Spectralink VIEW Certified Configuration Guide

Aruba Networks

Aruba Instant APs IAP-11x, 20x, 21x, 22x

721-1008-000 Rev: B
May 2016

Copyright Notice

Notice

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3769 9800

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, R612 8PE
United Kingdom

infoemea@spectralink.com

Contents

Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink Wireless Telephones and wireless LAN (WLAN) infrastructure products.

The products listed below have been tested in Spectralink's lab and have passed VIEW Certification.

Certified Product Summary

Manufacturer:	Aruba Networks: www.arubanetworks.com
Certified products:	Access Points: Aruba Instant APs – AP-11x, 20x, 21x, 22x
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)
Security:	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2) with OKC
QoS:	Wi-Fi Standard for Spectralink PIVOT, 8440/8441/8450/8452/8453,8741/8742/8744/8753
Network topology:	Switched Ethernet (recommended)
AP and WLC software versions approved:	6.4.3.1-4.2.0.3

Handset models tested:*	*Spectralink PIVOT*		
Handset radio mode:	802.11b	802.11b/g	802.11a
Meets VIEW minimum call capacity per AP:	8	8	10

Handset models tested:	*Spectralink 8440/8441/8450/8452/8453 Wireless Telephone*		
Handset radio mode:	802.11b	802.11b/g	802.11a
Meets VIEW minimum call capacity per AP:	8	8	10

*****Spectralink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as "Spectralink Wireless Telephones", "phones" or "handsets".

** Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls

Known Limitations

The following limitations were discovered during VIEW testing of this product:

- 1Mb/s and 2Mb/s data rates must be disabled to meet maximum call capacity.
- 802.11n must be disabled on the handsets to meet maximum call capacity with background data traffic.
- The Spectralink phones must use the single antenna mode to communicate in 2.4 GHz with the IAP-115. This is accomplished with the csd-override parameter, use of which is described below.
- Broadcast filtering none instead of the default Broadcast filtering ARP must be used on any SSID serving Spectralink voice for proper SIP server connection and PTT operation. Aruba does not recommend this setting on other SSIDs as it may cause heavy network traffic.
- 802.11r is not implemented on the Spectralink products

The following limitations apply only to the indicated models:

- IAP-11x

  Use the single antenna mode to communicate in 2.4 GHz. This is accomplished with the csd-override parameter, use of which is described below.

- IAP-20x

  Turn off the TSPEC feature.

  Data traffic must be carried on the same SSID as the voice packets to be prioritized properly, on both 2.4 GHz and 5 GHz radios. Or, provide a voice SSID for the Spectralink handset on separate radio channels or a different radio from clients with heavy data use.

- IAP-21x

  Data traffic must be carried on the same SSID as the voice packets to be prioritized properly, on both 2.4 GHz and 5 GHz radios. Or, provide a voice SSID for the Spectralink handsets on separate radio channels or a different radio from clients with heavy data use.

- IAP-22x

  Data traffic must be carried on the same SSID as the voice packets to be prioritized properly, on the 2.4 GHz radio. Or, provide a voice SSID for the Spectralink handset on separate radio channels or a different radio from clients with heavy data use.

VIEW Certification Testing Feature Summary Results

WLAN infrastructure products including access points (APs), their related controllers, and cloud management products, as applicable that interoperate with Spectralink handsets must meet certain requirements to achieve VIEW Certification.

The minimum VIEW requirements listed below are necessary to meet acceptable voice quality, battery life, and Wi-Fi roaming performance for enterprise-grade deployments of Spectralink handsets. WLAN products must fulfill all of the minimum requirements to be listed as VIEW-certified.

The optional enhanced capabilities can be tested and documented as supported for WLAN products that support any or all of them. These items may provide additional feature support, such as support for Spectralink's Push-to-talk (PTT), or improved performance in more demanding deployments.

The table below indicates which capabilities have been verified by Spectralink for the AP models described in this document.

Defined and tested VIEW certification interoperability features – IAP-20x

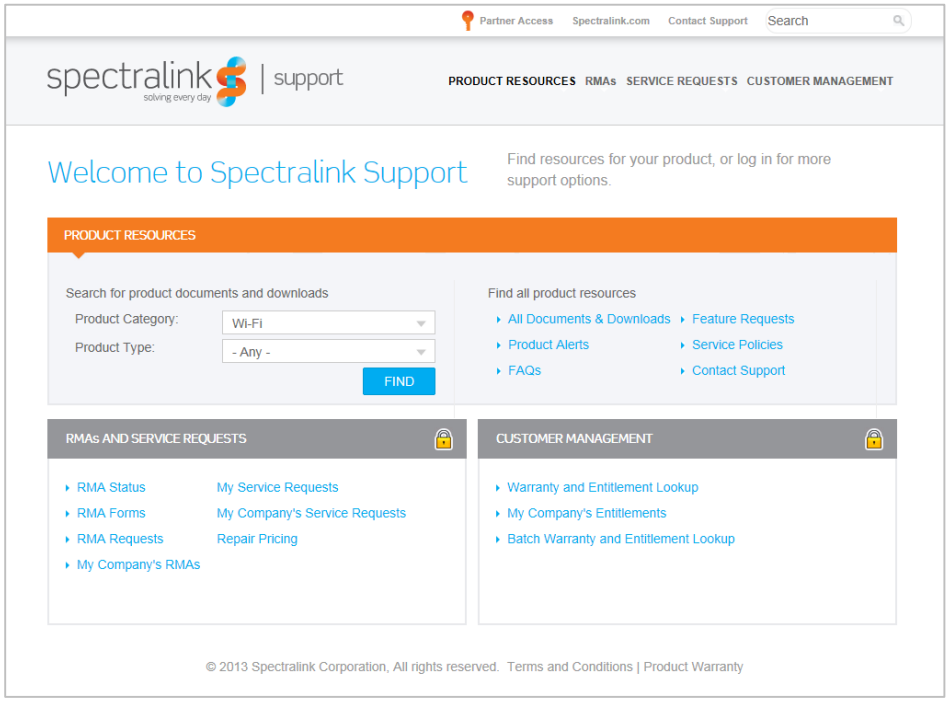
Interop Feature	*Minimum VIEW requirements*	*Optional enhanced capabilities*
WMM QoS	X	
WMM U-APSD	X	
Security – WPA2-PSK	X	
Performance in call, with ftp, during handoffs	X	
Radar Avoidance (DFS)	X	
Proxy ARP	X	
Security – PEAP/EAP TLS and handoff performance		X
Security – EAP-FAST		X
802.11n A-MSDU Aggregation		X
802.11n A-MPDU Aggregation		X
Admission control based on TSPEC		
Multicast and IGMPv2 (for PTT)		X
802.11ac		X

