



Spectralink VIEW Certified Configuration Guide

ExtremeCloud IQ

AP's 302w, 305c, 305cx, 410c, 460c, 510c and 510cx

Copyright Notice

© 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

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 1344 206591

Spectralink Europe Aps—UK branch
Suite B1, The Lightbox
Bracknell, Berkshire, RG12 8FB
United Kingdom

infoemea@spectralink.com

Contents

- Chapter 1: Introduction 4**
 - Certified Product Summary4
 - Known Limitations.....5
 - Spectralink References6
 - Support Documents*6
 - Product Support7

- Chapter 2: Overview 8**
 - Network Topology8

- Chapter 3: Setting Up Your Cloud Network 9**
 - Login and AP Onboarding9
 - Create a Network Policy.....11
 - Add APs to the Network Policy12

- Chapter 4: Configure SSIDs 14**
 - Define the SSIDs14
 - SSID Usage* 15
 - Additional SSID settings (can be applied to SSIDs of all Usage types)*..... 17
 - Additional Settings (Applied to Network Policy)* 19
 - Radio settings20

- Chapter 5: Firmware Upgrades 23**

Chapter 1: 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 ExtremeCloud IQ products listed have been tested in the Spectralink lab and found to be interoperable as noted.

Certified Product Summary

Manufacturer:	Extreme Networks
Certified products:	ExtremeCloudIQ-Controlled APs 302w, 305c, 305cx, 410c, 460c, 510c and 510cx
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n/ac/ax)
Security:	None, WEP, WPA2-PSK, WPA2-Enterprise (PEAPv0/MSCHAPv2, and EAP-TLS) with OKC, 802.11r (FT-enabled)
QoS:	Wi-Fi Standard for Spectralink 84 series, Versity92/95/96
Network topology:	Bridged
Version approved:	10.1.4*

<i>Handset* models tested:</i>	<i>Spectralink</i>			<i>Smartphone (Versity)</i>
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a, 802.11n & 802.11ac
Meets VIEW minimum call capacity per AP**	8	8	8	10

<i>Handset models tested:</i>	<i>Spectralink</i>			<i>Wireless Telephone (84-Series)</i>
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a, 802.11n & 802.11ac
Meets VIEW minimum call capacity per AP**	8	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”.

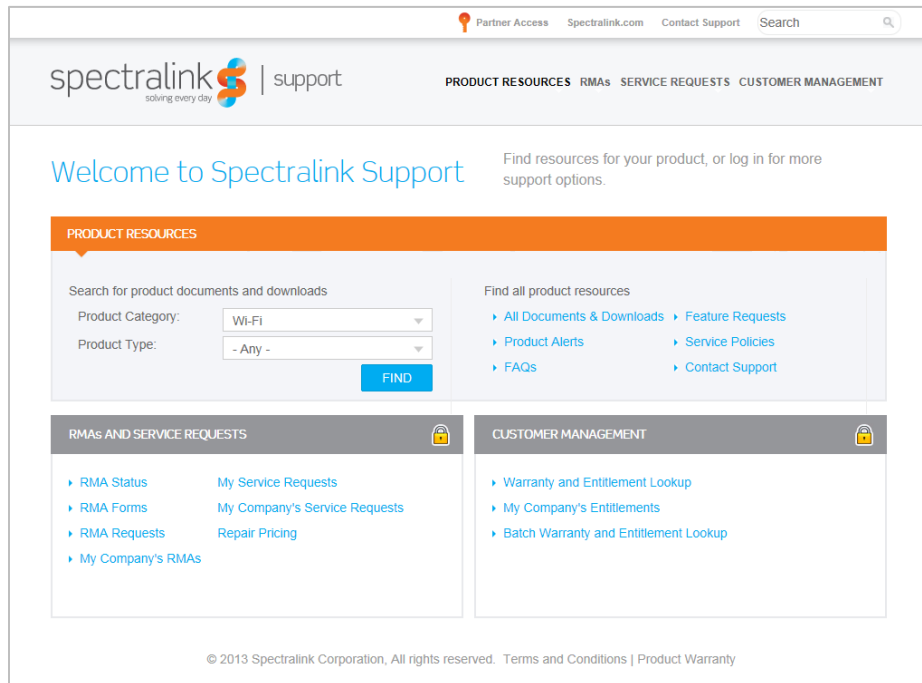
** Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls.

