Spectralink VIEW Certified Configuration Guide

Aruba

A Hewlett Packard Enterprise Company

ArubaOS 8.x+

Aruba Controllers (Series) 7000, 7200
Aruba APs: AP-305, AP-31x, AP-33x, AP-505, AP-515, AP-535, AP-555
Copyright Notice

© 2018-2021 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink’s products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient’s personal use, without the express written permission of Spectralink.

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

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

Android is a trademark of Google LLC.

Notice

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

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

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

Warranty

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

Contact Information

<table>
<thead>
<tr>
<th>US Location</th>
<th>Denmark Location</th>
<th>UK Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1 800-775-5330</td>
<td>+45 7560 2850</td>
<td>+44 1344 206591</td>
</tr>
<tr>
<td>2560 55th Street</td>
<td>Bygholm Soepark 21 E Stuen</td>
<td>Suite B1, The Lightbox</td>
</tr>
<tr>
<td>Boulder, CO 80301</td>
<td>8700 Horsens</td>
<td>Bracknell, Berkshire, RG12 8FB</td>
</tr>
<tr>
<td>USA</td>
<td>Denmark</td>
<td>United Kingdom</td>
</tr>
<tr>
<td><a href="mailto:info@spectralink.com">info@spectralink.com</a></td>
<td><a href="mailto:infoemea@spectralink.com">infoemea@spectralink.com</a></td>
<td><a href="mailto:infoemea@spectralink.com">infoemea@spectralink.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction .......................................................................................................................... 5
Certified Product Summary ................................................................................................... 5
Known Limitations ............................................................................................................... 6
Spectralink References ......................................................................................................... 7
  Support Documents ............................................................................................................ 7
  White Papers ..................................................................................................................... 8
Product Support .................................................................................................................. 8
Command, Comment, and Screen Text Key ................................................................. 9

Part I: Deployment Setup ................................................................................................. 10

Chapter 1: Initial Administrative Setup .......................................................................... 11
  Network Topology ............................................................................................................. 11
  Connecting to the Mobility Controller ............................................................................ 12
    Via console ....................................................................................................................... 12
    Via the Command Line Interface (CLI) .......................................................................... 12
    Via the Web interface (WebUI) ...................................................................................... 12
  Initializing the Controller ................................................................................................ 14
  Licensing the Controller .................................................................................................. 16

Part II: Configuration from the WebUI ............................................................................ 19

Chapter 2: WebUI—Configure the Environment .......................................................... 20
  Logical and Physical Interfaces ....................................................................................... 20
    Define a VLAN for voice on the WLAN ..................................................................... 20
    Create a User-Role Derivation Rule ............................................................................ 22
    Create convenience profiles ....................................................................................... 24
    Create passthroughs in the firewall ............................................................................ 26

Chapter 3: WebUI—Configure Wireless Security ....................................................... 28
  Configuration Steps for Open Security and WPA2-PSK ........................................... 28
    Define the authentication profile for no security ......................................................... 28
    Define the authentication profile and 802.1x profile for security WPA2-PSK .......... 29
  Configuration Steps for PEAP and EAP-TLS ............................................................... 33
    Define a Radius Server and Server Group ................................................................. 33
    Define the 802.1x profile and authentication profile for PEAP/EAP-TLS ................. 35
### Chapter 4: WebUI—Configure SSID Profiles and Virtual APs

- **Create SSID Profiles**
- **Create Virtual APs**

### Chapter 5: WebUI: Configure Radio Profiles

### Part III: Configuration from the CLI

### Chapter 6: CLI—Configure the Environment

- **Logical and Physical Interfaces**
- **Define a VLAN for voice on the WLAN**
- **Create passthroughs in the firewall**
- **Create a User-Role Derivation Rule**
- **Define a logging (syslog) server and level if desired**
- **Define a time server if desired**
- **Create convenience profiles**

### Chapter 7: CLI—Configure Wireless Security

- **Configuration Steps for Open Security and WPA2-PSK**
- **Define the authentication profile for no security**
- **Define the authentication profile and 802.1x profile for security WPA2-PSK**
- **Configuration Steps for PEAP and EAP-TLS**
- **Define a Radius Server and Server Group**
- **Define the 802.1x profile and authentication profile for PEAP/EAP-TLS**

### Chapter 8: CLI—Configure SSID Profiles and Virtual APs

- **Create SSID Profiles**
- **Create Virtual APs**

### Chapter 9: CLI—Configure Radio Profiles

### Part IV: The Final Step—Define and Deploy

### Chapter 10: Defining AP Groups and Deploying Them to APs

- **AP Group Definition**
- **Deploying AP Groups to APs**
**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**

