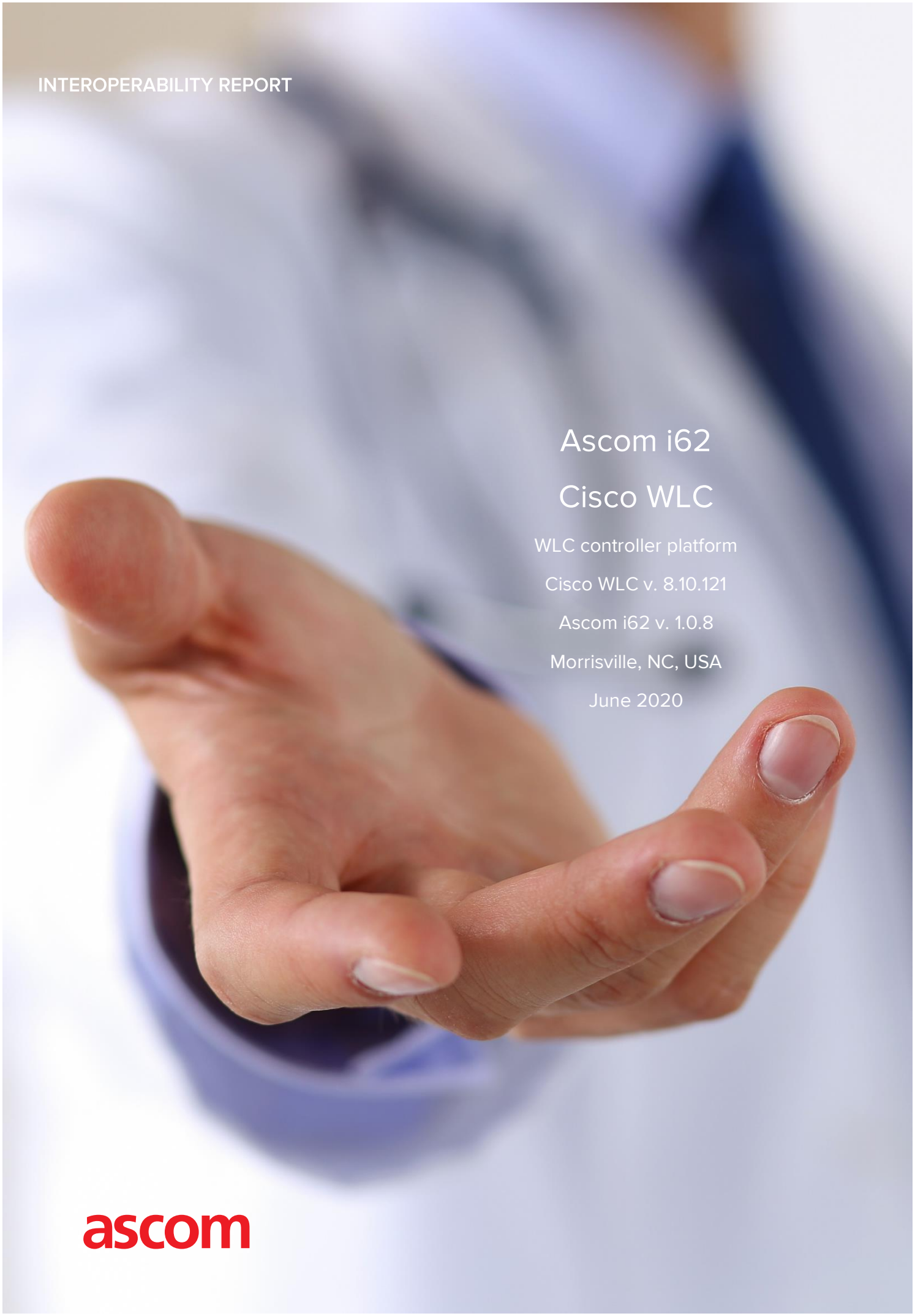
INTEROPERABILITY REPORT



# Ascom i62

# Cisco WLC

WLC controller platform

Cisco WLC v. 8.10.121

Ascom i62 v. 1.0.8

Morrisville, NC, USA

June 2020

ascom

# Contents

# Introduction

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

Ascom is headquartered in Baar (Switzerland), has operating businesses in 18 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