Known Limitations

- ExtremeCloud IQ products are controlled from the cloud. This means that access to the internet is necessary for product configuration. In general, the APs continue to provide service when disconnected from the Internet.
- The ExtremeCloud IQ system was tested with its default system of multicast-to-unicast disabled. To facilitate group announcements through PTT (Push-to-talk), the number of access points and phones must support a one-way call to every phone at the same time.
- Spectralink 84 Series devices are incompatible with the enforcing WMM-AC for video and voice under SSID settings. Unselecting these features has not degraded performance.
- When WMM-AC Video is enabled Spectralink devices receive downlink at Controller Load tag. This hasn't degraded performance.
- Ensure FT is set to enabled on the VQO app to gain 802.11r functionality on Versity devices
- Versity 92 supports FT but does not support 802.11r Adaptive. However it is compatible with it in that it will use legacy roaming mechanism when Adaptive is enabled.

Spectralink References

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 Versity software and support documents are available on the Spectralink support site at <http://support.spectralink.com/versity>.

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.

Product Support

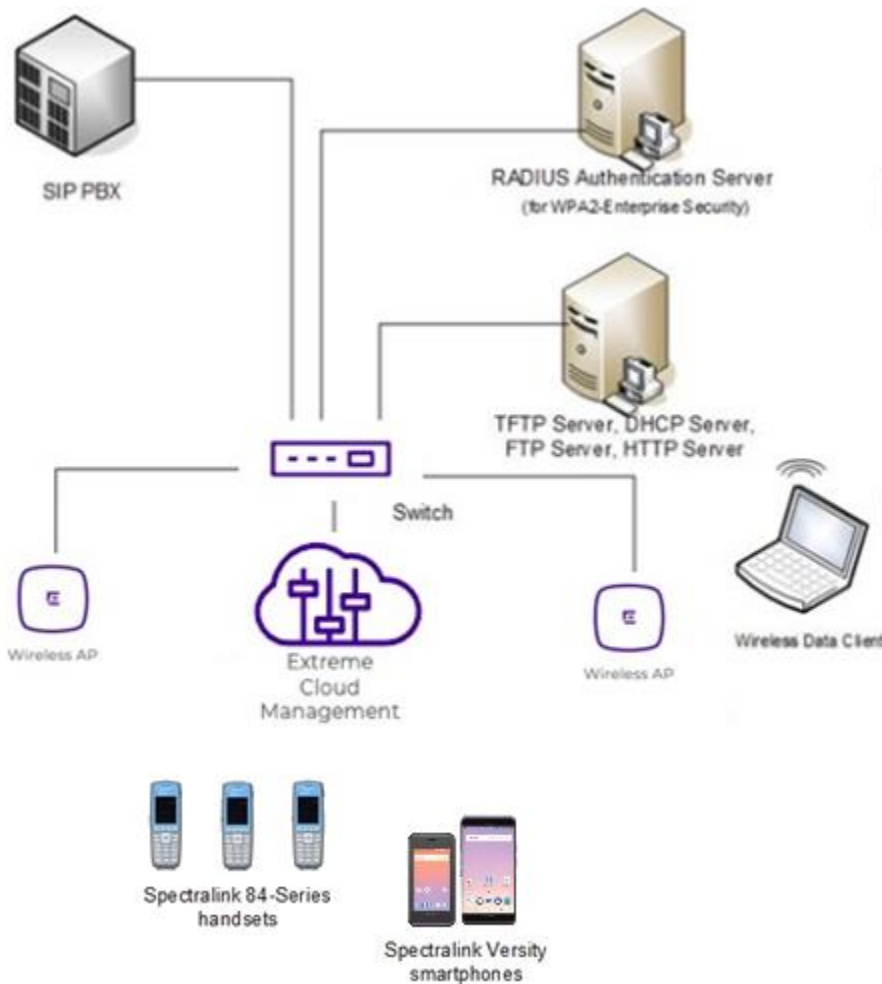
Spectralink support can be reached at support.spectralink.com.

Extreme Networks support can be reached by accessing the CloudIQ account at <https://extremecloudiq.com> from the help dropdown menu. Support may be reached at <https://extremenetworks.com/support> prior to obtaining a CloudIQ login.

Chapter 2: Overview

The following configuration was tested during VIEW certification.

Network Topology



Note: Example configuration shown

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



Note: Radius server setup

The setup for a Radius server for Enterprise security is outside the scope of this document.

Chapter 3: Setting Up Your Cloud Network

Initial network setup is performed when APs and CloudIQ support are purchased from Extreme. The dashboard is used to log in, network is created, and APs are added to the network.



