0		yes	Admin menus, HAT, SSON, config files
WLAN_RADIO_MODE	a, b&b/g, g	none		yes	Admin menus, HAT, SSON, config files
WLAN_A_SUBBANDS	Comma separated list of 1-6[9]	none	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_A1	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_A2	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_A3	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
WLAN_TX_POWER_A4	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_A5	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_A6	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio mode a	yes	Admin menus, HAT, SSON, config files
WLAN_TX_POWER_BG	5mW, 10mW, 20mW, 30mW, 40mW, 50mW, 100mW	30mW	radio modes b&b/g, g	yes	Admin menus, HAT, SSON, config files
DIAG_DISPLAY_ENABLE	0,1 (0=disable, 1=enable)	0		yes	Admin menus, HAT, SSON, config files
SYSLOG_MODE	disabled, errors, event, full	disabled		yes	Admin menus, HAT, SSON, config files
ERROR_HANDLING	halt, restart	restart		yes	Admin menus, HAT, SSON, config files
OAI_ENABLE	0,1 (0=disable, 1=enable)	0		yes	Admin menus, HAT, SSON, config files
RTLS_ENABLE	0,1(0=disable, 1=enable)	0		yes	Admin menus, HAT, SSON, config files
RTLSSRVR	ip addr or NULL[6]	not set		yes	Admin menus, HAT, SSON, config files
RTLS_PORT	1-65535	8552		yes	Admin menus, HAT, SSON, config files
RTLS_INTERVAL	15sec, 30sec, 1min, 5min, 10min	10min		yes	Admin menus, HAT, SSON, config files
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION*_	seconds; 60-31536000	86400	PPM_ENABLE=1	no	SSON, config files[15]
PTT_OR_EMERGENCY_DIAL	ptt, emergency_dial, none	none		yes	Admin menus, HAT, SSON, config files
PHNEMERGNAME	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	null		yes	Admin menus, HAT, SSON, config files
PHNEMERGNUM*	1-16 numeric digits or NULL[6]	null		yes	Admin menus, HAT, SSON, config files
PPM_ENABLE[12]	0, 1 (0 = Disabled, 1 = Enabled)	1		no	SSON, config files
PTT_CHANNELS	1,2,3,….24 (any or none)	all 24		yes	Admin menus, HAT, SSON, config files
PTT_CH_NAME_01-24	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes	Admin menus, HAT, SSON, config files

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
PTT_PRIORITY_CH_ENABLE	0,1 (0=disable, 1=enable)	0		yes	Admin menus, HAT, SSON, config files
PTT_PRIORITY_CH_NAME	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes	Admin menus, HAT, SSON, config files
RDS_INITIAL_RETRY_TIME*	seconds; 2 – 60	2	PPM_ENABLE=1	no	SSON, config files
RDS_MAX_RETRY_TIME*	seconds; 2 – 3600	600	PPM_ENABLE=1	no	SSON, config files
RDS_INITIAL_RETRY_ATTEMPTS*	1 – 30	15	PPM_ENABLE=1	no	SSON, config files
SIP_USERNAME1	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes	Admin menus, HAT, SSON, config files
SIP_USERNAME2-6	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		no	Admin menus, HAT, SSON, config files
SIP_PASSWORD1	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		yes	Admin menus, HAT, SSON, config files
SIP_PASSWORD2-6	1-16 chars or NULL[6]. Valid chars: A-Z, a-z, 0-9, *.-_!$%&'()+,:;/\=@~# and space.	not set		no	Admin menus, HAT, SSON, config files
CODEC_LIST	one or more (in preferred order) of: g711u, g711a, g729	g711a, g711u		no	SSON, config files
SIPPORT*	0-65535	5060		no	SSON, config files
SIPPROXYSRVR*	ip addr/ DNS name[10]	none		no	HAT, SSON, config files
SEND_DTMF_TYPE*	1=in-band, 2=rfc2833	1		no	SSON, config files
SIP_SEND_INFO[11]	0,1 (0=do not send INFO requests, 1=send INFO requests)	0		no	SSON, config files
USE_QUAD_ZEROES_FOR_HOLD*	0,1 (0=disable, 1=enable)	0		no	SSON, config files
SIP_PRACKING	0,1 (0=disable, 1=enable)	0		no	SSON, config files
REGISTERWAIT*	seconds; 0-65535	3600		no	SSON, config files
SIP_KEEPALIVE_INTERVAL	seconds; 10-3600 or 0 (no keep alives)	0 (no keep alives)		no	SSON, config files