## About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at thenetwork.cisco.com and follow us on Twitter at @Cisco.

# Site Information

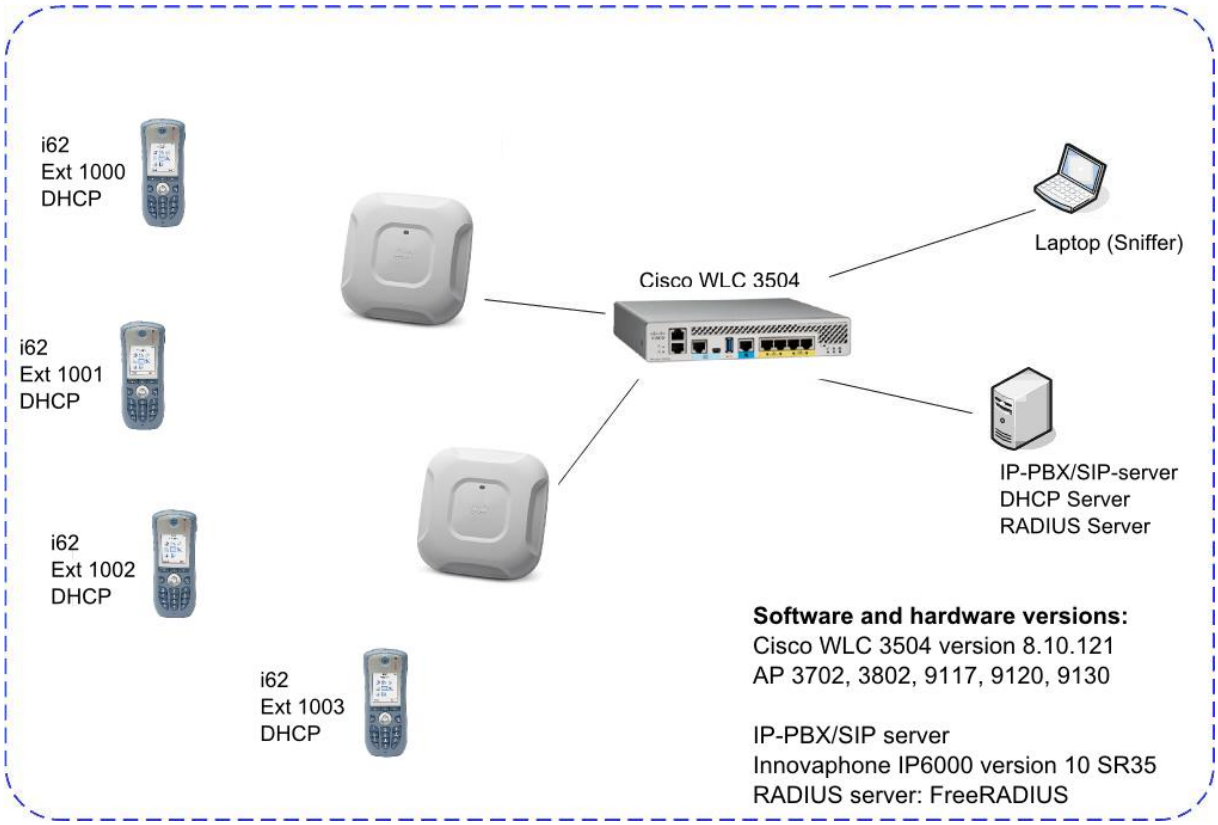
### Verification site

Ascom US
300 Perimeter park drive
Morrisville, NC, US-27560
USA

### Participants

Karl-Magnus Olsson, Ascom, Morrisville

### Verification topology



# Summary

## General conclusions

Overall the outcome of interoperability verification, including association, authentication and roaming produced good results. Roaming times are in general fully acceptable with for example expected roaming times of 40-60ms both when using WPA2-AES and PEAP-MSCHAPv2 (OKC).