Note: Use an incognito window

An “incognito window” must be used with some web browsers to avoid confusing field entry behavior. Touch the browser “More” menu (3 vertical dots) and select “Use an incognito window”.

Login and AP Onboarding

- 1 Navigate to <https://extremecloudiq.com> for an initial login.

ExtremeCloud IQ

Email

Password

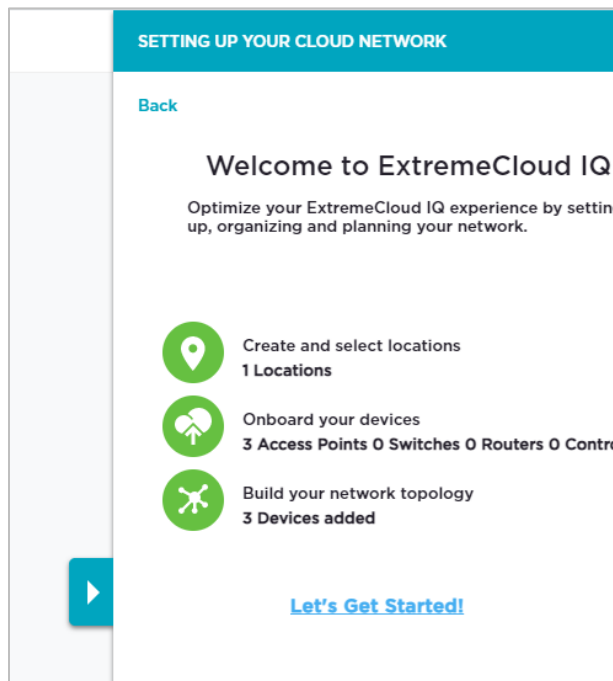
.....

LOGIN

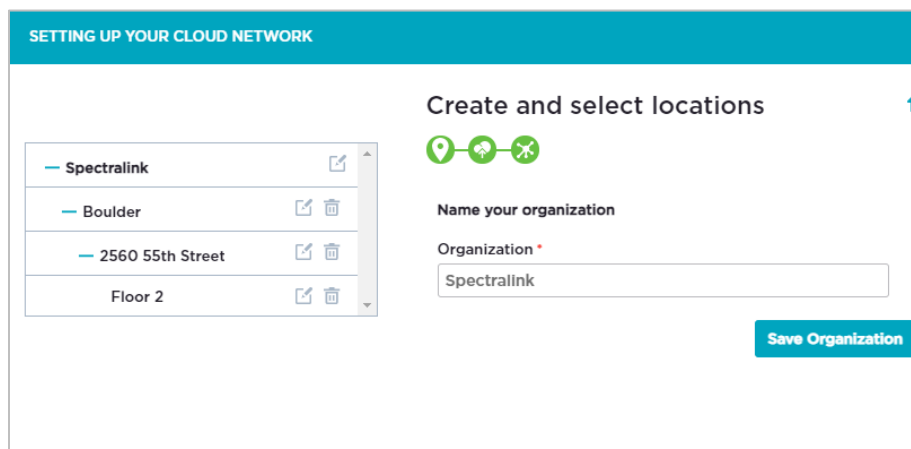
Forgot your password? [Reset it here](#)

Don't have an account? [Register here](#)

- 2 On the dashboard, expand the arrow on the right edge of the window and select the first option: Deploy your devices directly to the cloud.



- 3 Click on **Create and select locations** and enter the details of the deployment site.



- 4 Click on **onboard devices** to begin AP onboarding process.
- 5 Select **Real** under **Device Type** and either select manual entry or import a csv file and **Select Device Make** from the dropdown menu and click on **Onboard Devices**.

Onboard your devices

Device Type

Real
 Simulated

SERIAL NUMBER
When onboarding multiple devices, insert serial numbers that are part of the same platform family (for full explanation see the help system).