Defined and tested VIEW certification interoperability features – IAP-11x

Interop Feature	*Minimum VIEW requirements*	*Optional enhanced capabilities*
WMM QoS	X	
WMM U-APSD	X	
Security – WPA2-PSK	X	
Performance in call, with ftp, during handoffs	X	
Radar Avoidance (DFS)	X	
Proxy ARP	X	
Security – PEAP/EAP TLS and handoff performance		X
Security – EAP-FAST		X
802.11n A-MSDU Aggregation		X
802.11n A-MPDU Aggregation		X
Admission control based on TSPEC		X
Multicast and IGMPv2 (for PTT)		X
802.11ac		

Spectralink References

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



To go to a specific product page:

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

Support documents

Spectralink 87-Series Wireless Telephone Administration Guide The Admin Guide provides detailed information about every setting and option available to the administrator on both the CMS and handset menus. Time-saving shortcuts, troubleshooting tips and other important maintenance instructions are also found in this document.

Spectralink 87-Series Wireless Telephone Deployment Guide The Deployment Guide provides sequential information for provisioning and deploying the handsets. It covers deployment using the SLIC tool and CMS as well as manual deployment.

The Spectralink 84-Series Wireless Telephone Administration Guide provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

The Spectralink 84-Series Deployment Guide is your essential reference for provisioning and deploying Spectralink 84-Series handsets in any environment.

The Web Configuration Utility User Guide explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

White Papers

Spectralink White Papers are available at http://www.spectralink.com/resources/white-papers.

For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Handsets* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony.

These White Papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

Product Support

If you encounter difficulties or have questions regarding the configuration process, please contact Aruba customer service at: http://www.arubanetworks.com/support.php or Spectralink at support.spectralink.com.

Note: RADIUS server configuration

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise security types.

Configuration for Wi-Fi Standard QoS

Introduction

PIVOT and 84-Series handsets only support Wi-Fi Standard QoS.

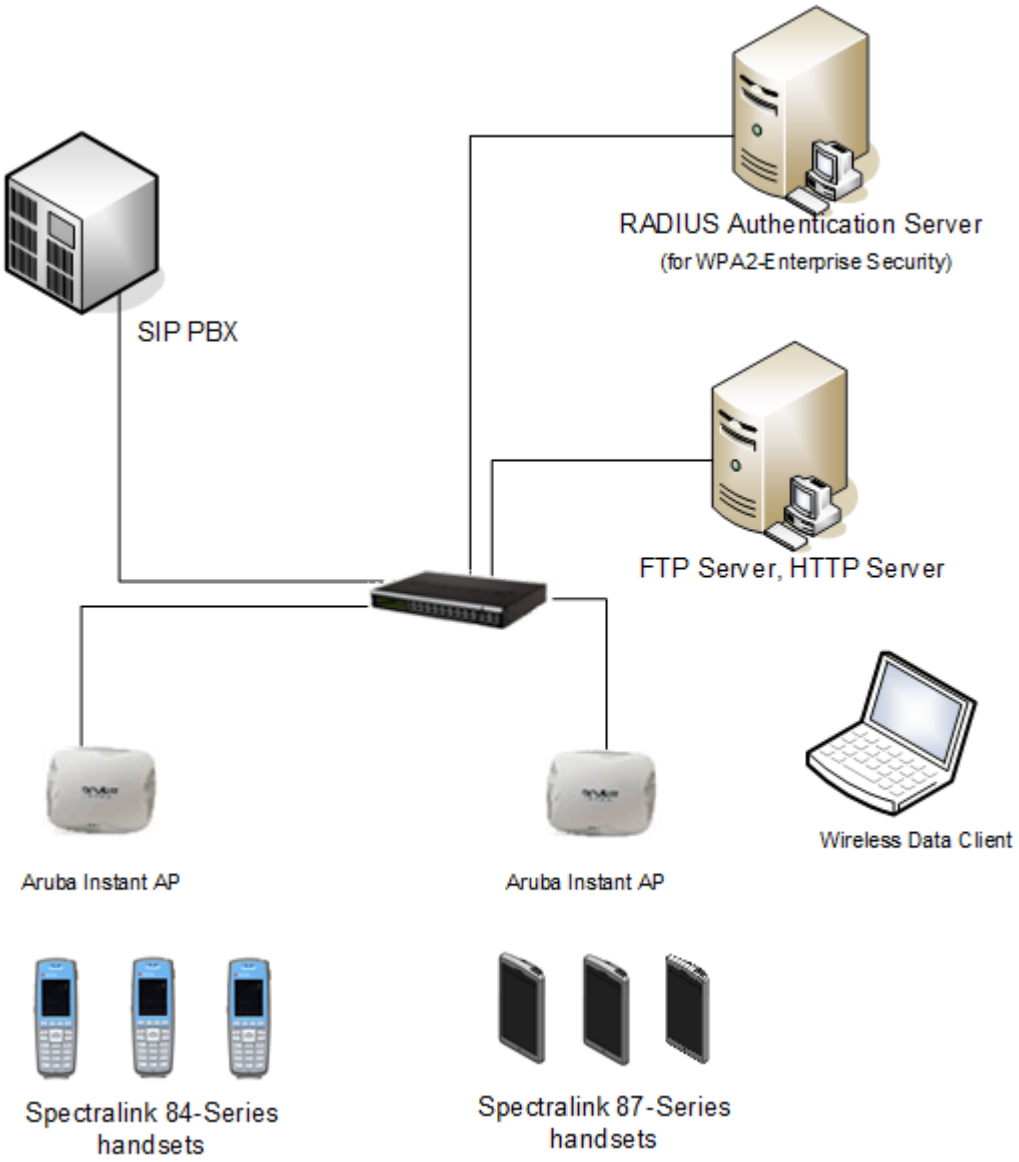
Command, Comment, and Screen Text Key

In the sections below you will find commands, comments, prompts, system responses, or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

Text Style	*Denotes:*
`xxxxxxxx`	Typed command
`<xxxxxxxx>`	Encryption key, domain name or other information specific to your system that needs to be entered
`(xxxxxxxx)`	Comment about a command or set of commands
`xxxxxxxx`	Prompt, system response or other displayed information

Network Topology

The following configuration was tested during VIEW Certification.



Note: Example configuration shown

This is a modified diagram and not all components are shown for every system type.

