

INTEROPERABILITY REPORT

Ascom i63
Extreme Networks

Cloud platform

v. 10.8.3.0 (AP)

Ascom i63 v. 6.2.4

Utrecht, The Netherlands

August 2025

ascom

Contents

Introduction.....	3
About Ascom.....	3
About Extreme Networks	3
Verification site.....	4
Participants	4
Verification topology.....	4
Summary	5
General conclusions	5
Verification overview	6
Known limitations.....	7
Appendix A: Verification Configurations.....	8
<i>Extreme Networks Cloud and Access Points configurations.</i>	8
WPA2 PSK (Personal)	8
WPA3 SAE (Personal)	10
WPA2 802.1X (Enterprise)	11
WPA3 802.1X (Enterprise)	12
802.1X (Enterprise) – External Radius Server Configuration.....	13
Ascom i63 v. 6.2.4 Network Settings.....	21
Appendix B: Interoperability Verification Records	25
Document History	25

Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Extreme Networks CloudIQ platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Extreme Networks and Ascom's platform configuration guides.

About Ascom

Ascom is a global solutions provider focused on healthcare ICT and mobile workflow solutions. The vision of Ascom is to close digital information gaps, allowing for the best possible decisions - anytime and anywhere. Ascom's mission is to provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. Ascom uses its unique product and solutions portfolio and software architecture capabilities to devise integration and mobilization solutions that provide truly smooth, complete and efficient workflows for healthcare as well as for industry and retail sectors.

Ascom is headquartered in Baar (Switzerland), has operating businesses in 19 countries and employs around 1,400 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Extreme Networks

Since our founding in Silicon Valley in 1996, Extreme Networks (EXTR) has been on the forefront of technological innovation. During the past 25+ years, we've grown to more than \$1.3 billion in annual revenue and more than 2,700 dedicated employees worldwide.

At Extreme Networks, we simplify and secure connectivity to enhance value, drive innovation, accelerate growth, and provide peace of mind. Trusted by tens of thousands of customers globally, we deliver AI-native cloud networking solutions that seamlessly connect people, applications, data, and devices.

Our comprehensive portfolio includes intelligent cloud management, security, and analytics capabilities. Whether your needs are cloud-based, on-premises, or at the edge, our solutions are designed to run anywhere and can be managed through a single, unified platform. Our customer-first services and flexible licensing options ensure that you can easily adapt and scale your network as your business grows.

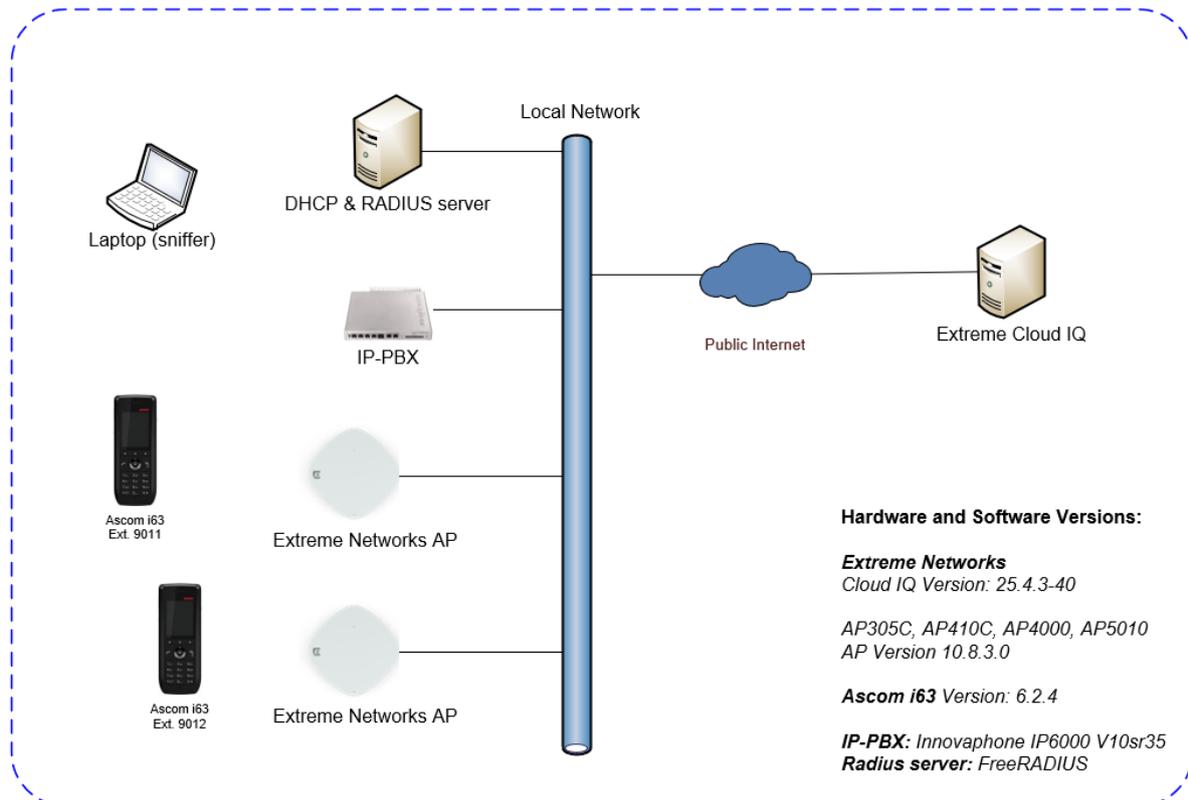
Verification site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