<table>
<thead>
<tr>
<th>Manufacturer: Aruba Networks: <a href="http://www.arubanetworks.com">www.arubanetworks.com</a></th>
</tr>
</thead>
</table>
| Certified products: Controllers (Series): Aruba 7000,7200  
Access Points: Aruba 305, 31x, 33x, AP-505, AP-515, AP-535, AP-555 |
| AP Radio(s): 2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n/ac) |
| Security: None, WPA2-PSK, WPA2-Enterprise (PEAPv0/MSCHAPv2 and EAP-TLS) with OKC/802.11r Fast Roaming (FT-enabled) |
| Network topology: Switched Ethernet (recommended) |
| AP and WLC software versions approved: 8.3.0.6, 8.6.0.6 |

**Handset models tested:** Spectralink Versity smartphone* (all models including 92, 95, 96 Series)

| Handset radio mode: 802.11bgn 802.11ac |
| Meets VIEW minimum call capacity per AP: 10** 12** |

**Handset models tested:** Spectralink 84-Series wireless telephone*

| Handset radio mode: 802.11bg 802.11a |
| AP radio mode: 802.11bgn 802.11ac |
| Meets VIEW minimum call capacity per AP: 8** 10** |

**Handset* models tested:** Spectralink 87-Series smartphone (PIVOT)

| Handset radio mode: 802.11bg 802.11a |
| AP radio mode: 802.11bgn 802.11ac |
| Meets VIEW minimum call capacity per AP**: 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”, “smartphones” 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.
- Paired-channel deployment is not recommended on the 2.4 GHz radio by Aruba.
- The Client Match features were tested with the Spectralink handsets. The 84-Series handsets and PIVOT smartphones will act as clients that do not support 802.11v. The Versity handsets advertise that they support 802.11v and respond to the client move commands appropriately. It is recommended to check the VOIP Aware and Client Aware options. Spectralink has not tested the feature in a complex network.
- 84-Series handsets and PIVOT smartphones do not respond to Channel Switch Announcements. Versity smartphones do implement the channel switching standard. Even with channel switching, DFS channels will cause a gap of many seconds when they are switching. When channels are switched, the handsets will perform a Lost AP roam. This may cause audio gaps. For this reason, it is important to deploy network changes in a careful manner. This should be kept in mind when using ARM profiles. ARM maintain or rare scanning is recommended.
- 802.11r is not implemented on the 84-Series handsets or PIVOT smartphones. 802.11r is implemented in Versity models. Turning on both 802.11r and OKC in an SSID-profile allows all models to operate. There is a scenario-specific issue with Versity versions 1.6 and below. If multiple roaming methods are allowed, a workaround in version 1.6 will be activated. The fix for this problem will be released in version 1.7 of the Versity software.
- Spectralink handsets do not support 802.11r when FT is set to Adaptive. Ensure FT is set to enabled on the VQO app to gain 802.11r functionality.
- The 84-Series handsets and 87-Series smartphones should be operated with 802.11n disabled on the handsets for best overall network performance.
- Management Frame Protection is available in the Versity handsets but not in the 84-Series handsets or 87-Series smartphones.
- Aruba no longer supports the WMM-AC (TSPEC) method for controlling priority/bandwidth use in the network. The Versity phones also do not support the WMM-AC method. Other Aruba methods, outside of the scope of this document, must be used for bandwidth planning to ensure that the packets for audio/video calls are not delayed.
• Currently for Versity, multicast must be set up to send traffic for the PTT multicast address on all switch ports that may be connected to Versity smartphones without expecting query responses.

**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**

*Versity Deployment Guide* describes how to distribute Versity phones in a large environment using the Spectralink SAM (Spectralink Application Management) server and a Third-Party EMM (Enterprise Mobile Management) server.
CS-18-07 Spectralink Versity Manual Deployment is a white paper describing how to distribute Versity phones for a small deployment using phone menus.

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.

PIVOT by Spectralink Configuration Guide The PIVOT Configuration Guide provides detailed information about PIVOT menu items that have been developed specifically for the PIVOT handset.

Spectralink 87-Series Smartphone 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 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


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 challenges of ensuring excellent voice quality in a Wi-Fi workplace and 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

Note: Not covered: Radius server, complex firewall setup, and bandwidth control

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise security types. It does not cover complex firewall or user role definitions. It does not cover bandwidth usage planning. Contact Aruba support for help in these areas.

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.
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.