Initial Configuration of the IAP

Connecting an IAP

Based on the type of the power source used, perform one of the following steps to connect an IAP to the power source:

- PoE switch—Connect the ENET 0 port of the IAP to the appropriate port on the PoE switch.
- PoE midspan—Connect the ENET 0 port of the IAP to the appropriate port on the PoE midspan.
- AC to DC power adapter—Connect the 12V DC power jack socket to the AC to DC power adapter.

Obtaining IP address for an IAP

The IAP needs an IP address for network connectivity. When you connect an IAP to a network, it receives an IP address from a DHCP server. To obtain an IP address for an IAP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the ENET 0 port of IAP to a switch or router using an Ethernet cable.
3. Connect the IAP to a power source. The IAP receives an IP address provided by the switch or router.

Connecting a device to the provisioning IAP network

To connect to the **instant** provisioning Wi-Fi network:

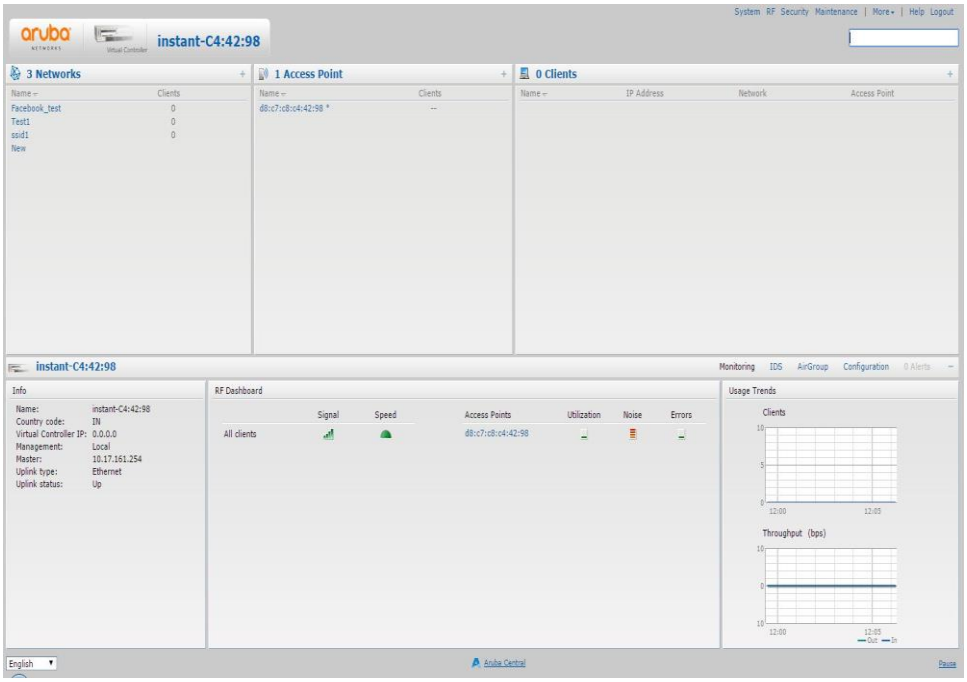
1. Ensure that the client is not connected to any wired network.
2. Click the wireless network connection icon in the system tray.
3. Click on the **instant** network and then click **Connect**.

Logging in to an IAP

To connect to the IAP:

1. Launch a web browser and enter http://instant.arubanetworks.com. The IAP can be accessed **https://<IAP IP address>:4343**. When the IAP UI is launched successfully, the user is prompted with the username and password.
2. Log in to the Instant UI with **admin** and **admin** as username and password respectively. The **Country Code** pop-up is displayed if the IAP-RW (Rest of World) variants are installed. The country code setting is not applicable to the IAPs designed for US, Japan, and Israel.

3 If the **Country Code** window is displayed after a successful login, select a country from the list. On successful login, the main window is displayed.



Wireless LAN Configuration for Wi-Fi Standard QoS

To configure a new wireless network profile using the GUID of the IAP, complete the following procedures:

1 Configuring WLAN Settings

2 Configuring VLAN Settings

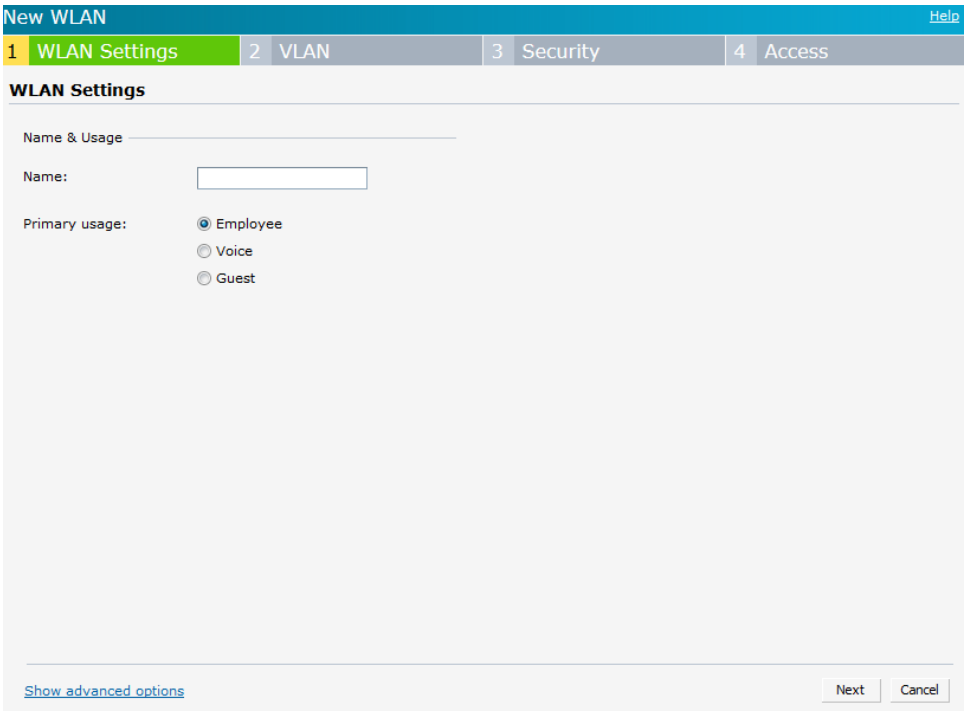
3 Configuring Security Settings

4 Configuring Access Rules for a Network

Configuring WLAN settings for an SSID profile

To configure WLAN settings:

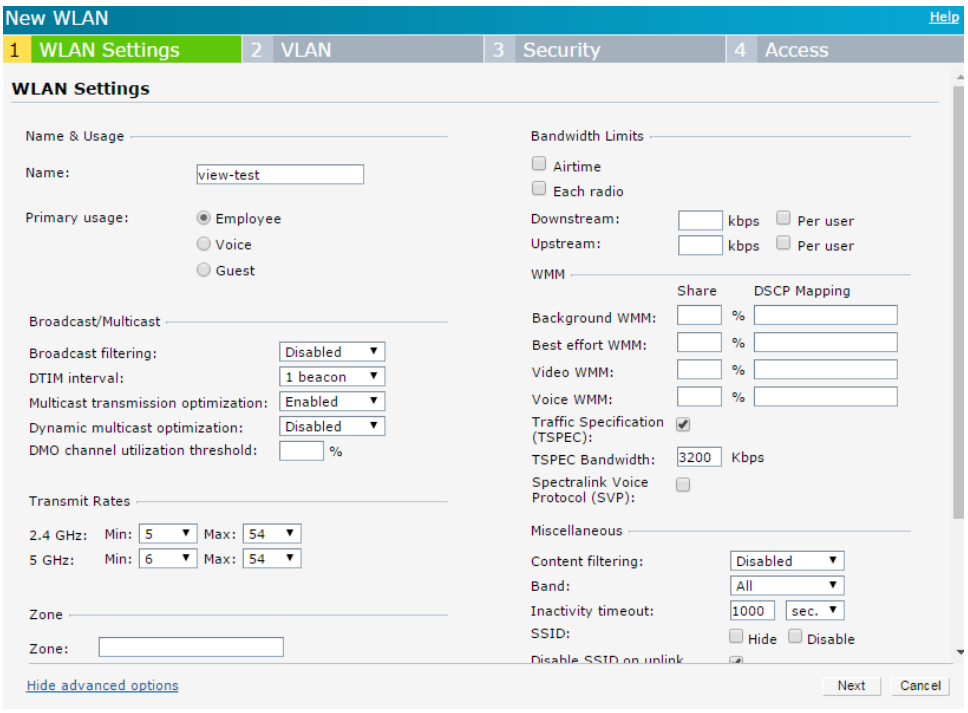
1 From the Instant UI main window, click **New** under the **Networks** section. The **New WLAN** window appears.



2 In the **WLAN Settings** tab, enter a name (SSID) for the network. This name is used for identifying the Network.

3 Select **Employee** as the type of network.

4 Click **Show advanced options**. Additional configuration options are displayed.



5 Set **Broadcast filtering** to **Disabled**.

6 Set **Multicast transmission optimization** to **Enabled.**

7 Retain the default configuration values for **DTIM interval** and **Dynamic multicast optimization**.

8 Ensure that **Traffic Specification (TSPEC)** check box is selected and set the TPSEC bandwidth to the desired value, as described here: **For the IAP-20x models only, *ensure that the* Traffic Specification (TSPEC) *is NOT selected.***

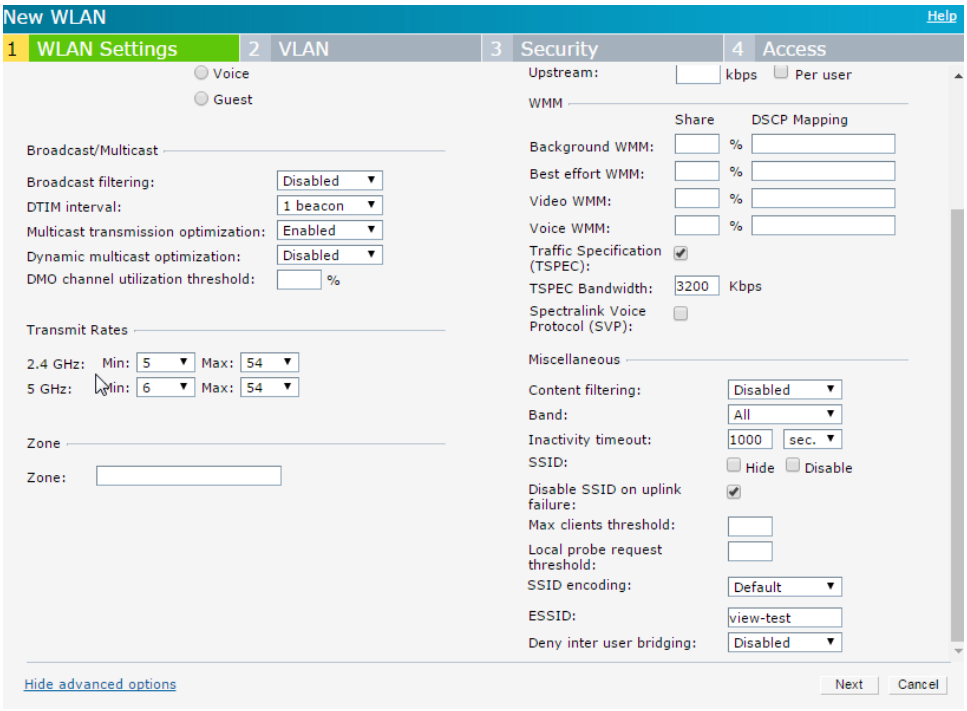
9 Use the bandwidth from the table below that corresponds to the codec the phones on the network will be using. As described in *Spectralink 84-Series Wireless Telephone Administration Guide*, the 84-Series handsets support the codecs shown in the table below. The most common codecs supported by the 84-series are shown. For others, consult with Spectralink technical support.

Choose the bandwidth from the table below that is the largest number needed to support the type of phones or codecs expected so that the number of calls will be limited to what the AP can support.

84-Series handsets Default Codecs (in priority order)

Codec	*Radio*	*Bandwidth*
G.722	5.0 GHz	3200
G.722	2.4 GHz	2400
G.711Mu-law	5.0 GHz	3200
G.711Mu-law	2.4 GHz	2400
G.711A-law	5.0 GHz	3200
G.711A-law	2.4 GHz	2400
G.729AB	5.0 GHz	1200
G.729AB	2.4 GHz	1000

10 Scroll down to reveal the rest of the advanced settings.



11 Ensure that **Deny user bridging** is set to **Disabled** (the default setting) if peer-to-peer (handset-to-handset without the SIP server in the middle) calls are to be allowed. Otherwise, the calls will appear to be working but will not have any audio.

Note: Data and voice SSID assignment

For proper prioritization of voice packets (to avoid audio gaps in calls or dropped calls), ensure that other clients with heavy data usage are on the same SSID or, alternatively, on a different radio. This guideline was found to be necessary for the IAP-22x models in 2.4 GHz radio and for the IAP-20x and IAP-21x models in both 2.4 GHz and 5 GHz radio band.