Participants

Remco van den Pangaart, Ascom,

Verification topology



Summary

General conclusions

The result of the verified test areas, such as authentication, association, handover and call stability test, produced very good results. The roaming times for WPA2, PSK and 802.1X (FT and non-FT) were excellent and were in the range of 30 ms for all combinations. WPA3 roaming times were longer when using SAE and 802.1X without 802.11r/FT, averaging between 97 and 138 ms. However, enabling 802.11r/FT significantly improved performance, reducing roaming times to between 26 and 38 ms. As such, enabling 802.11r is recommended to optimize roaming efficiency in WPA3 environments

Compatibility information

To ensure representative coverage across product generations and groups, one access point model was selected from each category: **305, 410, 4000, and 5010**. By testing these models, we effectively cover the performance characteristics of all access point models listed below.

Supported Partner Access Points running version 10.8.3.0:

AP305c/305cx

AP410c

AP460c

AP510c/510cx

AP650/650x

AP4000

AP5010

Verification overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association with WPA2-PSK / AES Encryption	OK	
Association with PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association with EAP-TLS authentication	OK	
Association with WPA3-Personal	OK	
Association with WPA3-Enterprise	OK	
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 27ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 22ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 29ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 25ms
Roaming with WPA3-Personal	OK	Typical roaming time 97ms
Roaming with WPA3-Personal, 802.11r/FT	OK	Typical roaming time 26ms
Roaming with WPA3-Enterprise	OK	Typical roaming time 128ms
Roaming with WPA3-Enterprise, 802.11r/FT	OK	Typical roaming time 35ms
Channel usage controlled by 802.11k	OK	
Association with Protected Management Frames 802.11w	OK	

Average roaming times are measured using on the 5GHz band. Refer to Appendix B for detailed test results

*) Measured times is with opportunistic/proactive Key Caching enabled (default enabled)

Known limitations

Description and Consequence	Workaround	Ticket(s) raised

For additional information regarding the known limitations please contact interop@ascom.com or support@ascom.com.

For detailed verification results, refer to Appendix B: Interoperability Verification Records.

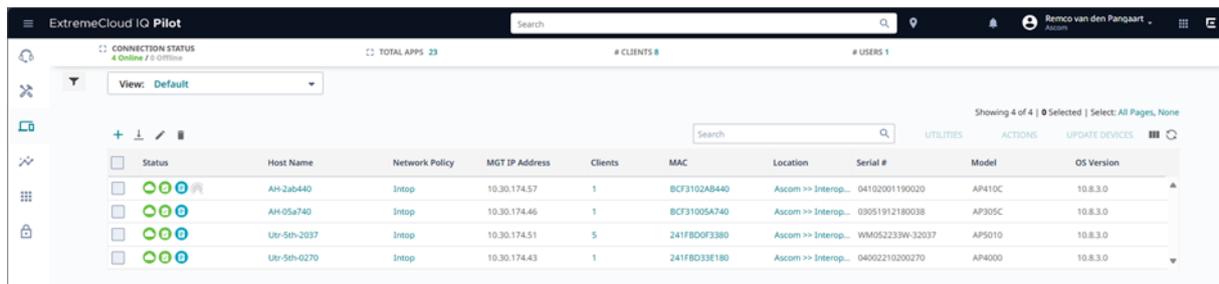
Appendix A: Verification Configurations

Extreme Networks Cloud and Access Points configurations.

In the following chapter you will find screenshots and explanations of basic settings to get the Extreme Networks solution operational with Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

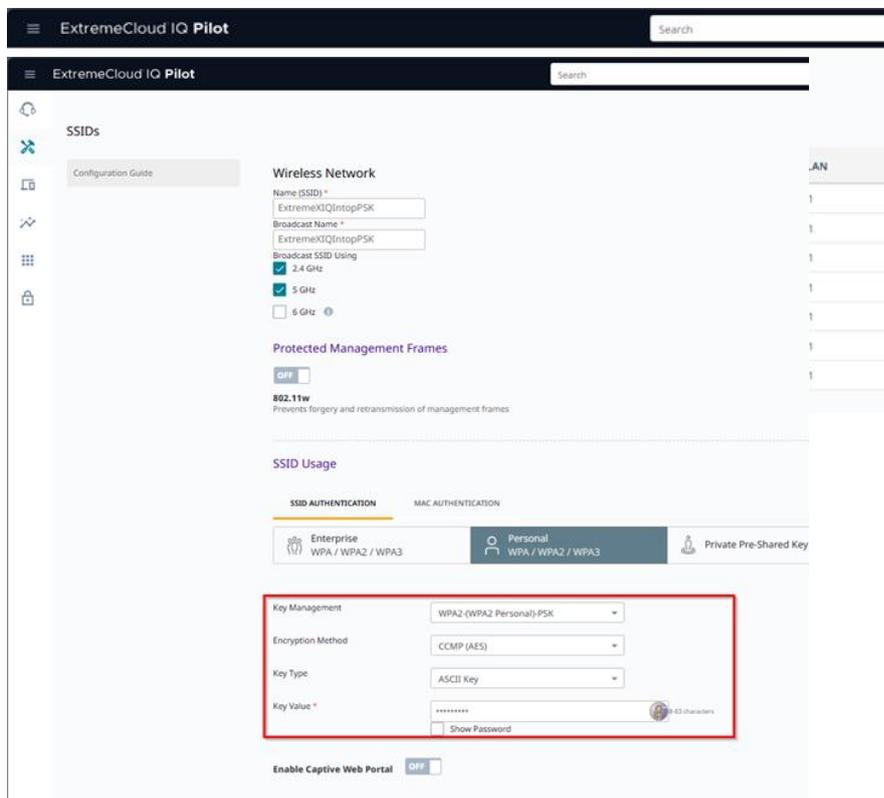
ESS, Security settings.