Enter manually
 Import CSV

1234354364576789900

Select Device Make
Extreme - Aerohive

Onboard Devices

6 Drag and drop unassigned devices to location data previously entered and click **Finish**.

SETTING UP YOUR CLOUD NETWORK

Build your network topology

LOCATIONS ● Devices Assigned

Spectralink (3)
Boulder (3)
2560 55th Street (3)
Floor 2 (3)

1 UNASSIGNED DEVICES
Select a floor from list then select, drag and drop devices to the floor map

Search by serial number

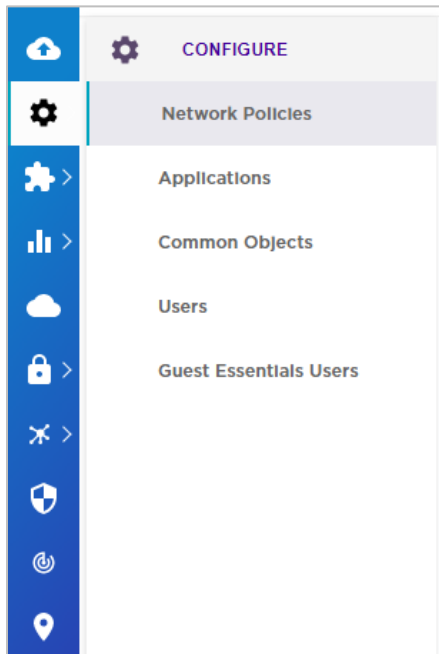
SIM-55B8D7
98454240287626 | AP460C

Previous: Onboard Devices **Finish**

Create a Network Policy

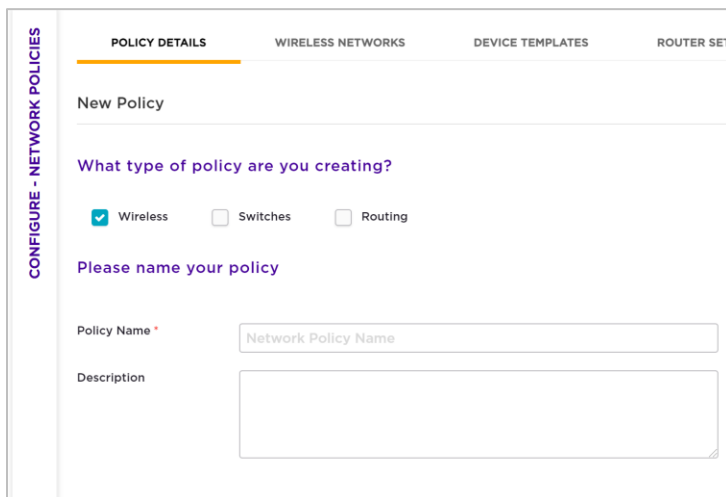
Create a network policy to organize the APs.

1 Navigate to **Configure > Network Policies** and select **Add Network Policy**



On the **New policy** screen:

- 2 Enter a name for the network policy.
- 3 Select the **Wireless Policy** Option and **Save**



Add APs to the Network Policy

Now that the network policy has been created, APs need to be added to the system.

The devices are selected using the lower part of the **Configure > Network Policies > (Policy Name) > Deploy Policy** screen.

- 1 Click Eligible and select devices to be added and click **upload**.

Network Policies > Test > Deploy Policy

POLICY DETAILS WIRELESS NETWORKS DEVICE T

Apply the network policy to selected

Only show devices that are:

Assigned Eligible Filtered

<input type="checkbox"/>	STATUS	DEVICE NAME	DEVICE MODEL
<input type="checkbox"/>		VIEW-AP-510C	AP650
<input type="checkbox"/>		VIEW-AP-410C	AP410C
<input type="checkbox"/>		VIEW-AP-305C	AP305C
<input type="checkbox"/>		SIM-55B8D7	AP460C

Chapter 4: Configure SSIDs

The wireless settings are configured by defining the SSID settings on the APs.