Configuring VLAN settings for a wireless SSID profile

To define VLANs for the SSID profile:

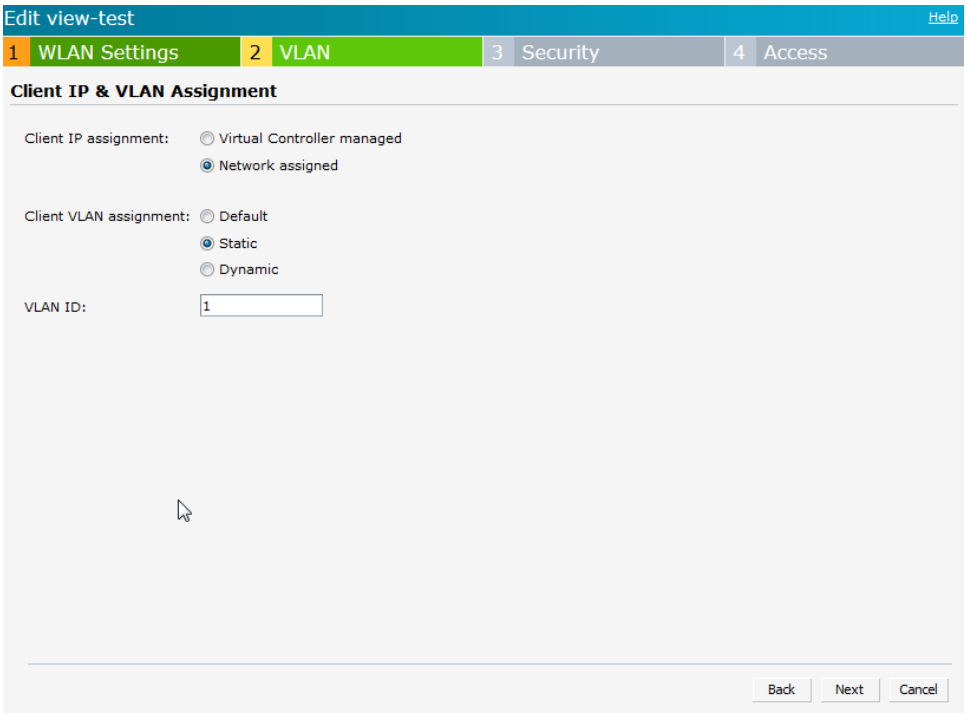
1 In the new **Network** wizard, click the **VLAN** tab or click **Next** from the last section end.

2 Select **Network assigned** under **Client IP assignment**. On selecting this option, the IP address is obtained from the network.

3 Select **Static** under **Client VLAN assignment**.

4 Enter the VLAN Id or range of Ids.

5 Click **Next** to define an authentication profile.



Assigning ports on uplink switch

If you are using Aruba switch, configure a switching profile and assign ports by executing the following commands at the command prompt of the Aruba switch:

```
interface-profile switching-profile <profile-name> switchport-mode {trunk}
trunk allowed vlan <SSID VLAN> exit
```

The **SSID VLAN** corresponds to the VLAN Id used in the Static section above on the **VLAN** tab. For Non-Aruba switches, refer to the respective vendor documentation on how to configure the port to which the AP is attached to allow the VLAN id specified.

Configuring security settings for a wireless SSID profile

The type of security for the SSID Profile is selected next.

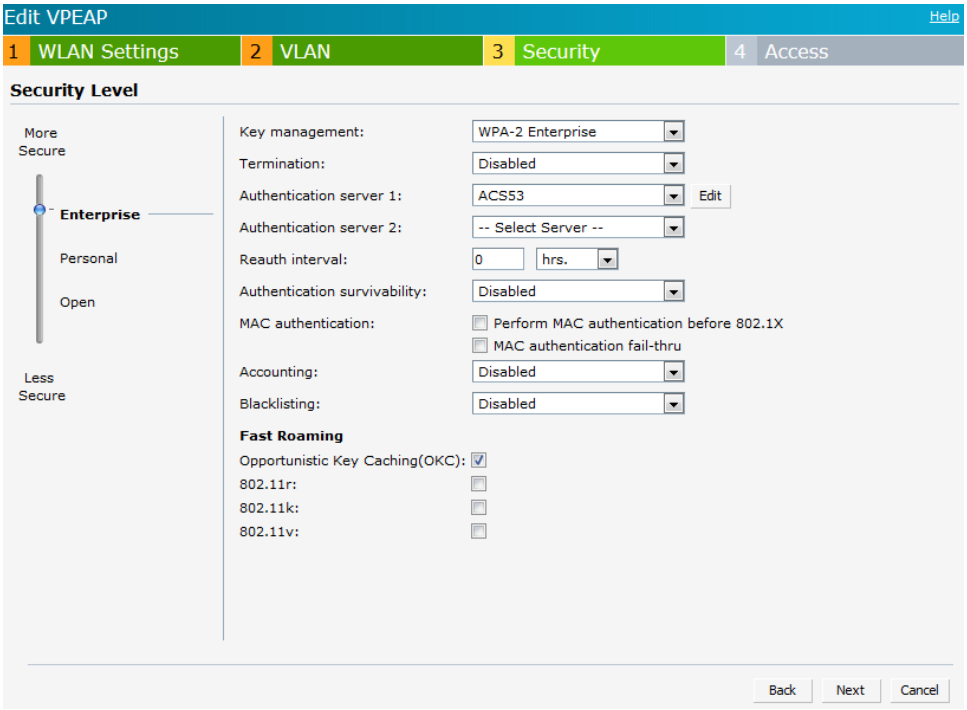
Defining enterprise security

For PEAP, EAP-FAST, or TLS security on the handset, perform the following:

1. On the **Security** tab of the WLAN SSID wizard (or by pressing **Next** from the last section), set the slider to **Enterprise** security level.
2. Select **WPA-2 Enterprise** from the **Key management** drop-down list. (Only WPA-2 Enterprise is supported as a type of Enterprise security on the Spectralink handsets.)
3. To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server, set **Termination** to **Enabled.** See the Aruba Instant User Guide on the Aruba

Network side for more details. VIEW testing was performed with **Termination** set to **Disabled**.

4 Under Fast Roaming, enable **Opportunistic Key Caching (OKC)**.



5 Specify the type of authentication server to use. To configure a new authentication server, select **New** from the **Authentication Server 1** drop-down and configure the following parameters on the **New Server** screen.

a **Name**—Enter the name of the RADIUS server.

b **IP address**—Enter the server IP address.

c Set **RadSec** to **Enabled** to enable secure communication between the RADIUS server and IAP clients by creating a TLS tunnel between the IAP and the server. Fill in the popup with the additional parameters. See the Aruba Instant Access Point User's Guide for more details.

d **Auth port**—Enter the authorization port number of the external RADIUS server. The default port number is 1812.

e **Accounting port**—Enter the accounting port number. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.

f **Shared key**—Enter a shared key for communicating with the external RADIUS server.

g **Retype key**—Re-enter the shared key.

h **Timeout**—Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The IAP retries to send the request several times (as configured in the Retry count), before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.