Dashboard overview (Monitor) of active access points



Status	Host Name	Network Policy	MGT IP Address	Clients	MAC	Location	Serial #	Model	OS Version
	AH-2ab440	Intop	10.30.174.57	1	BCF3102AB440	Ascom >> Interop...	04102001190020	AP410C	10.8.3.0
	AH-05a740	Intop	10.30.174.46	1	BCF31005A740	Ascom >> Interop...	03051912180038	AP305C	10.8.3.0
	Utr-5th-2037	Intop	10.30.174.51	5	241FBD0F3380	Ascom >> Interop...	WM052233W-32037	AP5010	10.8.3.0
	Utr-5th-0270	Intop	10.30.174.43	1	241FBD33E180	Ascom >> Interop...	04002210200270	AP4000	10.8.3.0

List of all configured SSIDs



Wireless Network

Name (SSID) * ExtremeXQ(Intop)PSK

Broadcast Name * ExtremeXQ(Intop)PSK

Broadcast SSID Using

- 2.4 GHz
- 5 GHz
- 6 GHz

Protected Management Frames

OFF

802.11w Prevents forgery and retransmission of management frames

SSID Usage

SSID AUTHENTICATION MAC AUTHENTICATION

Enterprise WPA / WPA2 / WPA3 Personal WPA / WPA2 / WPA3 Private Pre-Shared Key

Key Management: WPA2-(WPA2 Personal)-PSK

Encryption Method: CCMP (AES)

Key Type: ASCII Key

Key Value * *****

Enable Captive Web Portal: OFF

WPA2 PSK (Personal)

WPA2 PSK (Personal)

- Select WPA/WPA2/WPA3 (Personal)
- Select WPA2-(WPA2 Personal)-PSK as Key Management.
- Select CCMP (AES) as Encryption Method.
- Key can be entered in HEX or in ASCII format. Example shows a key entered in ASCII format.

WPA3 SAE (Personal)

The screenshot displays the configuration interface for a wireless network in the ExtremeCloud IQ Pilot. The main configuration area is titled "Wireless Network" and includes sections for "Protected Management Frames" and "SSID Usage". The "SSID Usage" section is currently set to "MAC AUTHENTICATION". A red box highlights the "Key Management" section, which is currently set to "WPA3 (SAE)". The "Key Management" section includes the following fields:

- Key Management: WPA3 (SAE)
- Method: H2E
- Encryption Method: CCMP (AES)
- SAE Group: All
- Transition Mode: Off
- Key Value: [Redacted]
- Anti-logging Threshold: 5
- Key Type: ASCII Key

WPA3 SAE (Personal)

- Select WPA/WPA2/WPA3 (Personal)
- Select WPA3 (SAE) as Key Management.
- Select CCMP (AES) as Encryption Method.
- Key can be entered in HEX or in ASCII format. Example shows a key entered in ASCII format.

WPA2 802.1X (Enterprise)

The screenshot displays the configuration page for a wireless network in the ExtremeCloud IQ Pilot interface. The page is titled 'Wireless Network' and includes several sections:

- Wireless Network:** Fields for Name (SSID), Broadcast Name, and Broadcast SSID Using (5 GHz selected).
- Protected Management Frames:** A toggle switch set to OFF.
- 802.11w:** A toggle switch set to OFF, with a note: 'Prevents forgery and retransmission of management frames.'
- SSID Usage:** A section with two tabs: 'SSID AUTHENTICATION' (selected) and 'MAC AUTHENTICATION'. Under 'SSID AUTHENTICATION', there are five radio button options: 'Enterprise WPA / WPA2 / WPA3' (selected), 'Personal WPA / WPA2 / WPA3', 'Private Pre-Shared Key', 'Open Unsecured', and 'Enhanced Open Secured'.
- Hotspot:** A dropdown menu set to 'Disabled'.
- Key Management:** A dropdown menu set to 'WPA2-802.1X'.
- Encryption Method:** A dropdown menu set to 'CCMP (AES)'.
- Enable Captive Web Portal:** A toggle switch set to OFF.
- Authentication Settings:** A toggle switch set to OFF.
- Authenticate via RADIUS Server:** A section with a table listing RADIUS servers. The table has columns for Name, Type, IP/Host Name, and Order. One server is listed: 'FreeRADIUS-RSA' of type 'External RADIUS Server' with IP/Host Name '10.30.174.5'.