To use U-APSD, make sure to set QoS to Platinum for the current WLAN profile and set WMM to Allowed. Also set EDCA profile for each band to "Voice Optimized" and disable low latency MAC.

## Compatibility information

One Access point model from every product generation has been selected as a representation (3702, 3802, 9117, 9120 and 9130). By testing these access points we are considered cover all supported major Cisco access points based on chipset compatibility listed below

**Supported Partner Access Points with SW version 8.10.121:**

AP1702, 2702, 3702

AP1832, 1852

AP2802, 3802

AP 4800

AP 9115, 9117, 9120, 9130

**Supported Partner Controller Platforms with SW version 8.10.121:**

Cisco 3504 Wireless Controller

Cisco 5520 Wireless Controller

Cisco 8540 Wireless Controller

Cisco Virtual Wireless Controller (vWLC)

Cisco Wireless Controllers for High Availability for Cisco 3504 WLC, Cisco 5520 WLC, and Cisco 8540 WLC.

Cisco Mobility Express Solution

## Verification overview

**WLAN Compatibility and Performance**

| High Level Functionality | Result | Comments |
|---|---|---|
| Association, Open with No Encryption | OK | |
| Association, WPA2-PSK / AES Encryption | OK | |
| Association, PEAP-MSCHAPv2 Auth, AES Encryption | OK | |
| Association with EAP-TLS authentication | OK | |
| Association, Multiple ESSIDs | OK | |
| Beacon Interval and DTIM Period | OK | |
| PMKSA Caching | OK | |
| WPA2-opportunistic/proactive Key Caching | OK | |
| WMM Prioritization | OK | |
| 802.11 Power-save mode | OK | |
| 802.11e U-APSD | OK | |
| 802.11e U-APSD (load test) | OK | |
| Roaming, WPA2-PSK, AES Encryption | OK * | Typical roaming time 55 ms |
| Roaming, PEAP-MSCHAPv2 Auth, AES Encryption | OK ** | Typical roaming time 40 ms |
| Roaming, EAP-FAST, CCKM | - | Not tested |

*) Average roaming times are measured using 802.11a/n. 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 |
|---|---|---|
| Not able to test EAP-FAST due to lack of supported authentication server | | |