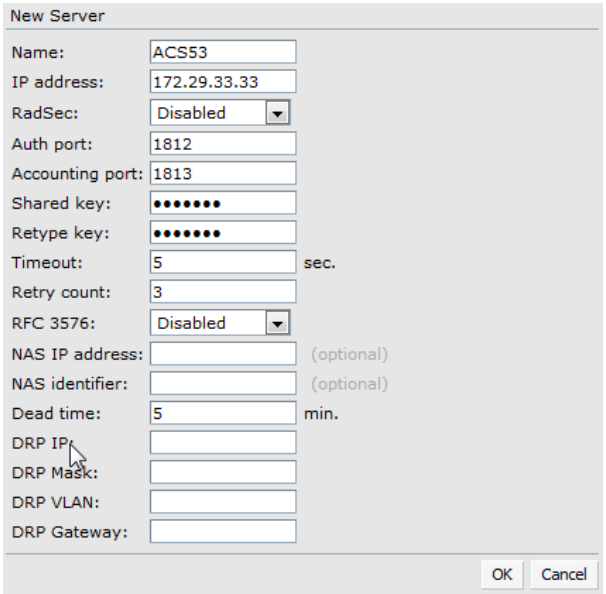
i **Retry count**—Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.

j **NAS IP address**—Allows you to configure an arbitrary IP address to be used as RADIUS Attribute 4, NAS IP Address, without changing source IP Address in IP header of RADIUS packet.

k **Note**: If you do not enter the IP address, the Virtual Controller IP address is used by default when Dynamic RADIUS Proxy is enabled.

l **NAS identifier**—Allows you to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.

m For the other parameters, see the Aruba Instant Access Point User's Guide for more details.

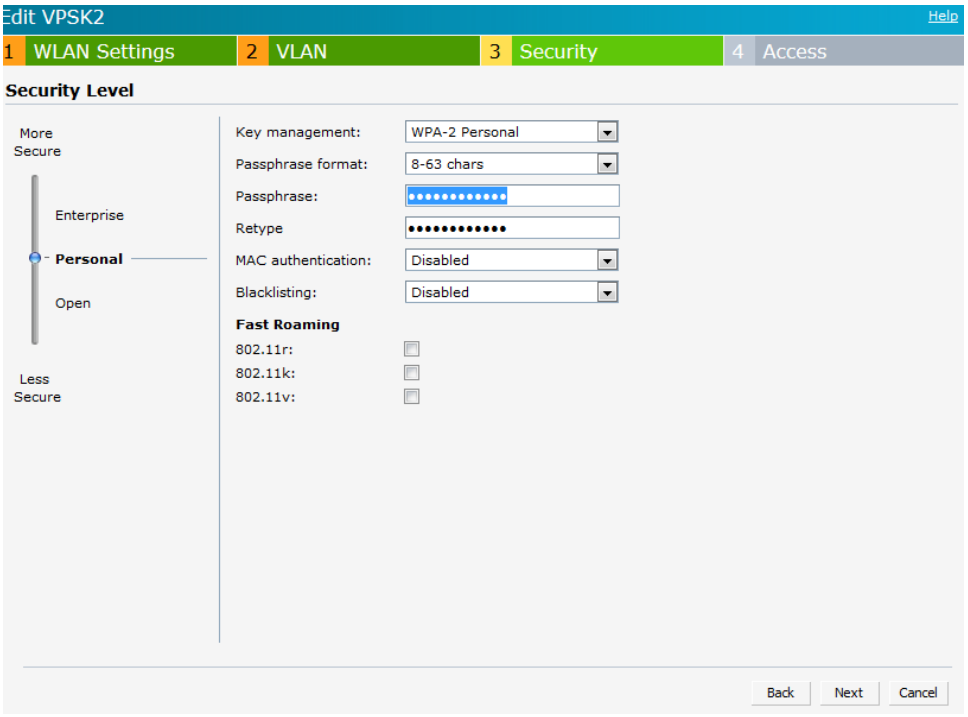


n Click **OK**.

Defining personal security

For WPA2-PSK, WPA-PSK, or WEP security on the handset, perform the following:

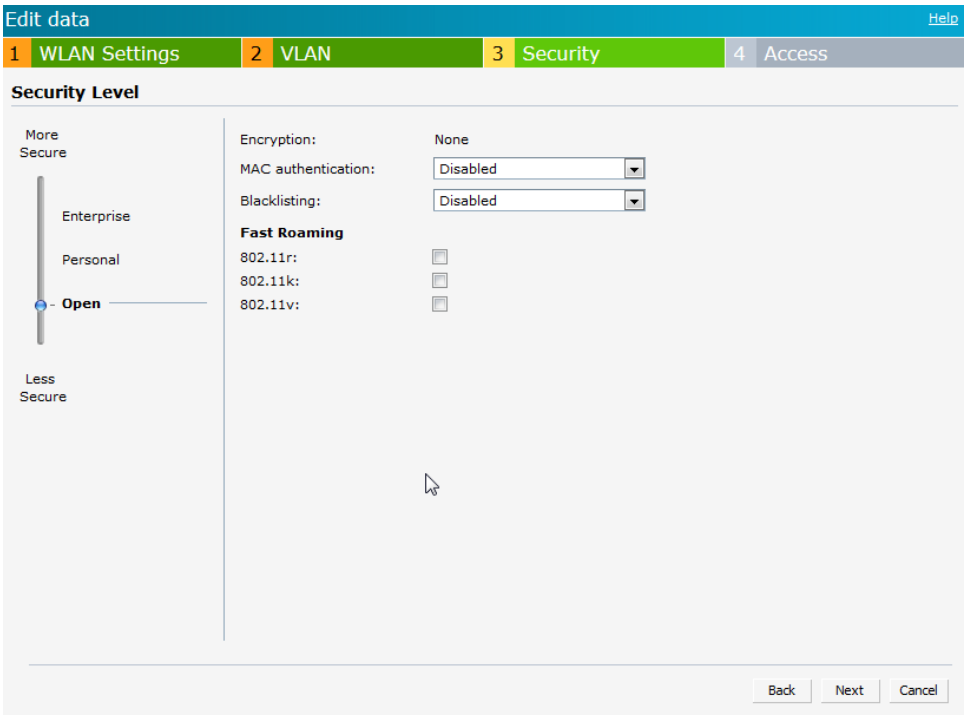
1. On the **Security** tab of the WLAN SSID wizard (or by pressing **Next** from the last section), set the slider to **Personal** security level.
2. From the **Key management** drop-down list, select **WPA-2 Personal** for WPA2-PSK, **WPA-Personal (TKIP Encryption only)** for WPA-PSK, or **Static WEP** for WEP on the handsets.
3. Enter the passphrase or WEP parameters as appropriate. (Note: only index 1 for WEP is supported on the PIVOT handsets. Only Open WEP is supported by the Aruba IAPs.)
4. Do not select any of the fast roaming radio boxes.