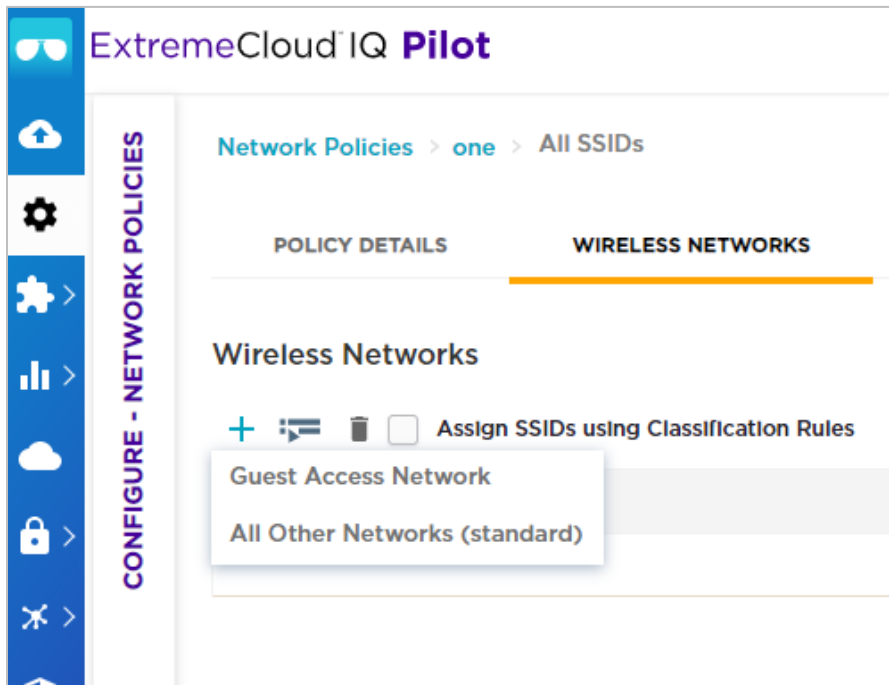
Define the SSIDs



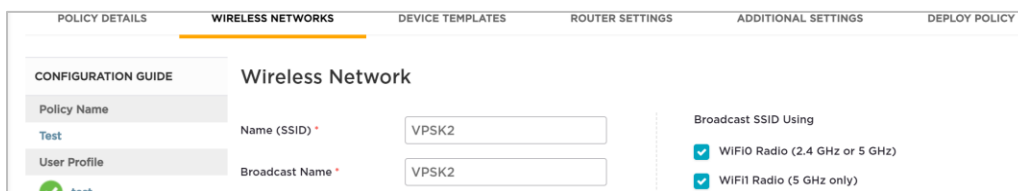
Note: 3 enabled SSIDs per AP recommended

Best Practice is enabling a maximum of 3 SSIDs per AP.

- 1 Navigate to **Configure > Network Policies > (Policy Name) > Wireless Networks** and click on **Add All Other Networks**



- 2 Enter the **SSID name, Broadcast Name**. Select **both WIFI radio** options for broadcasting SSID.



SSID Usage

The **SSID Usage** settings for an SSID vary depending on the type of security desired.

No security

- 1 For no security, click on the **Open Unsecured** button.

The screenshot shows the 'Wireless Network' configuration page. Under 'SSID Usage', there are two tabs: 'SSID AUTHENTICATION' and 'MAC AUTHENTICATION'. The 'SSID AUTHENTICATION' tab is active, showing five security options: Enterprise WPA / WPA2 / WPA3, Personal WPA / WPA2 / WPA3, Private Pre-Shared Key, WEP, and Open Unsecured. The 'Open Unsecured' option is highlighted with a dark blue background. Below the security options, there is a toggle for 'Enable Captive Web Portal' which is currently set to 'OFF'.

WEP



Note: WEP is insecure

Spectralink and Extreme do not recommend the user of WEP security due to its security weaknesses.

- 1 Select **WEP** from the menu.
- 2 Enter a ASCII Key in the Key Value 1 argument. This same key must be entered in the WEP key fields on the phones.

The screenshot shows the 'SSID Usage' configuration page with the 'WEP' security option selected. The 'Key Management' dropdown is set to 'WEP'. The 'Encryption Method' is 'WEP 104', and the 'Authentication Method' is 'Open'. The 'Key Type' is 'ASCII Key', and the 'Default Key' is 'Key Value 1'. The 'Key Value 1' field contains the text '1234' and has a 'Show Password' checkbox checked.

WPA2-PSK

- 1 Select the **Personal** and choose **WPA2-PSK** from the dropdown menu.
- 2 Enter an ASCII passphrase in the **Key Value** box. This same key must be entered in the password or passphrase fields on the phones.

SSID Usage

SSID AUTHENTICATION MAC AUTHENTICATION

Enterprise WPA / WPA2 / WPA3 Personal WPA / WPA2 / WPA3 Private Pre-Shared Key WEP Open Unsecured

Key Management: WPA2-(WPA2 Personal)-PSK

Encryption Method: CCMP (AES)

Key Type: ASCII Key

Key Value * 8-63 characters

Show Password

Enterprise securities



Note: Radius server setup

The setup for a Radius server for Enterprise security is outside the scope of this document.