WPA2 802.1X (Enterprise)

- Select WPA/WPA2 802.1X (Enterprise)
- Select WPA2-802.1X as Key Management
- Select CCMP as Encryption Method
- Select RADIUS server (defined in step 802.1X (Enterprise) – External Radius Server Configuration).

WPA3 802.1X (Enterprise)

The screenshot displays the configuration page for a wireless network in the ExtremeCloud IQ Pilot interface. The page is titled "Wireless Network" and includes several sections:

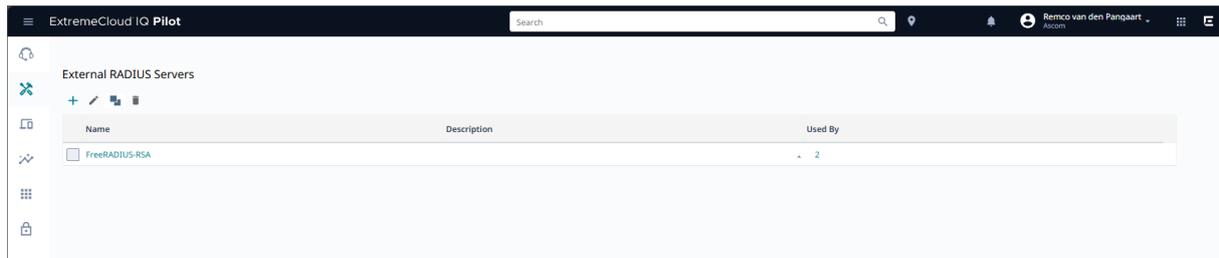
- Wireless Network:** Name (SSID) is "ExtremeXIQ(Intop-WPA3-E)", Broadcast Name is "ExtremeXIQ(Intop-WPA3-E)", and Broadcast SSID Using is checked for 2.4 GHz, 5 GHz, and 6 GHz.
- Protected Management Frames:** 802.11w is enabled, and "Enable Beacon Protection" is checked.
- SSID Usage:** SSID AUTHENTICATION is selected, and Enterprise WPA3 is chosen.
- Key Management:** WPA3-802.1X is selected. A note states: "WPA3 (SAE or 802.1X) will only be applied to IQ Engine versions 8.4-7 (SAE) and 8.4-8 (802.1X) or greater".
- Encryption Method:** CCMP (AES) is selected.
- Authentication Settings:** Authentication with ExtremeCloud IQ Authentication Service is disabled. Authentication is configured to "Authenticate via RADIUS Server".
- RADIUS Server Configuration:** A table lists the RADIUS server configuration:

Name	Type	IP/Host Name	Order
FreeRADIUS-RSA	External RADIUS Server	10.30.174.5	

WPA3 802.1X (Enterprise)

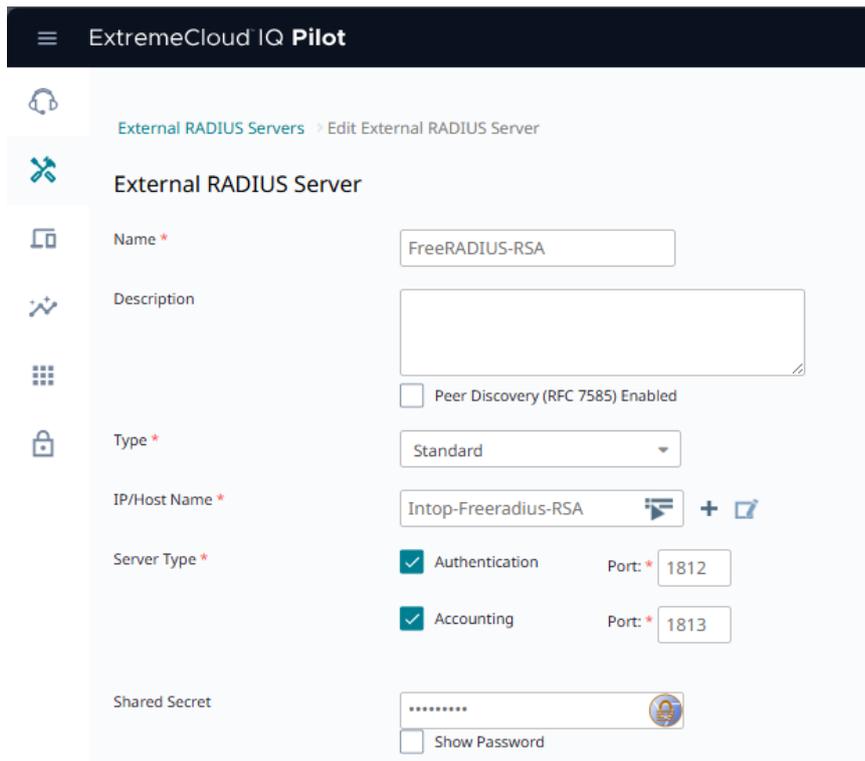
- Select WPA / WPA2 / WPA3 (Enterprise).
- Select WPA3-802.1X as Key Management.
- Select CCMP (AES) as Encryption Method.
- Select RADIUS server (defined in step 802.1X (Enterprise) – External Radius Server Configuration).

802.1X (Enterprise) – External Radius Server Configuration



Name	Description	Used By
FreeRADIUS-RSA		2

Overview of configured External Radius Servers.