<table>
<thead>
<tr>
<th>Text Style</th>
<th>Denotes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxxxxx</td>
<td>Typed command</td>
</tr>
<tr>
<td>&lt;xxxxxxxxx&gt;</td>
<td>Encryption key, domain name or other information specific to your system that needs to be entered</td>
</tr>
<tr>
<td>(xxxxxxxxx)</td>
<td>Comment about a command or set of commands</td>
</tr>
<tr>
<td>xxxxxxxx</td>
<td>Prompt, system response or other displayed information</td>
</tr>
<tr>
<td>SL_aaa_bbbb</td>
<td>Profile configurations on the Aruba added to support the Spectralink handsets. aaa represents the profile type (i.e. rp for radio profile) and bbbb is a description. “_” characters are specific to defined configurations.</td>
</tr>
<tr>
<td>aaa-bbbb</td>
<td>CLI keywords are denoted with lower case letters connected by hyphens (“.”) to differentiate keywords from configurations.</td>
</tr>
</tbody>
</table>
Part I: Deployment Setup
Chapter 1: Initial Administrative Setup

Network Topology

Note: Example configuration shown
This is a modified diagram and not all components are shown for every system type.
Connecting to the Mobility Controller

Via console

Using a standard RS-232 cable, connect the Aruba mobility controller to the serial port of a terminal or PC.

Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

Use this mode of connection during the initialization phase of the controller to configure login credentials.

1. Press Enter to display the Aruba mobility controller login screen.
2. Enter the default login: admin and the default password: admin. These are case sensitive.
3. Enter enable and the default password: enable to get into the command mode.

Via the Command Line Interface (CLI)

By default, only SSH (Secure Shell) access to the switch (mobility controller) is permitted.

1. From a management system that has network connectivity to the switch, connect to the switch using SSH:
   
   ```bash
   ssh admin@<switch IP address>
   ```

2. Enter the admin password at the password prompt:
   
   Type enable at the > prompt to enter the enable mode.

3. Type the enable password when prompted for a password.

Via the Web interface (WebUI)

Once the connectivity to the switch is verified, open a Web browser and enter the switch's IP address in the navigator bar.

The switch can be accessed using http at

```
http://<switch IP Address> :4343
```

or https at

```
https://<switch IP Address> :4343.
```
The user is prompted with the username and password configured (in the example above, the username/password configured is admin/admin). On successful login the following Dashboard screen is displayed.
Initializing the Controller

When powered up from a factory default state, the controller will present the following screen on the serial console. Please fill in basic network details when prompted. The following is a sample of the information presenting which may vary depending on the controller model and software version:

Example
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...

'enable-debug' : Enable auto-provisioning debug logs
'disable-debug' : Disable auto-provisioning debug logs
'mini-setup' : Start mini setup dialog. Provides minimal customization and requires DHCP server
'full-setup' : Start full setup dialog. Provides full customization
'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for master information

Enter Option (partial string is acceptable):
full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes

***************** Welcome to the Aruba7010 setup dialog *****************
This dialog will help you to set the basic configuration for the switch. These settings, except for the Country Code, can later be changed from the Command Line Interface or Graphical User Interface.

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help <ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end <ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line <ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

Enter System name [Aruba7010]: VIEWAruba7010
Enter Switch Role (standalone|md) [md]: standalone
Enter Controller VLAN ID [1]:
Enter Controller VLAN port [GE 0/0/0]: GE 0/0/16
Enter Controller VLAN port mode (access|trunk) [access]:
Enter VLAN interface IP address [172.16.0.254]: 172.29.109.108
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.128
Enter IP Default gateway [none]: 172.29.109.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: America/Denver
Enter Time in UTC [18:57:07]: 13:03:03
Enter Date (MM/DD/YYYY) [9/18/2018]: 
Enter Password for admin login (up to 32 chars): ********
Re-type Password for admin login: ********

Current choices are:

System name: VIEWAruba7010
Switch Role: standalone
Controller VLAN id: 1
Controller VLAN port: GE 0/0/16
Controller VLAN port mode: access
VLAN interface IP address: 172.29.109.108
VLAN interface subnet mask: 255.255.255.128
IP Default gateway: 172.29.109.1
Option to configure VLAN interface IPV6 address: no
Country code: US
IANA Time Zone: America/Denver

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
Creating configuration... Done.

System will now restart!
**Licensing the Controller**

A license for the Next Generation Policy Enforcement Firewall Module must be installed for the firewall features and Spectralink voice prioritization to work. Please contact your local Aruba representative. License Management can be performed using the License Wizard of the WebUI.

You will need

- The Serial Number of the Mobility Controller.
- The License Certificate Number of the service to be activated (Please contact your local Aruba team).