- 1 Choose **Enterprise** option under **SSID Usage**.
- 2 Choose **WPA2-802.1X** under **Key Management**. Click on **Add RADIUS server group** to enter an external Radius server

Enterprise WPA / WPA2 / WPA3 Personal WPA / WPA2 / WPA3 Private Pre-Shared Key WEP Open Unsecured

Key Management: WPA2-802.1X

Encryption Method: CCMP (AES)



Note: Extreme cloud-based authentication services not tested

The ExtremeCloudIQ authentication option was not tested by Spectralink during VIEW program testing.

Configure RADIUS Servers

RADIUS Server Group Name * RADIUS Server Group Description

EXTERNAL RADIUS SERVER (0) EXTREME NETWORKS A3 (0) EXTREM

NAME

Cisco-ISE

- 3 If an external Radius server is used:
 - a Click **Add a server**.
 - b Enter the **Host** IP Address or DNS name, the **Port**, and the **Secret** entered on the Radius server.

Configure RADIUS Servers

RADIUS Server Group Name * RADIUS Server Group Description

EXTERNAL RADIUS SERVER (0) EXTREME NETWORKS A3 (0) EXTREME NETWORKS RADIUS S

New External RADIUS Server

Name *

Description

IP/Host Name * +

Server Type *

Authentication Port: *

Accounting Port: *

Shared Secret

Additional SSID settings (can be applied to SSIDs of all Usage types)

- 1 Select the **Additional Settings** option under the SSID and customize **Optional Settings**.

Additional Settings ▾
 Configure your Availability Scheduling, Security Controls, Optional Settings, and Client Monitoring

SSID Availability Schedule Restrict the availability of this SSID to selected schedules CUSTOMIZE

Advanced Access Security Controls 802.11w, Authentication timeout options CUSTOMIZE

Optional Settings Radio and Rates, DoS Prevention, and MAC filters CUSTOMIZE

- Set the Minimum bitrate to 11 Mbps under 2.4GHz Radio and Rates. Note: the Spectralink phones are 802.11g devices, so the 11 Mbps rate was left enabled.

bgRateSetting

Customize 2.4 GHz 11 b/g Rate Setting

1 Mbps	<input type="text" value="N/A"/>	9 Mbps	<input type="text" value="Optional"/>	24 Mbps	<input type="text" value="Optional"/>
2 Mbps	<input type="text" value="N/A"/>	11 Mbps	<input type="text" value="Basic"/>	36 Mbps	<input type="text" value="Optional"/>
5.5 Mbps	<input type="text" value="N/A"/>	12 Mbps	<input type="text" value="Optional"/>	48 Mbps	<input type="text" value="Optional"/>
6 Mbps	<input type="text" value="Optional"/>	18 Mbps	<input type="text" value="Optional"/>	54 Mbps	<input type="text" value="Optional"/>

- Enable **SSH, Ping, SNMP** and **Inter-station Traffic** under **Traffic Filters**.
- Select **Custom** under **Voice Enterprise** and **Enable 802.11k** and **802.11r**.

Voice Enterprise

Enable voice enterprise

Voice Enterprise is not supported on AP110, AP120, AP170, AP320, AP340, AP370, and AP390

Custom

Enable 802.11k

Enable dualband neighbor list

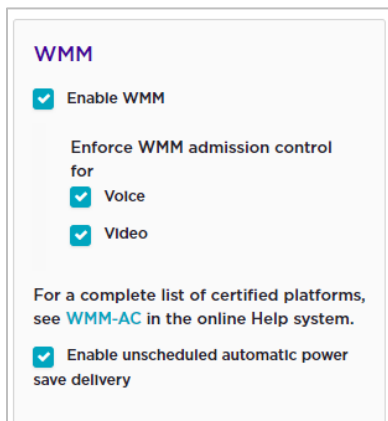
Max. neighbor APs: Range: 1 - 10

Enable 802.11v

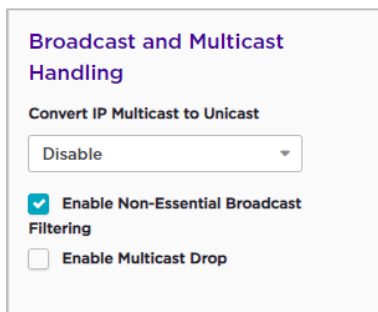
Enable 802.11r

For a complete list of certified platforms, see [Voice Enterprise](#) in the online Help system.

- Under **WMM**, check **Enable WMM**, and under **Enforce WMM admission control** for check **Voice** and **Video**. Also check **Enable unscheduled automatic power save delivery (U-APSD)**.