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

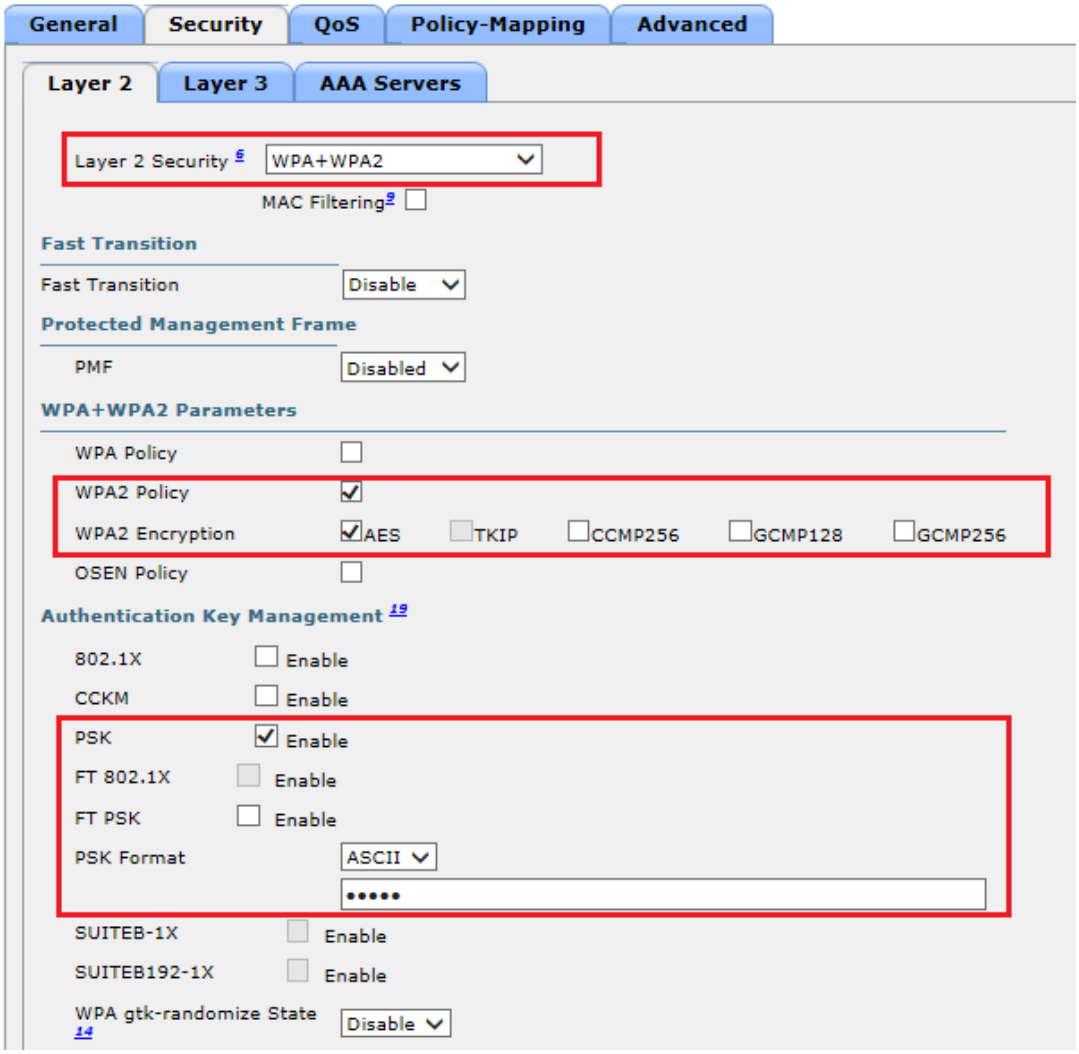
For detailed verification results, refer to Appendix B: Interoperability Validation Records.

# Appendix A: Validation Configurations

### Cisco WLC platform Version 8.10.121

In the following chapter you will find screenshots and explanations of basic settings in order to get a Cisco WLC WLAN system to operate with an Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