Obtain the license Key from: [https://licensing.arubanetworks.com](https://licensing.arubanetworks.com)

**On the WebUI**

1. On the hierarchy status bar, select the topmost level **Mobility Controller**.

2. Click **Configuration > System**.

3. Click the **Licensing** tab.

4. Expand **Inventory**.
5. Click the + to add a new license.

6. Enter the license Key in the space provided and click OK.

**Install Licenses**

To install new licenses you will need:

- The Serial Number of this Mobility Controller: CG0021300
- The License Key for each service you wish to activate
- License Passphrase: Command is not supported for this platform

Obtain License Keys from HPE Aruba My Networking Portal

Enter the license keys in the text box below, one key per line.

7. Repeat 5 and 6 for all the licenses desired.

8. Navigate up to the Usage screen and check each box for each license added so that it will be placed into service.
9  Click **Submit**.

10  Centralized Licensing and a license server may also be used. See the Aruba User’s Guide for details.
Part II: Configuration from the WebUI

Admin Tip: Confirmation step
After configuring a setting and clicking Submit, in order for the said changes to be applied, the steps shown here should be completed.

While using the WebUI, the procedure is:

1. Configure the item.

2. Click Submit.

3. Click Pending Changes.

4. Select Deploy changes.

The configuration is not final until these steps are completed.

These steps are omitted in the following sections for brevity.
Chapter 2: WebUI—Configure the Environment

Note See Admin tip at the start of this section

Admin tip: Part II: Configuration from the WebUI

Logical and Physical Interfaces

This section defines the Layer 2/3 framework that connects the Spectralink phones with the WLAN Mobility Controller (MC) and the Access Points.

Spectralink requirement

The Spectralink phones and Spectralink infrastructure must be connected over Layer-2 and have the L2 subnet span across L3 switching/routing fabric.

Some profiles used for convenience are also defined in this section.

Define a VLAN for voice on the WLAN

1. Click the Configuration item on the left menu.
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller> <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. On the left pane, click Interfaces.
   On the upper menu Click VLANs.

3. Click the default VLAN line.(Other VLAN’s may be entered here: see Aruba documentation for details.)
4 Enter details for the VLAN on which the phones are desired – **VLAN ID/Range, VLAN name**. Click the new line representing the VLAN.

5 Set **VLAN IDs:**

![VLAN Configuration](image)

a **IPv4 Address** Enter an IP address for the VLAN interface on the controller and the subnet mask. (Please bear in mind that L2 connectivity is required for the phones to reach the voice server and gateway).

i Add a **DHCP helper** if an external DHCP server will be used to supply addresses to the phones

ii Uncheck the **Suppress ARP** radio box so that phones may use the proxy ARP feature.
iii  Expand the IGMP item. Choose proxy from the dropdown list and list the interface or port channel through which the controller is connected to the switch so that IGMP messages will be passed through.

b  Click Port Members > Edit to choose the ports assigned to the VLAN (default is all available ports).

Create a User-Role Derivation Rule

1  Click Configuration on the left navigation menu.
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller > <controller-name> on the status bar so that the configuration is occurring at the correct level.

2  Click Authentication.

3  Click User Rules and Click the plus sign to add.
4 Type a name for the user rule, such as spectralink.

5 Click **Submit**.

6 Click the newly entered name in the tree in the table.

7 Click **Add**.

8 Fill the following parameters
   a Set Type – Role
   b Rule Type – MAC Address
   c Condition – starts with Value=00:90:7a
   d Roles – authenticated.
   e Description – Allow all protocols
   f Click **Submit**.
Create convenience profiles

Some profiles are created for convenience in later use.

Create SL_11r_off and SL_11r_on

1. Navigate to Configuration > System > Profiles
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller > <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Under All Profiles, expand Wireless LAN.

3. Expand 802.11r.

4. Click the plus sign under 802.11r Profile: New Profile.

5. Define a profile with a name such as SL_11r_on. For the on profile, check the Advertise 802.11r Capability. For the off profile, uncheck Advertise 802.11r Capability.
Create SL_arm_maintain

1. Under All Profiles, expand Adaptive Radio Management
2. Click the plus sign under Adaptive Radio Management (ARM) profile: New Profile and expand the General item.
   a. Profile name – in this example SL_arm_maintain is used.
   b. Assignment – choose maintain
   c. The other values can be set as desired for the network wireless cell design.
   d. Click Submit
3. Expand the **Scanning** item. Uncheck the **Scanning** radio box.

**Create SL_scan**

1. Navigate to **All Profile > RF Management > AM Scanning**
2. Under **AM Scanning profile: New Profile** Click the plus sign.
3. **Scan Mode** – select rare.