- 6 For **Broadcast and Multicast Handling**, under **Convert IP Multicast to Unicast** select **Disable**. Check **Enable Non-Essential Broadcast Filtering**.



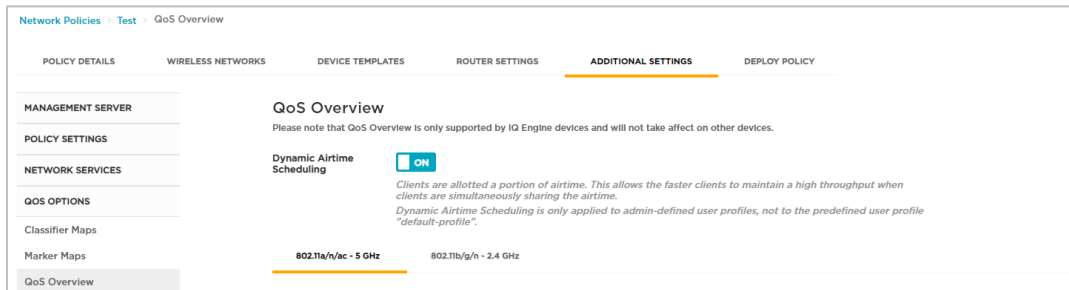
Note: WMM-AC Incompatible

Enabling Voice and Video for WMM-AC is incompatible with Spectralink 8400 devices. Ensure WMM- AC is not enabled on SSID's used by 8400's.

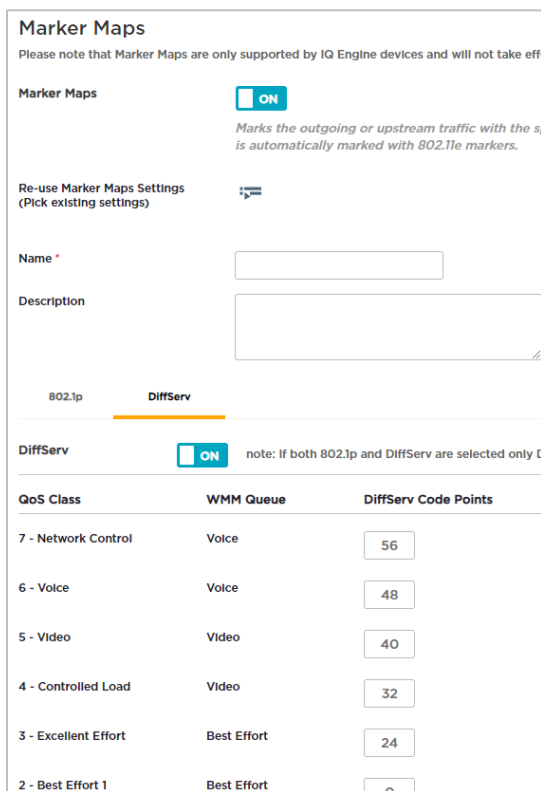
Additional Settings (Applied to Network Policy)

Under **Network Policies > (Policy Name) > Additional Settings**

- 1 Navigate to **QoS Options**
- 2 **Enable Dynamic Airtime Scheduling** under **QoS Overview**.



- Under **Market Maps**, set the **DSCP** tagging to 56 or whatever voice and video should have for the call server the phones are using.



- Enable Classifier Maps, enable 802.1p and 802.11e.

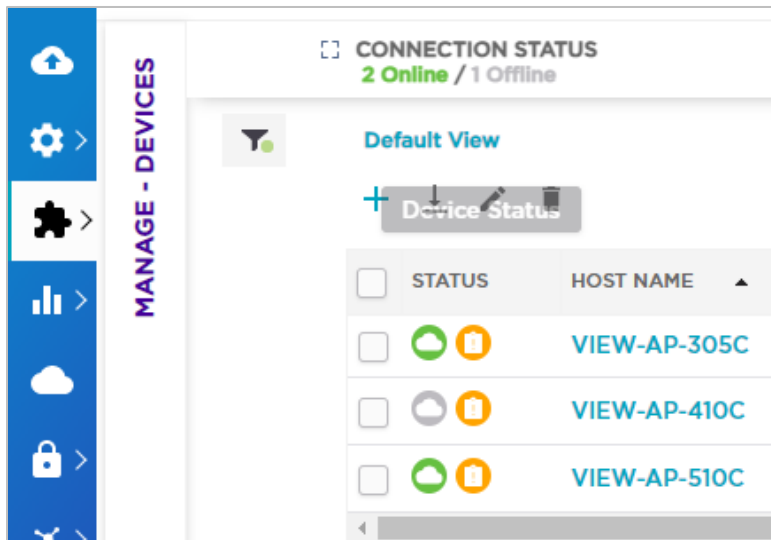
To define a Marker Map:

- Select **Diffserv** and **Enable** it.
- Enter Name and Diffserv Code Points to be used and save it.