#### Security settings (PSK)

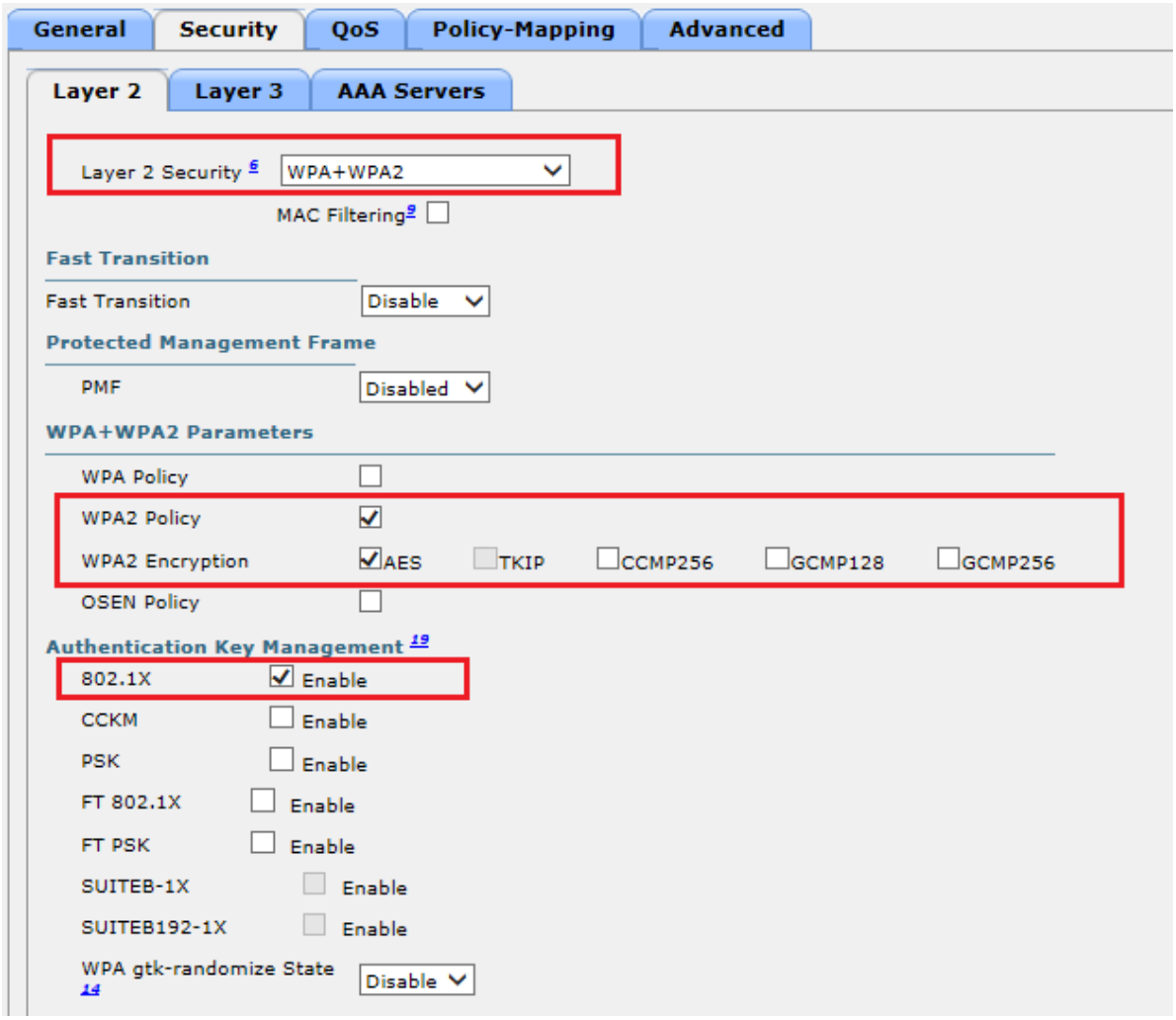



Example of how to configure the system for PSK (WPA2-AES)

Security profile WPA2-PSK, AES encryption

- Select WPA2 Policy with AES encryption.
- Select PSK and enter a key (Here in ASCII format)