External RADIUS Server configuration page:

- Name: FreeRADIUS-RSA
- Description: [Empty text area]
- Peer Discovery (RFC 7585) Enabled:
- Type: Standard
- IP/Host Name: Intop-Freeradius-RSA
- Server Type:
 - Authentication Port: 1812
 - Accounting Port: 1813
- Shared Secret: [Masked password field]
- Show Password:

External Radius Server configuration

- Configure the IP Address to the Radius server.
- Enter the “Shared Secret” that corresponds to the secret configured in the Radius server.

Advanced Access Security Settings

OFF

802.11w
Prevents forgery and retransmission of management frames

Advanced Authentication Options

<input type="checkbox"/>	Generate new Group Master key (GMK) after	<input type="text" value="0"/>	Seconds
<input type="checkbox"/>	Generate new Group Temporal key (GTK) after	<input type="text" value="0"/>	Seconds
	GTK timeout period	<input type="text" value="4000"/>	Milliseconds
	Number of GTK retries	<input type="text" value="3"/>	
<input type="checkbox"/>	Generate a new Pairwise Transient Key (PTK) after	<input type="text" value="0"/>	Seconds
	PTK timeout period	<input type="text" value="4000"/>	Milliseconds
	Number of PTK retries	<input type="text" value="3"/>	
	Replay window	<input type="text" value="0"/>	
<input type="checkbox"/>	Force the user to reauthenticate after	<input type="text" value="0"/>	Seconds
<input checked="" type="checkbox"/>	Local TKIP Countermeasure		
<input checked="" type="checkbox"/>	Remote TKIP Countermeasure		
<input checked="" type="checkbox"/>	Refresh GTK when the client disassociates from the SSID		
<input type="checkbox"/>	Enable Preauthentication (accelerates roaming)		
<input checked="" type="checkbox"/>	Enable proactive PMK-ID response (uses cached PMKs to supports fast roaming with certain clients)		

(Enterprise) - Additional settings - Advanced Access Security Controls

- Make sure that Enable Proactive PMK ID response is checked. (Not needed if 802.11r/FT is enabled)

Additional Settings ▾

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

SSID Availability Schedule	<input type="checkbox"/> 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
Client Monitor	<input checked="" type="checkbox"/> ON	

When enabled, Aerohive devices detect client issues, report client connection activities and problems to HiveManager.

Data rate configuration. (Per SSID)

- Go to optional Settings

Optional Settings ✕

bgRateSetting

Customize 2.4 GHz 11 b/g Rate Setting

1 Mbps	N/A	9 Mbps	N/A	24 Mbps	Optional
2 Mbps	N/A	11 Mbps	N/A	36 Mbps	Optional
5.5 Mbps	N/A	12 Mbps	Basic	48 Mbps	Optional
6 Mbps	N/A	18 Mbps	Optional	54 Mbps	Optional

Data rate configuration.2.4GHz

- To improve the performance in the wireless system it is recommended to disable the lowest data rates.

Optional Settings



aRateSetting

Customize 5.0 GHz 11a Rate Setting

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

CANCEL

SAVE RATE SETTING

Data rate configuration.5GHz

- To improve the performance in the wireless system it is recommended to disable the lowest data rates.

Optional Settings



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 forced disassociation

Enable 802.11r

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

WMM

Enable WMM

Enforce WMM admission control for

Voice
 Video

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

Enable unscheduled automatic power save delivery

Broadcast and Multicast Handling

Convert IP Multicast to Unicast

Channel utilization threshold

Range: 1 - 100

Membership count threshold

Range: 1 - 30

Enable Non-Essential Broadcast Filtering
 Enable Multicast Drop

Client Related Network Settings

Maximum client limit <input type="text" value="100"/> <small>Range: 1 - 255</small>	EAP timeout <input type="text" value="30"/> Seconds <small>Range: 5 - 300</small>	RTS threshold <input type="text" value="2346"/> bytes <small>Range: 1 - 2346</small>
Fragment threshold <input type="text" value="2346"/> bytes <small>Range: 256 - 2346</small>	DTIM settings <input type="text" value="2"/> <small>Range: 1 - 255</small>	Inactive client ageout <input type="text" value="5"/> Minutes <small>Range: 1 - 30</small>
EAP retries <input type="text" value="3"/> <small>Range: 1 - 5</small>	Roaming cache update interval <input type="text" value="60"/> Seconds <small>Range: 10 - 36000</small>	Roaming cache ageout <input type="text" value="60"/> <small>Range: 1 - 1000</small>
Local cache timeout		

CANCEL **SAVE OPTIONAL SETTINGS**

Optional SSID settings

- Enable 802.11k support.
- Enable 802.11v support. (802.11v is not really needed for i63, but still recommended if mixing with other Ascom products)
- Enable 802.11r support. (strongly recommended for enhanced roaming performance.)

- Make sure Enable WMM is checked.
- Make sure Unscheduled Automatic Power Save Delivery is checked.
- Make sure “Convert IP Multicast to Unicast” is enabled

- Ascom recommends a DTIM period of at least 2 but no higher than 5.

Quality of Service (QoS)

Classifier Maps > Classifier Maps

Classifier Maps

Please note that Classifier Maps are only supported by IQ Engine devices and will not take effect on other devices.