**Create passthroughs in the firewall**

---

**Note: Adapt the VIEW test facility firewall example to your facility**

In the section below, the firewall passthroughs are applied to the overall system. In an actual facility, firewall values would be role-based. Allow the necessary servers/ports through the firewall at the role level rather than at the general level as shown.

The SIP server and provisioning servers must be able to pass through the firewall. There are different ways to accomplish this. These are beyond the scope of this document. Here is a simple approach for a few items used in VIEW testing.

1. Navigate to **Configuration > Services**.
2. Click the **Firewall** tab.
3. Scroll down and expand **ACL White List**

4. Click the plus sign.
5. The example below is for UDP packets for a SIP server located at 172.29.109.109
6. The same screen with a protocol of 17 opens a TCP Sip call.

7. The ftp provisioning server can be pushed through the firewall by selecting a protocol value of ftp from the IP protocol number dropdown.
Chapter 3: WebUI—Configure Wireless Security

Note See Admin tip at the start of this section
Admin tip: Part II: Configuration from the WebUI

Configuration Steps for Open Security and WPA2-PSK

Define the authentication profile for no security

1. Navigate to Configuration and Authentication.
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller> <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Click the AAA Profiles tab.

3. Expand the AAA item.

4. Click the plus sign under AAA Profile: New Profile.
   a. Enter a Profile name (SL_ap_data in this example).
Set the Initial role to **authenticated** from the dropdown.

Define the authentication profile and 802.1x profile for security WPA2-PSK

1. Navigate to **Configuration** and **Authentication**. Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller> <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Click the **AAA Profiles** tab.

3. Expand the **AAA** item.
4 Click the plus sign under **AAA Profile: New Profile**.
   a Enter a Profile name (SL_ap_VPSK2 in this example).
   b Set the Initial role to **logon** from the dropdown.
   c Set the MAC Authentication Default Role to logon.
   d Set the 802.1X Authentication Default Role to logon.
   e Set the **User derivation rules** to the role defined above in the User derivation rules section, here **spectralink**.
   f Click Submit.
5 Click **802.1X Authentication Profile** in the middle-pane with the new profile highlighted to expand the tree and click **default-psk** from the dropdown list. Note: this assumes no changes have been made to the factory default **default-psk** profile.
Configuration Steps for PEAP and EAP-TLS

Define a Radius Server and Server Group

1. Navigate to Configuration and Authentication.
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller-><controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Click the Auth Servers tab.

3. Click the plus sign in the All Servers group to add a new server.
   a. Enter the Name, IP address/hostname, and Type.
   b. Click Submit.

4. Back on the All Servers table, Click the row for the authentication server entered and enter appropriate Server Options. Click Submit when finished.
In the **Server Groups** table, click the plus sign and create a new server group (example RadiusServers) or use the default server group.

Click the plus in the **Server Group** <server group name> table.

Assign the required RADIUS server under Server Name, click **Add Server** and **Apply** button.
8 Drag rows to reorder the authentication servers as necessary.

Define the 802.1x profile and authentication profile for PEAP/EAP-TLS

1 Navigate to Configuration and Authentication.
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller-><controller-name> on the status bar so that the configuration is occurring at the correct level.

2 Click the L2 Authentication tab.

3 Expand the 802.1X Authentication item.

4 Click the plus sign under 802.1X Authentication Profile: New Profile.
   a Enter a Profile name (SL_a1X_VPEAP in this example).
   b Set the Machine Authentication: Default Machine Role to authenticated.
   c Set the Machine Authentication: Default User Role to authenticated.
5 Scroll down and add `eap-tls` and `eap-peap` for the TERMINATION EAP-TYPE and `eap-mschapv2` and `eap-gtc` for TERMINATION INNER EAP-TYPE.
6 Ensure that the Termination radio box is unchecked.
7 Navigate to **Configuration** and **Authentication**.
8 Click the **AAA Profiles** tab.
9 Expand the **AAA** item.

![Configuration and Authentication](image)

10 Click the plus sign under **AAA Profile: New Profile**.
   a Enter a Profile name (SL_ap_VPEAP in this example).
   b Set the Initial role to **logon** from the dropdown.
   c Set the 802.1X Authentication Default Role to authenticated.
   d Set the **User derivation rules** to the role defined above in the User derivation rules section, here **spectralink**.
   e Click Submit.
11. Click **802.1X Authentication Profile** in the middle-pane with the new profile highlighted to expand the tree. Then click the 802.1X profile defined in the beginning for the PEAP/EAP-TLS section from the dropdown list (SL_a1x_VPEAP in this example). Click Submit to accept.