**802.1X authentication (PEAP-MSCHAPv2).**

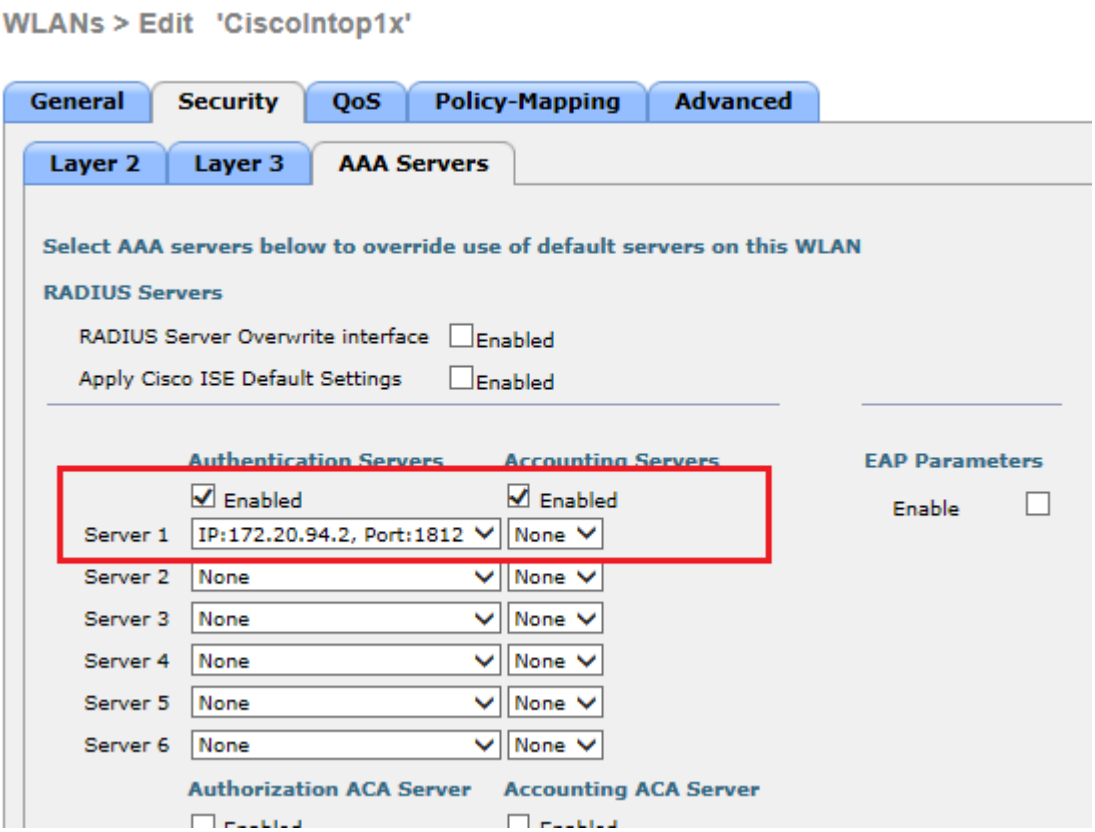



Example of how to configure the system for .1X authentication

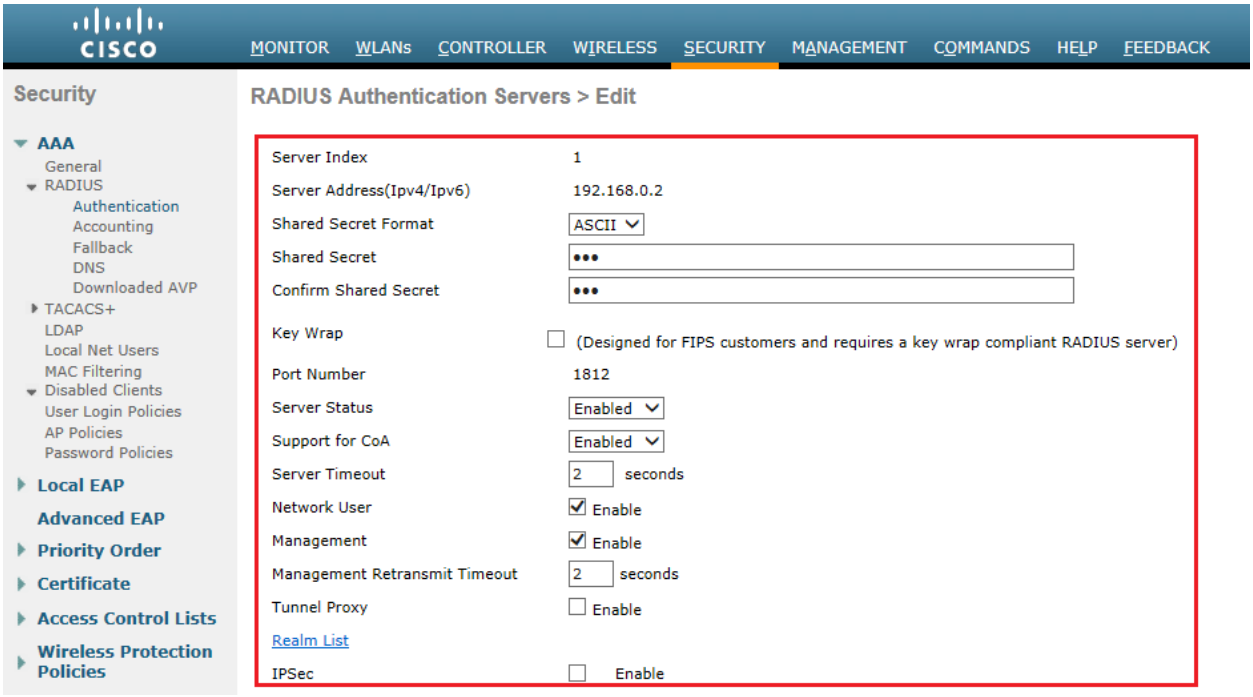
Configuration of authentication using external Radius server, 802.1X (Step 1). In this example is WPA2-AES used. Select 802.1X as Authentication Key Management.