Name *

Description

SERVICES MAC OUIs SSIDs **802.1p/DiffServ/802.11e**

OFF 802.1p ON DiffServ OFF 802.11e

802.1p	QoS Class	DiffServ	QoS Class	802.11e	QoS Class
7	Network Control	56-63	Network Control	7	Network Control
6	Voice	48-55	Voice	6	Voice
5	Video	40-47	Voice	5	Video
4	Controlled Load	32-39	Controlled Load	4	Controlled Load
3	Excellent Effort	24-31	Excellent Effort	3	Excellent Effort
0	Best Effort 1	00-07	Best Effort 1	0	Best Effort 1
2	Best Effort 2	16-23	Best Effort 2	2	Best Effort 2
1	Background	08-15	Background	1	Background

Classifier Maps

- Create classifier map according to the screenshot and enable DiffServ and 802.11e
- **Important. For DiffServ 40-47 select QoS Class: 6 – Voice.**

ExtremeCloud IQ Pilot

Marker Maps > Ascom

Ascom

Please note that Marker Maps are only supported by IQ Engine devices and will not take effect on other devices.

Name *

Description

802.1p **DiffServ**

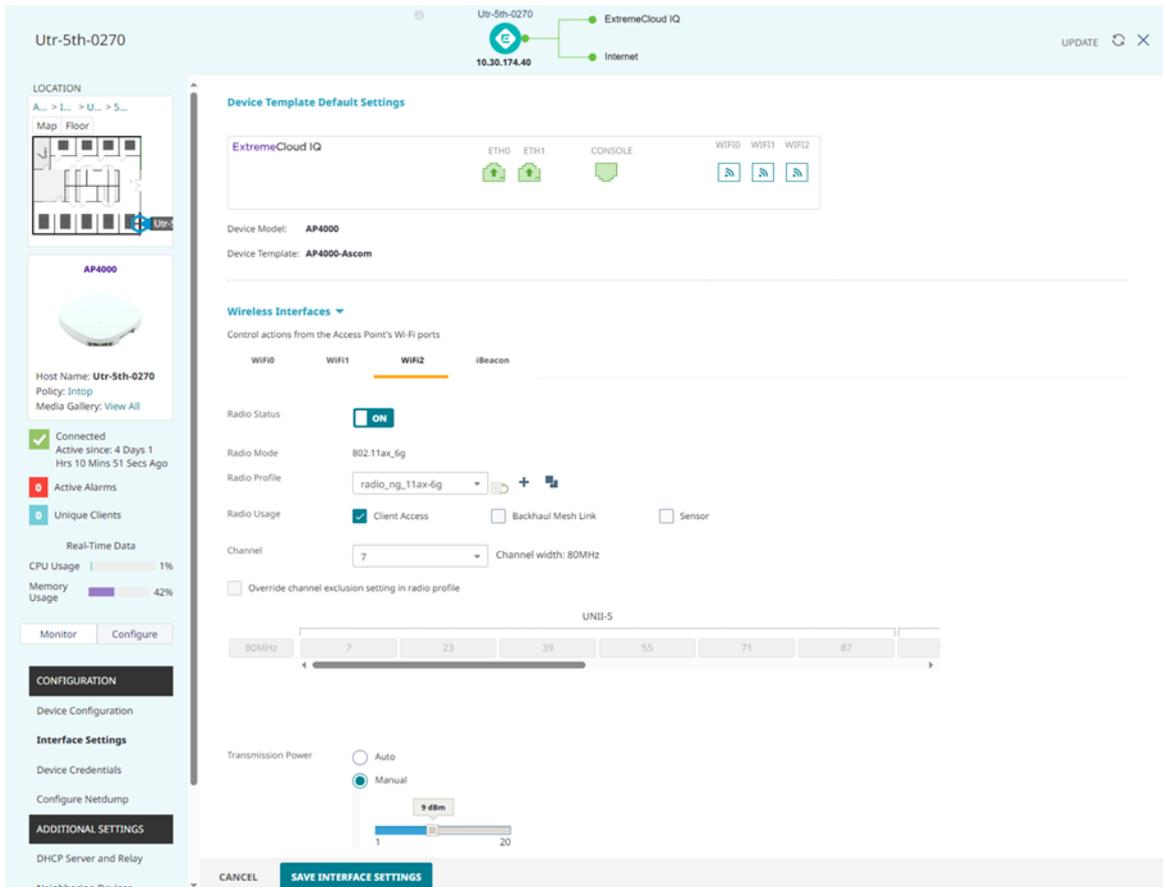
DiffServ **ON** note: If both 802.1p and DiffServ are selected only DiffServ will take effect.