Defining open security

For “None” Security on the handset, perform the following:

1. On the **Security** tab of the WLAN SSID wizard (or by pressing **Next** from the last section), set the slider to **Open** security level.
2. Do not select any of the fast roaming radio boxes.



3. After defining the security parameters for the Wireless SSID Profile, click on **Next.**

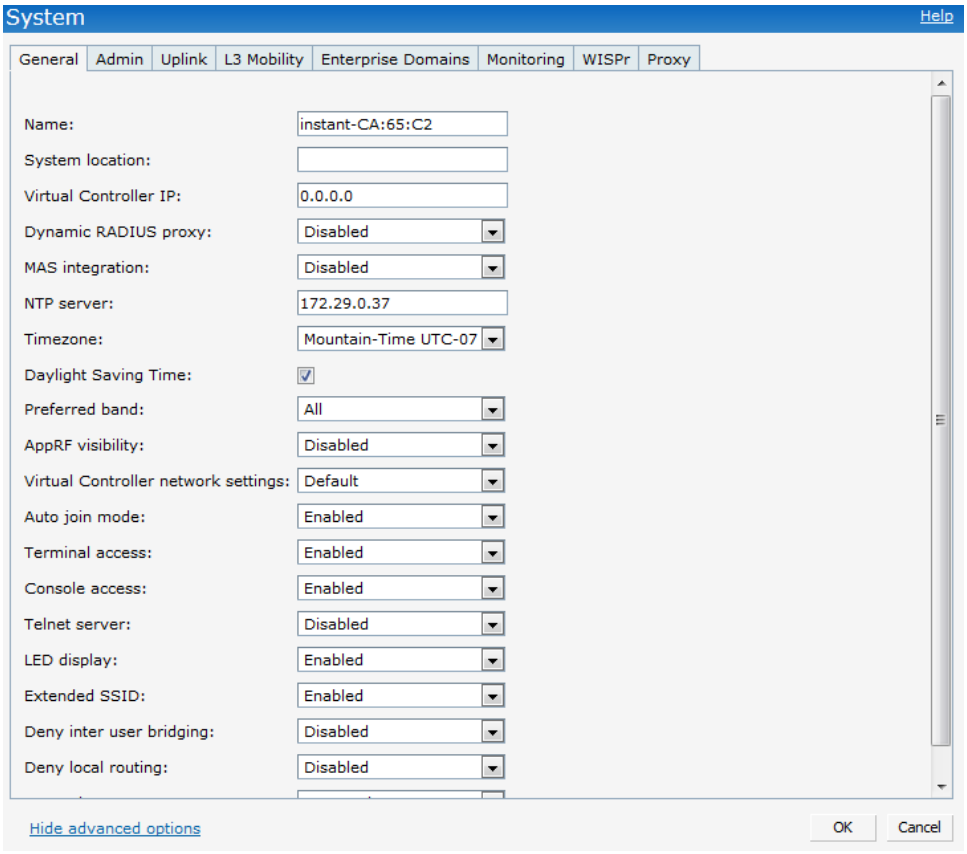
Configuring access settings for a wireless SSID profile

Enter firewall rules and user roles as necessary as appropriate for the network setup. Spectralink phones must have access to the wired network while using DHCP, SIP, IGMP, syslog, TFTP, FTP, HTTP, HTTPS, FTPS, and SNTP to operate correctly.

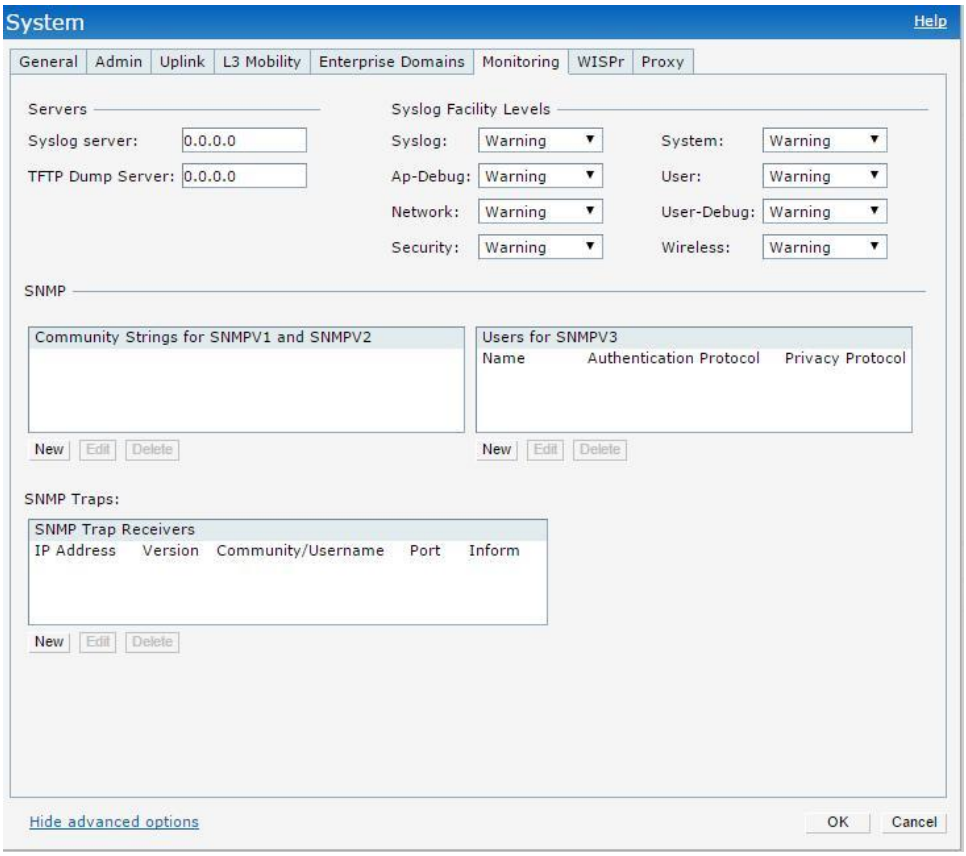
Syslog Server Configuration

To log diagnostics to a syslog server, ensure that the syslog server is configured on the IAP.