**Note. Ascom i62 can operate on a SSID that has both 802.1X and FT 802.1X enabled.**

**Note. To use CCKM, replace 802.1X with CCKM check box. The "security mode" in the i62 has to be set to "Advanced" and CCKM has to be selected as "Authentication Key Management" instead of the default 802.1X.**




Example of authentication configuration using external Radius server (Step 2). Select the server to use. The server is configured under tab Security/Radius. See configuration of server below.

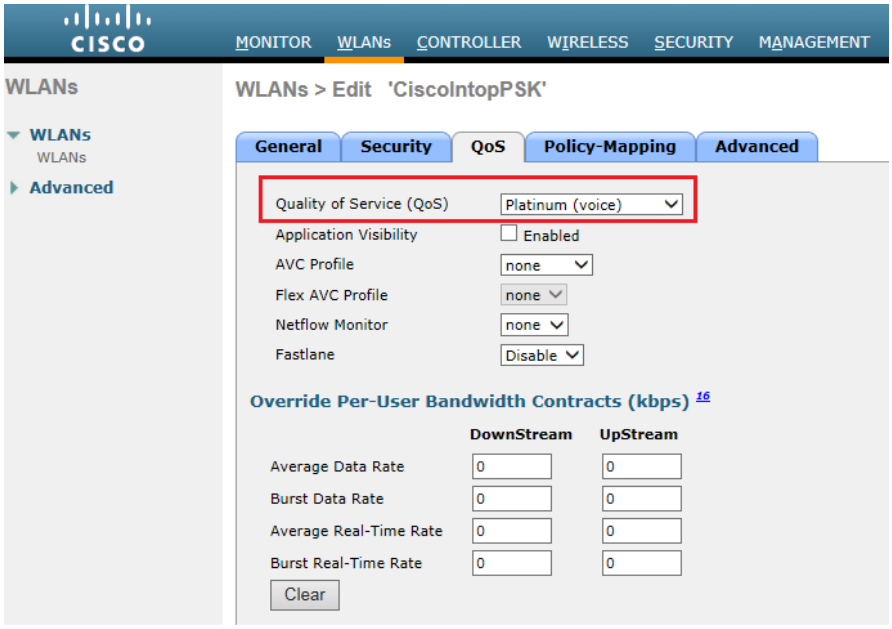



Configuration of authentication using external Radius server (Step 3). The IP address and the secret must correspond to the IP and the credential used by the Radius server. Tests were performed using FreeRadius as RADIUS server.