QoS Class	WMM Queue	DiffServ Code Points
7 - Network Control	Voice	<input type="text" value="56"/>
6 - Voice	Voice	<input type="text" value="46"/>
5 - Video	Video	<input type="text" value="40"/>
4 - Controlled Load	Video	<input type="text" value="32"/>
3 - Excellent Effort	Best Effort	<input type="text" value="24"/>
2 - Best Effort 1	Best Effort	<input type="text" value="0"/>
1 - Best Effort 2	Background	<input type="text" value="16"/>
0 - Background	Background	<input type="text" value="8"/>

Marker Maps

- Create a Marker Map and assign QoS Class 6 - voice to 46

Radio Configuration



Configuration of access points

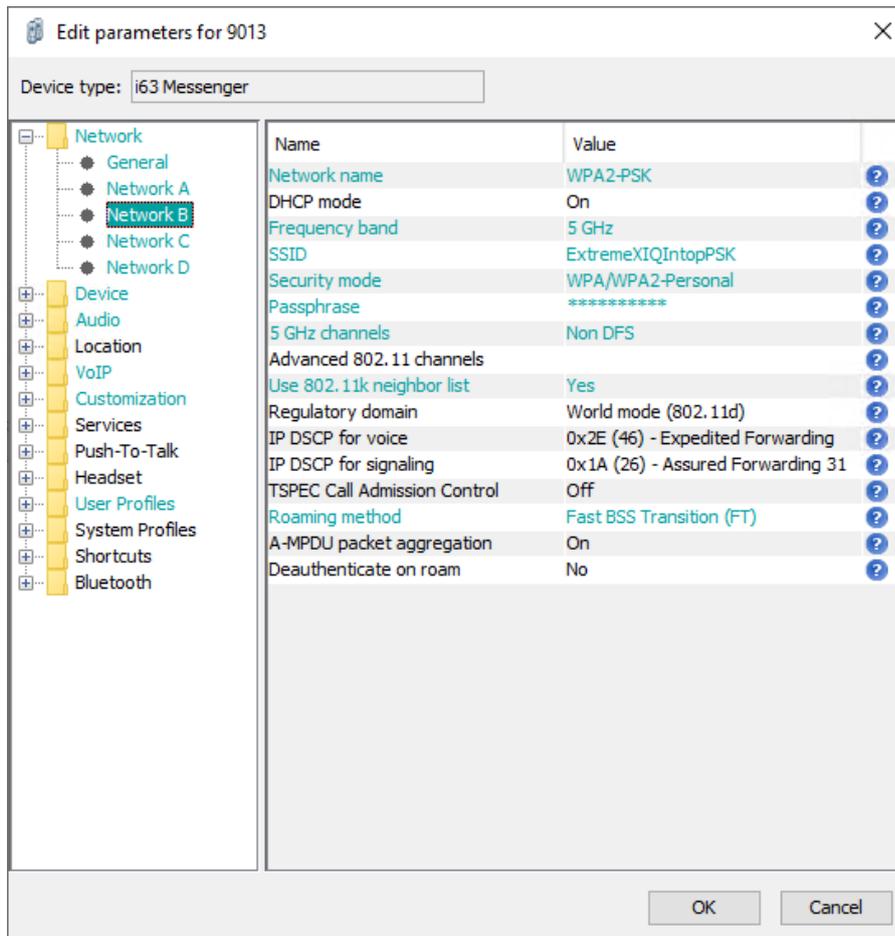
- Radio profiles used are the default (Default radio profiles **radio_ng_11ax-2g** for WiFi0, **radio_ng_11ax-5g** for WiFi1 and **radio_ng_11ax-6g** for WiFi2 interface).
- In the example channel and Transmission power has been set manually for each access point (for testing).

General guidelines when deploying Ascom handsets in 802.11a/n/ac/ax environments:

1. For environments not utilizing 802.11k Neighbor Report - Enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 channels enabled can be allowed. Ascom does not recommend exceeding these limits unless 802.11k is in use.
2. Ascom support and can coexist in 40/80/160MHz channel bonding environments. The recommendation is, however, to avoid 80/160MHz channel bonding, as it severely reduces the number of available non-overlapping channels.
3. Make sure that all non-DFS channels are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to “unpredictability” introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends, if possible, avoiding the use of DFS channels in VoWi-Fi deployments.

*) Dynamic Frequency Selection (radar detection)

WPA2-Personal (PSK)