1. In the Instant main window, click the **System** link. The **System** window is displayed.
2. Click **Show advanced options** to display the advanced options.



3. Click the **Monitoring** tab. The **Monitoring** tab details are displayed.



In the **Syslog server** text box, enter the IP address of the server to which you want to send system logs.

4 Select the required logging level values for syslog facilities. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog:

AP-Debug— Detailed log about the AP device.

Network— Log about change of network, for example, when a new IAP is dded to a network.

Security— Log about network security, for example, when a client connects using wrong password.

System— Log about configuration and system status.

User— Important logs about client.

User-Debug— Detailed log about client.

Wireless— Log about radio.

5 Click OK.

ARM

The default parameters for ARM and Radio work with the Spectralink phones. It is important to note that **Client Match** is **Disabled** by default and **Airtime fairness mode** is set to **Fair Access**. These are believed to be necessary for proper operation.

One optional setting which is often popular is the ability to use DFS (radar avoidance) channels on the 5 GHz band. To set these up on the IAP in a manner that allows their use with the handsets:

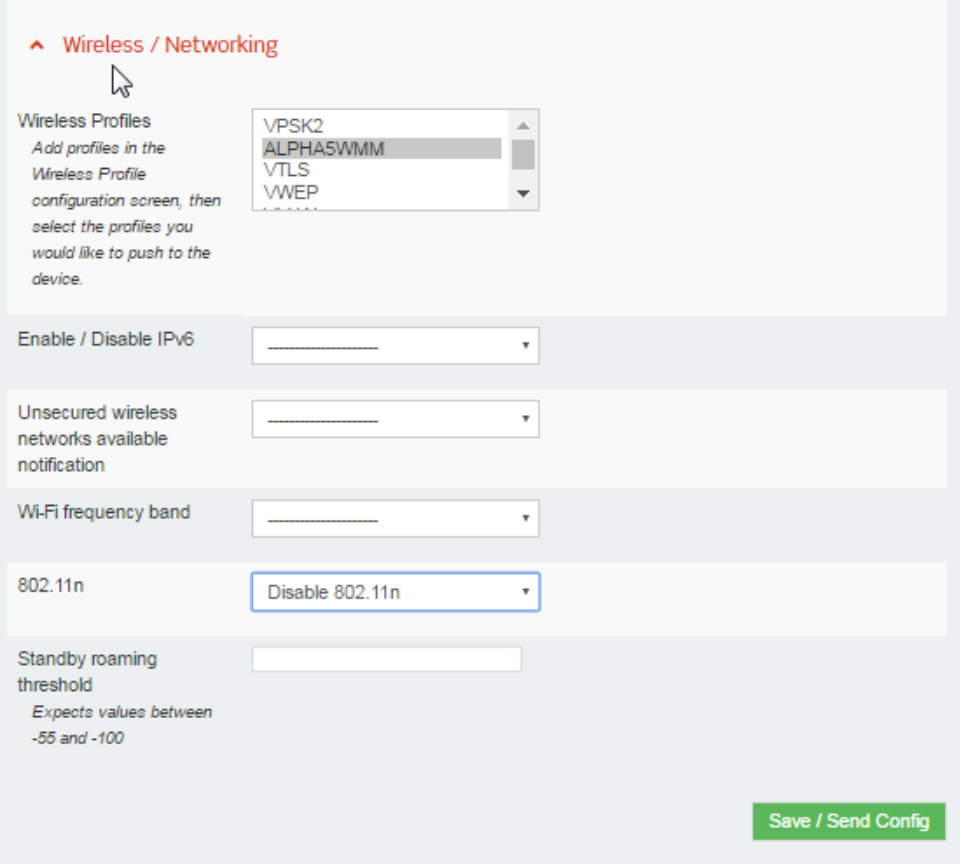
1. Navigate on the **RF** link at the top right on the Instant Access UI.
2. Click on **Show advanced options**.
3. Select the **Radio** tab.
4. In the 5 GHz band section:
   a. Set 802.11d/802.11h to Enabled.
   b. Set Channel switch announcement count to 4.

Set the Handsets into 802.11n Disabled Mode

For the best performance with Aruba-IAPs, 802.11n must be disabled on the handsets. *802.11n is enabled by default on all handsets, so these steps must be performed.*

PIVOT Handsets

1. On a handset by handset basis, disable 802.11n by navigating to **Settings> Admin settings> DEVELOPER OPTIONS> Disable 802.11n** and check the box to disable it.
2. As handsets are initially provisioned individually, the Installation and Configuration Tool (SLIC) has a setting to disable 802.11n, as described in the SLIC Administration Guide in the General Network Configuration section of the wizard. *The recommended method is to disable 802.11n at the time of initial connection to the wireless using SLIC.*
3. If a Configuration Management System (CMS) is installed, 802.11n can be disabled at the Enterprise, Group, or individual device levels. For PIVOT releases of 1.8 or below, consult the Configuration Management System Administration Guide. To disable 802.11n:
   a. Login to the CMS with a username and password that has administrative privileges.
   b. Navigate to **Configure devices>** <choose a device, a group, or enterprise>**> Wireless/Networking**
   c. Select **Disable 802.11n** and touch **Save/Send Config** to send it to the handset(s).



84-Series Handsets

802.11n is disabled on the 84-Series handsets using a configuration file. Configuration files can be provisioned using ftp, tftp, or http. The use of a configuration file is described in the Spectralink 84-Series Wireless Telephone Deployment Guide.

The settings that must be present to disable 802.11n are:

< device.wifi.dot11n.enabled=”0” >

< device.wifi.dot11n.enabled.set=”1” >

< device.set=”1” >

After the 84-Series are provisioned, the current state of the handset is displayed on the Settings> Status> Diagnostics> Wi-Fi Stats> Next screen as shown below:

Important Settings Available Only from CLI

There is an incompatibility between the radio chips in the IAP-11x and the Spectralink handsets in multi-antenna usage on the 2.4 GHz band. It is necessary to use single antenna mode for proper antenna usage.

CLI settings:

1. Access the AP or the virtual controller AP that is the master using ssh or telnet to the AP's IP address or a serial cable to reach the console port. See the *Accessing the Instant CLI* section of the *Instant Access Point User's Guide* on the Aruba website.
2. From the privileged mode, type:

```
rf dot11g-radio-profile
csd-override
exit
exit
commit apply
```

***** END OF DOCUMENT *****