12. Underneath the authentication profile created just above (SL_ap_VPEAP in this example), highlight the **802.1X Authentication Server Group**. Select the server group created above from the dropdown list.
Chapter 4: WebUI—Configure SSID Profiles and Virtual APs

Note See Admin tip at the start of this section
Admin tip: Part II: Configuration from the WebUI

Create SSID Profiles

1. Navigate to Configuration> System> Profiles
   Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller> <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Under All Profiles, expand Wireless LAN.

3. Scroll down to SSID and expand it.

4. Click the plus sign under AAA Profile: New Profile.
   Common to all security types (leave values not mentioned at their defaults):
   a. Enter a Profile name.
   b. Check SSID enable
   c. Enter an ESSID. This will be the name shown on the wireless, if it is not hidden.
   d. Leave 1 in the DTIM interval.
   e. Check 6, 12, and 24 for 802.11a Basic Rates.
   f. Check all the 802.11a Transmit Rates.
   g. Check 5, 11, and 24 for 802.11g Basic Rates.
   h. Check all of the 802.11g Transmit Rates except for 1 and 2.
   i. Check Wireless Multimedia (WMM).
   j. Enter 46 for DSCP mapping for WMM voice AC.
   k. Enter 40 for DSCP mapping for WMM video AC.
   l. Enter 0 for DSCP mapping for WMM best-effort AC.
   m. Enter 1 for DSCP mapping for WMM background AC.
   n. Choose voice from the dropdown for WMM Access Class of EAP traffic.
5 For Open security:
   a Under encryption, check `openssl`

6 For WPA2-PSK
   a Under encryption, check `wap2-psk-aes`.
   b Enter and Retype either a WPA Hexkey or a WPA Passphrase.

7 For PEAP or EAP-TLS
   a Check `wpa2-aes` for the encryption.

8 Click Submit
9 In the **All Profiles** list, expand the newly entered SSID profile

10 Choose the 802.11r profile that has 802.11r on.

![Profiles screen](image-url)

**Note:** Ensure EDCA Parameters are set to None

If the SSID profile is started from a factory default state, the EDCA parameters profiles within the SSID profile will default to None. The phones will not try to apply WMM_AC in this case. But if the profile has been imported from an earlier version of the Aruba OS, there may be values in these profiles. They must be off for proper handset/OS interaction.
Create Virtual APs

1. Navigate to Configuration > System > Profiles
2. Under All Profiles, expand Wireless LAN > Virtual AP.
3. Click the plus sign under Virtual AP profile: New Profile.
   a. Profile name – enter a profile name SL_vap_data in this example
   b. Convert Broadcast ARP requests to unicast – uncheck this item
   c. Click Submit
4. Expand the new virtual AP profile by clicking on the row with its name, then expand the RF item on the right pane.
   a. Uncheck Band Steering (band steering will delay probe responses, causing slow roaming)
   b. Click Submit
Chapter 5: WebUI: Configure Radio Profiles

Note See Admin tip at the start of this section

Admin tip: Part II: Configuration from the WebUI

Spectralink recommends obtaining a site survey and using the results to design channel assignments, channel widths, and transmit power settings rather than using automated scanning approaches. An audio or video call requires consistent small bandwidth packet delivery. When an AP goes off channel to scan or changes power or channel assignments, the steady stream is interrupted. The resultant gap is audible. The handsets do not have channel switch announcements implemented. A dropout occurs when changes are deployed.

Thus, many individual radio profiles should be defined. These should be assigned to APs using knowledge of the characteristics of the AP’s location.

1. Navigate to **Configuration > System > Profiles**
   - Ensure that you are on the lowest level of the hierarchy, i.e. Mobility Controller> <controller-name> on the status bar so that the configuration is occurring at the correct level.

2. Navigate to **RF Management** and expand it.

3. Navigate to **2.4 GHz radio** or **5 GHz radio** as desired.

4. Click the plus sign under **2.4 GHz radio profile** or the **5 GHz radio profile: New Profile**.
   - a. Give the profile a name that will aid in assigning it to APs.
   - b. Enter a Channel value.
   - c. Enable the radio and choose bandwidth and EIRP settings as determined by the site survey.
   - d. Click **Submit**.
5 Highlight the newly created radio profile name and expand the Advanced item.
   a Check Enable CSA. This is necessary to allow DFS channels to be used (5 GHz channels only).
   b Check Advertise 802.11d and 802.11h Capabilities.
   c Click Submit.
6. Expand the newly created radio profile name.

   a. In the Adaptive Radio Management (ARM) hierarchy item, select the `SL_arm_maintain` profile created in the Environment section or other maintain ARM profile.
b In the **AM Scanning** hierarchy item, select **SL_Scan** or other rare scanning protocol.