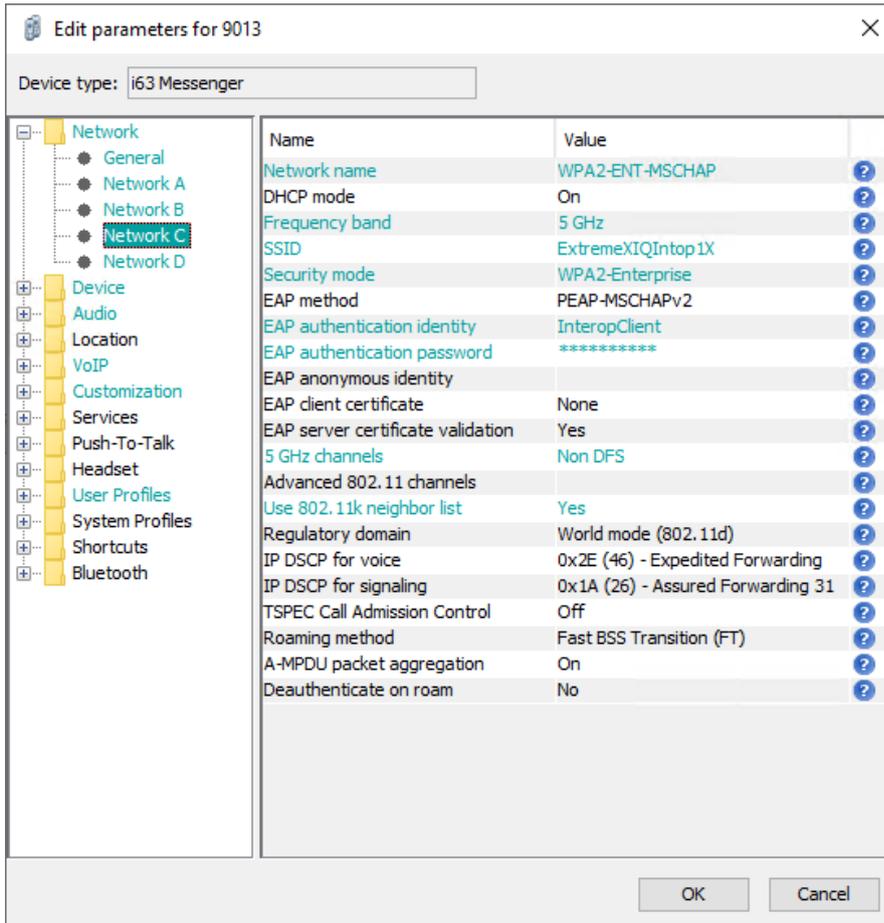


Network settings for WPA2-PSK

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA/WPA2-Personal.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list
- Set Roaming method to Fast BSS Transition (FT).

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to “USA”.

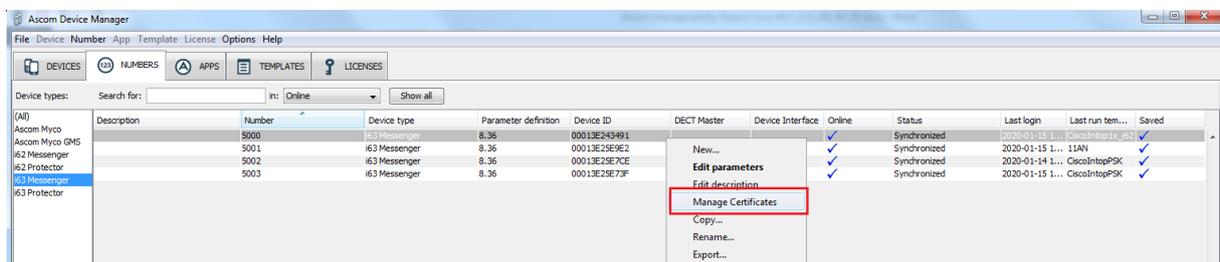
WPA2-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



Network settings for .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA2-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to “USA”.



802.1X Authentication requires a trusted certificate to be uploaded to the phone by “right clicking” -> Manage certificates.

Note that both Trusted Root and Application certificates are required when using EAP-TLS authentication.

WPA3-Personal (SAE)

Name	Value	
Network name	PSK	?
DHCP mode	On	?
Frequency band	5 GHz	?
SSID	CiscoIntopWPA3	?
Security mode	WPA3-Personal-FT	?
Passphrase	*****	?
5 GHz channels	UNII-1, UNII-2, UNII-3	?
Advanced 802.11 channels		?
Use 802.11k neighbor list	Yes	?
Regulatory domain	World mode (802.11d)	?
IP DSCP for voice	0x2E (46) - Expedited Forwar...	?
IP DSCP for signaling	0x1A (26) - Assured Forwardi...	?
TSPEC Call Admission Control	Off	?
A-MPDU packet aggregation	On	?
Deauthenticate on roam	No	?

Network settings for WPA3-Personal

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Personal-FT.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to “USA”.

WPA3-Enterprise (802.1X Authentication PEAP-MSCHAPv2)

Name	Value
Network name	MSCHAP
DHCP mode	On
Frequency band	5 GHz
SSID	CiscoIntopWPA3-1X9800
Security mode	WPA3-Enterprise
WPA3-Enterprise transition mode	No
EAP method	PEAP-MSCHAPv2
EAP authentication identity	InteropClient
EAP authentication password	*****
EAP anonymous identity	
EAP client certificate	None
EAP server certificate validation	Yes
5 GHz channels	UNII-1, UNII-2, UNII-3
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwar...
IP DSCP for signaling	0x1A (26) - Assured Forwardi...
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
A-MPDU packet aggregation	On
Deauthenticate on roam	No

Network settings for WPA3-Enterprise .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

NOTE: The FCC no longer allows 802.11d to determine the regulatory domain. Accordingly, devices deployed in the United States must have the “Regulatory domain” set to “USA”.

Description	Number	Device type	Parameter definition	Device ID	DECT Mas...	Device Int...	Online	Status	Saved	Last login	Last ru...
i63 Messenger	9010	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
i63 Protector	9011	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
	9012	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
	9013	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
	9014	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
	9015	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
	9016	i63 Messenger	OK				✓	Not synched	✓	2023-06...	CiscoInt...

802.1X Authentication requires a trusted certificate to be uploaded to the phone by “right clicking” -> Manage certificates.

Note that both Trusted Root and Application certificates are required when using EAP-TLS authentication.

Appendix B: Interoperability Verification Records

	2.4Ghz	5Ghz
Pass	23	25
Fail	0	0
Comments	4	2
Not verified	6	6
Total	33	33

Refer to the attached file for detailed verification results.

Document History

Rev	Date	Author	Description
D1	27-Aug-2025	NLRPA	Draft
D2		NLRPA	Minor corrections After internal review