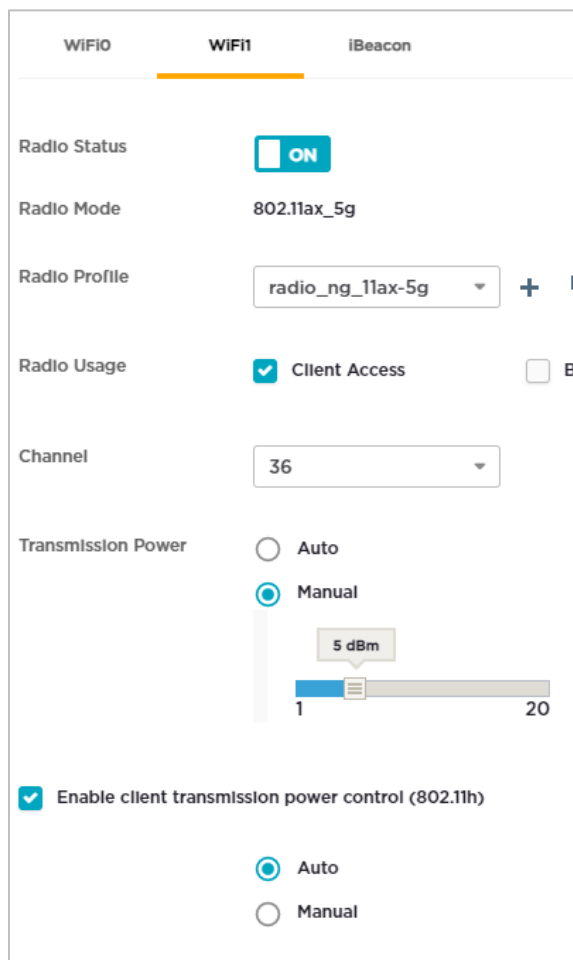
Radio settings

The radio settings for each AP must be set.

- 1 Navigate to **Manage> Devices**.
- 2 Select on an access point name in the list under Host Name.



- 3 Navigate to **Configure> Interface Settings> Wireless Interfaces**.
- 4 From the settings list that appears, choose channels and power settings as desired.



Note: Actual channel may be different than the manual channel setting

Due to radar or interference detection, the system may change the AP's channel.

The actual channel of an AP may be viewed by clicking on the name of an access point and navigating to **Monitor > Wireless Interfaces**

Chapter 5: Firmware Upgrades

ExtremeCloud IQ strives to minimize the administrative overhead of its systems. One of the ways this is accomplished is by centrally managing the software upgrade process.

- 1 Navigate to **User Profile> Communications> Notifications**.
- 2 The upgrade Notification is displayed along with New Features and enhancements.

NOTIFICATIONS

This page is used to list important notifications from Extreme Networks.

New Features and Enhancements

To see the new features and enhancements in ExtremeCloud™ IQ, visit [New Features and Enhancements](#).

ExtremeCloud IQ Upgrade Notification (Updated 05/9/2021)

In order to enhance current functionality and stability, we are upgrading some ExtremeCloud IQ components in following time window:

ExtremeCloud IQ Feature Upgrade:

- Sunday, May 9, 2021, 9:00 PM – 10:00 PM PDT for US and EU GDCs
- Monday, May 10, 2021, 2:00 PM – 4:00 PM PDT for the SE, ACH, and BH RDCs
- Tuesday, May 11, 2021, 3:00 AM – 5:00 AM PDT for the AUS RDC
- Tuesday, May 11, 2021, 9:00 AM – 11:00 AM PDT for the IN, JP, and SG-GCP RDCs
- Wednesday, May 12, 2021, 11:00 PM – 1:00 AM PDT for the VA RDC
- Thursday, May 13, 2021, 2:00 PM – 4:00 PM PDT for the IE, FRA, AGB, and NL-GCP RDCs
- Sunday, May 16, 2021, 11:00 PM – 1:00 AM PDT for the VA2, ACA, BR, AVA, and IA-GCP RDCs

End-User Impact: None

****END OF DOCUMENT****