![Image of AM Scanning hierarchy with SL_Scan selected]

**Note: Go to the Final Step**

The last step – applying Virtual APs and radio profile to AP groups and deploying them to APs – is described the Chapter 10: The Final Step.
Part III: Configuration from the CLI
Chapter 6: CLI—Configure the Environment

Logical and Physical Interfaces

This section defines the Layer 2/3 framework that connects the Spectralink phones with the WLAN Mobility Controller (MC) and the Access Points.

Spectralink requirement

The Spectralink phones and Spectralink infrastructure must be connected over Layer-2 and have the L2 subnet span across L3 switching/routing fabric.

Some profiles used for convenience are also defined in this section.

Define a VLAN for voice on the WLAN

```plaintext
interface gigabitethernet 0/0/16
    description "GE0/0/16"
    trusted
    trusted vlan 1

interface vlan 1
    ip address 172.29.109.108 255.255.255.128
    ip helper-address 172.29.109.4
    no suppress-arp
    ip igmp proxy gigabitethernet 0/0/16

Create passthroughs in the firewall

Note: Adapt the VIEW test facility firewall example to your facility

In the section below, the firewall passthroughs are applied to the overall system. In an actual facility, firewall values would be role-based. Allow the necessary servers/ports through the firewall at the role level rather than at the general level as shown.

```
(tcp for Sip server)
  ipv4 permit 172.29.109.15 255.255.255.255 proto 6 ports 21 21
(NTP server, ftp background data)
  ipv4 permit 172.29.109.10 255.255.255.255 proto 6 ports 21 21
(ftp client, ftp server for 8400s)

Create a User-Role Derivation Rule
!
  aaa derivation-rules user spectralink
  set role condition macaddr starts-with "00:90:7a" set-value authenticated
description "Allow all protocols"

Define a logging (syslog) server and level if desired

Other
!
  logging network subcat all level warnings
  logging network subcat mobility level warnings
  logging system subcat all level warnings
  logging wireless subcat all level warnings
  logging 172.29.109.109 format bsd-standard type user severity warnings
  facility local0
  logging 172.29.109.109 format bsd-standard type network severity warnings
  facility local0
  logging 172.29.109.109 format bsd-standard type wireless severity warnings
  facility local0

Define a time server if desired

ntp server 172.29.0.37

Create convenience profiles
!
  wlan dot11r-profile "SL_11r_on"
    dot11r
    !
  wlan dot11r-profile "SL_11r_off"
  !
  rf arm-profile "SL_arm_maintain"
    assignment maintain
    min-tx-power 3
    max-tx-power 3
    no scanning
    !
  rf am-scan-profile "SL_scan"
    scan-mode rare
Chapter 7: CLI—Configure Wireless Security

Configuration Steps for Open Security and WPA2-PSK

Define the authentication profile for no security

```
!  
aaa profile "SL_ap_data"
    initial-role "authenticated"
```

Define the authentication profile and 802.1x profile for security WPA2-PSK

```
!  
aaa profile "SL_ap_VPSK2"
    mac-default-role "logon"
    authentication-dot1x "default-psk"
    dot1x-default-role "logon"
    user-derivation-rules "spectralink"
```

Configuration Steps for PEAP and EAP-TLS

Define a Radius Server and Server Group

```
!  
aaa authentication-server radius "EXTRadius"
    host "172.29.65.18"
    key dd6579db8e4131df7b86b0f1d4e05d6c

!  
aaa server-group "RadiusServers"
    auth-server EXTRadius position 1
```

Define the 802.1x profile and authentication profile for PEAP/EAP-TLS

```
!  
aaa authentication dot1x "SL_alx_VPEAP"
    machine-authentication machine-default-role "authenticated"
    machine-authentication user-default-role "authenticated"
    termination eap-type eap-tls
    termination eap-type eap-peap
    termination inner-eap-type eap-mschapv2
    termination inner-eap-type eap-gtc
```
aaa profile "SL_ap_VPEAP"
  authentication-dot1x "SL_alx_VPEAP"
  dot1x-default-role "authenticated"
  dot1x-server-group "RadiusServers"
  user-derivation-rules "spectralink"
Chapter 8: CLI—Configure SSID Profiles and Virtual APs