Parameter name	Allowable values[1]	Default[2]	Assoc info[3]	Causes reboot	Source
SIPDOMAIN*	ip addr/FQDN no spaces; 1-60 chars or NULL[6]	null		no	SSON, config files
SIP_CALLID_PER_LINE[12]	0,1 (0=can use same Call-ID header value for different lines, 1=must use unique call id per line)	0		no	SSON, config files
MSGNUM*	dial string; 1-50 chars, no spaces or NULL[6]	none		no	SSON, config files
SIP_MAIL_SUBSCR	dial string; 1-50 chars, no spaces or NULL[6]	none		no	SSON, config files
SIP_FAVORITES	comma separated list of up to 15 "number";"name" (number can appear without quotes) or NULL[6]	none		no	config files
SIP_LINE1-5	1-16 chars or NULL[6]	not set		no	HAT (line1 only), SSON, config files
SIP_LINE_CALLID1-5	1-18 chars or NULL[6]	not set		no	SSON, config files
SNMPADD*	IP address/DNS name list or NULL[6] - up to 255 characters			no	User menus, HAT, SSON, config files[8], System Manager[14]
SNMPSTRING*	1-32 characters (no spaces) or NULL[6]			no	User menus, HAT, SSON, config files[8], System Manager
PAC_FILENAME	1-32 chars or NULL	none		yes	HAT, SSON, config files
SERVER_CERT_FILENAME	1-32 chars or NULL	none		yes	HAT, SSON, config files

Table footnotes

* This parameter already appears in the 46xxsettings.txt file and is common with at least one other Avaya phone.

1. These are the allowable values that can be set using the remote configuration parameter. The allowable values for the same configuration item in HAT and menus may not adhere to these listed allowable values.
2. Default: the value used if no value is specified in the saved parameters on the phone (from HAT, Admin menus or previous init of phone), or from dhcp, SSON dhcp, or 46xxsettings.txt file. Or the value has been cleared using NULL.
3. Assoc info: used to indicate when the parameter is used or ignored. Specifically it is to indicate:
    a. Which IP addresses belong to the group called static IP addresses. These appear on the IP Address menu in the Admin menus and HAT.
    b. The security type that a label goes with (e.g., WPA_PSK is used only with security types wpapsk and wpa2psk).
    c. Which power variables go with which radio modes.

d. WMM_ACCESS_CONTROL is only used for qos type wifiStandard.

4. The SYSLANG parameter value will always be overridden by any user entered language. That is, this parameter will take effect only if the user has not modified the language via the standby menus.
5. GMTOFFSET: Valid values are a positive or negative number of hours and minutes less than 13 hours. One to six ASCII characters, optionally beginning with “+” or “-”, followed by one or two ASCII numeric digits whose combined value is from 0 to 12, optionally followed by a “:” and two ASCII numeric digits that can be any of 00, 15, 30, or 45. Other minute values in the range 01 to 59 will not generate an error but will be interpreted as if they were 00. Minute values not 2 digits long will be rejected. Note: This parameter may specify minutes other than 00, 15, 30, or 45 on Avaya desksets.
6. SNTPSRVR: This is an existing parameter which allows a list for Avaya desk sets and also can be IP or DNS name but the Avaya 364x phone will only look at the first entry and it must be an IP address (no DNS).
7. HTTPSRVR and SNMPADD: These can be specified in HAT/Admin menus as well as the config files but we are not adding Admin menu or HAT support for lists of values. We are adding an Admin menu item for a single HTTP server IP address (not DNS name) and we are adding a user menu item for a single SNMP server IP address (not DNS name). The list and the single address will not exist in the phone at the same time. When the single IP address is set via HAT/menus, the list will be cleared. Whenever the list is encountered in config, the single IP address will be cleared. When the phone needs to do HTTP or SNMP, it will first try to use the single IP specified by the Admin menus. If this is not specified, the phone will move to using the servers on the list specified in SSON or the config files.
8. WLAN_A_SUBBANDS: Comma separated list of the following numbers. Only the sub-bands that are available in the selected Regulatory Domain will be used. Others, if listed, will be ignored.
    a. 1 = 5.150-5.250
    b. 2 = 5.250-5.350 DFS
    c. 3 = 5.470-5.725 DFS
    d. 4 = 5.725-5.825
    e. 5 = 5.725-5.850
    f. 6 = 5.470-5.650 DFS
9. SIPPROXYSRVR: This is an existing parameter which allows a list for Avaya desk sets but the Avaya 364x phone will only look at the first IP/DNS name in the list. If the first thing on the list is not an IP address, DNS will be attempted to resolve this for the SIP server IP address. Note that the same is true for the SIP Proxy Server value entered via HAT – if it is not an IP address, it is assumed to be a DNS name and DNS will be done to resolve it.
10. SIP_SEND_INFO controls generation SIP INFO request messages for key press events.
11. SIP_CALLID_PER_LINE controls whether a unique call ID must be used for registering each line (instead of unique per proxy) as required by some SIP servers.

12. Enabling the parameter PPM_ENABLED makes certain advanced Avaya Aura® handset features available. A value of 1 enables the parameter and a value of 0 disables the parameter. The parameter is in enabled state by default. If you disable this parameter, the features of remote configuration of SNMP parameters and remote rebooting of the handsets are not available.

    Note:
    The Avaya 3641/3645/6120/6140 IP Wireless Handsets for SIP are not Avaya AST devices. The Avaya 641/3645 IP Wireless Handsets for SIP support only those functionalities that are mentioned in this Administrator Guide.

13. You can configure the SNMP parameters SNMPADD and SNMPSTRING remotely through System Manager, provided you have the parameter PPM_ENABLED in the enabled state.
14. The parameter OUTBOUND_SUBSCRIPTION_REQUEST_DURATION controls the Avaya-ccs-profile event subscription. The REGISTERWAIT timer controls the subscription for message–summary.