Create SSID Profiles

```
! wlan ssid-profile "SL_sp_data"
  essid "data"
  g-basic-rates 5 11 24 36 48 54
  g-tx-rates 5 6 9 11 18 24 36 48 54
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "0"
  wmm-bk-dscp "1"
  wmm-eap-ac voice
!
```

```
wlan ssid-profile "SL_sp_VPEAP"
  essid "VPEAP"
  opmode wpa2-aes
  g-basic-rates 5 11 24
  g-tx-rates 5 6 9 11 12 18 24 36 48 54
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "0"
  wmm-bk-dscp "1"
  wmm-eap-ac voice
  qbss-load-enable
  dot11r-profile "SL_11r_on"

!
```

```
wlan ssid-profile "SL_sp_VPSK2"
  essid "VPSK2"
  opmode wpa2-psk-aes
  g-basic-rates 5 11 24
  g-tx-rates 5 6 9 11 12 18 24 36 48 54
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "0"
  wmm-bk-dscp "1"
  wmm-eap-ac voice
  wpa-passphrase b0d0583c5d6a1af5c5b097c7a90eb0381d239eb4d20c35e6
  qbss-load-enable
```
Create Virtual APs

wlan virtual-ap "SL_vap_data"
    aaa-profile "SL_ap_data"
    ssid-profile "SL_sp_data"
    no openflow-enable
    no broadcast-filter arp

wlan virtual-ap "SL_vap_VPEAP"
    aaa-profile "SL_ap_VPEAP"
    ssid-profile "SL_sp_VPEAP"
    no openflow-enable
    no broadcast-filter arp

wlan virtual-ap "SL_vap_VPSK2"
    aaa-profile "SL_ap_VPSK2"
    ssid-profile "SL_sp_VPSK2"
    no openflow-enable
    no broadcast-filter arp
Chapter 9: CLI—Configure Radio Profiles

Spectralink recommends performing network changes during low usage periods. An audio or video call requires consistent small bandwidth packet delivery. When an AP goes off channel to scan or changes power or channel assignments, the steady stream is interrupted. The resultant gap is audible. The 84-Series handsets and PIVOT smartphones do not have channel switch announcements implemented, increasing the length of the gap. A dropout occurs when changes are deployed.

```
! rf dot11a-radio-profile "SL_rp_315_Main_Floor_a"
csa
dot11h
  arm-profile "SL_arm_maintain"
  am-scan-profile "SL_scan"
eirp-min 3
eirp-max 3
!
rf dot11a-radio-profile "SL_rp_325_Main_Floor_a"
csa
dot11h
  arm-profile "SL_arm_maintain"
  am-scan-profile "SL_scan"
!
rf dot11g-radio-profile "SL_rp_315_Main_Floor_g"
csa
dot11h
  arm-profile "SL_arm_maintain"
  am-scan-profile "SL_scan"
!
rf dot11g-radio-profile "SL_rp_325_Main_Floor_g"
  no high-throughput-enable
dot11h
  arm-profile "arm-maintain"
  am-scan-profile "SL_scan"
```
Part IV: The Final Step—Define and Deploy
Chapter 10: Defining AP Groups and Deploying Them to APs

Now that radio profiles and Virtual APs are defined, they are assigned to AP-groups. The WebUI approach to this uses regulatory domain profiles instead of radio profiles. Voice clients are better served by a network that changes slowly. If it is necessary to assign specific channels, it is more convenient to define the AP groups using cli.

**AP Group Definition**

Here are some examples.

```
ap-group "SL_apg_315_Main_Floor"
    virtual-ap "SL_vap_data"
    virtual-ap "SL_vap_VPSK2"
    virtual-ap "SL_vap_VPEAP"
    dot11a-radio-profile "SL_rp_315_Main_Floor_a"
    dot11g-radio-profile "SL_rp_315_Main_Floor_g"

nap-group "SL_apg_325_Main_Floor"
    virtual-ap "SL_vap_data"
    virtual-ap "SL_vap_VPSK2"
    virtual-ap "SL_vap_VPEAP"
    dot11a-radio-profile "SL_rp_325_Main_Floor_a"
    dot11g-radio-profile "SL_rp_325_Main_Floor_g"
```

**Deploying AP Groups to APs**

There are many ways to enter APs into the system. Some ways provide increased security. The method present here is a basic one. Other methods can be found in the Aruba support documentation.

1. Enter the MAC addresses of the APs into the Campus Whitelist.
   a. Navigate to Configuration> Access Points
   b. Click Campus AP Whitelist tab, then click the plus sign
   c. MAC address – enter the MAC address printed on the label of the AP
   d. AP name – give the AP a memorable name
   e. AP group – choose a group from the dropdown list
1. **Description** – enter a description if desired

2. Check the box beside the AP in the whitelist and Click **Approve**

3. Following one of the methods in Aruba support documentation, power cycle the AP and allow it to find the controller

****END OF DOCUMENT****