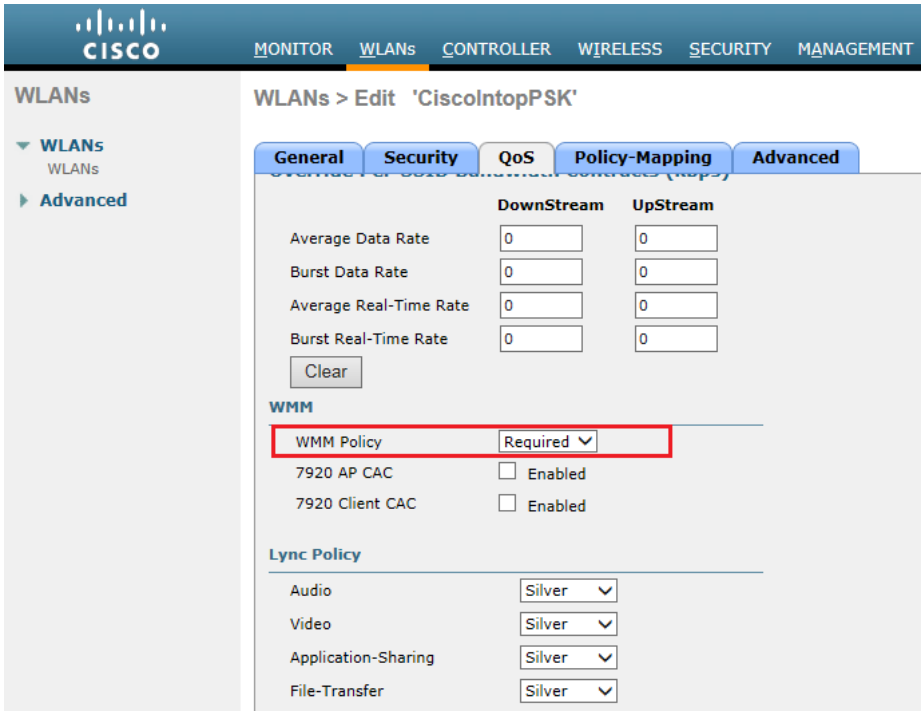
**Note. Depending on authentication method used it might be necessary to add a certificate into the i62. PEAP-MSCHAPv2 requires a CA certificate and EAP-TLS requires both a CA certificate and a client certificate. Server certificate validation can be overridden in version 4.1.12 and above per handset setting.**

**Note. Refer to the i62 section in for matching handset configurations.**

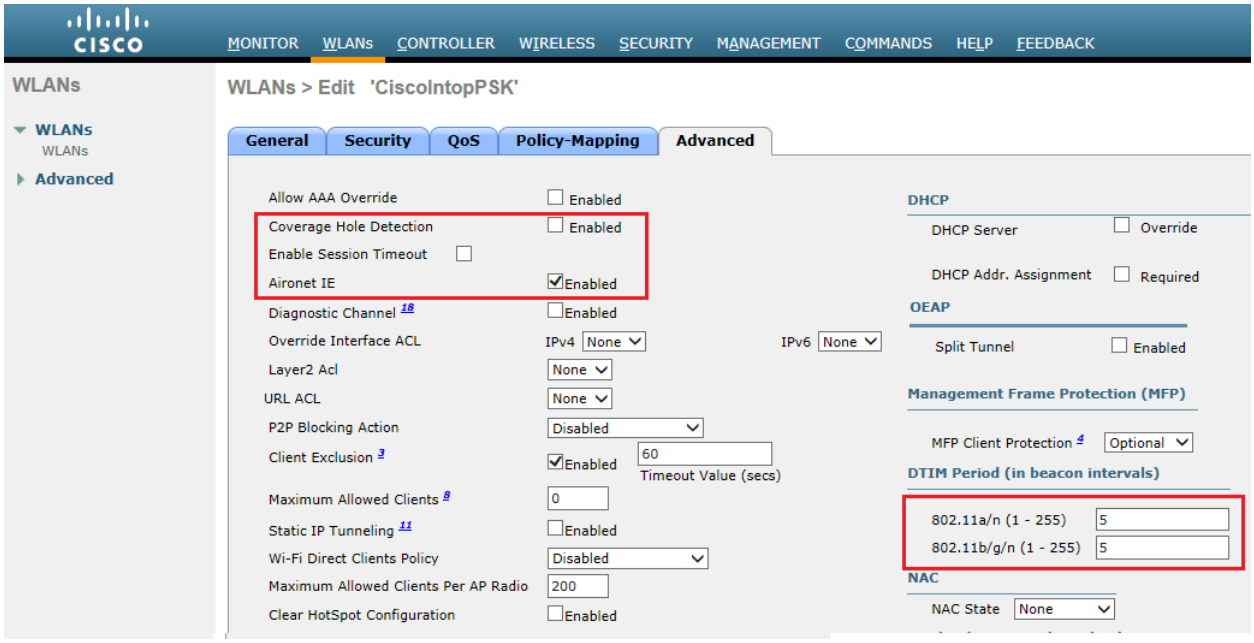
### General settings (QoS, Radio)



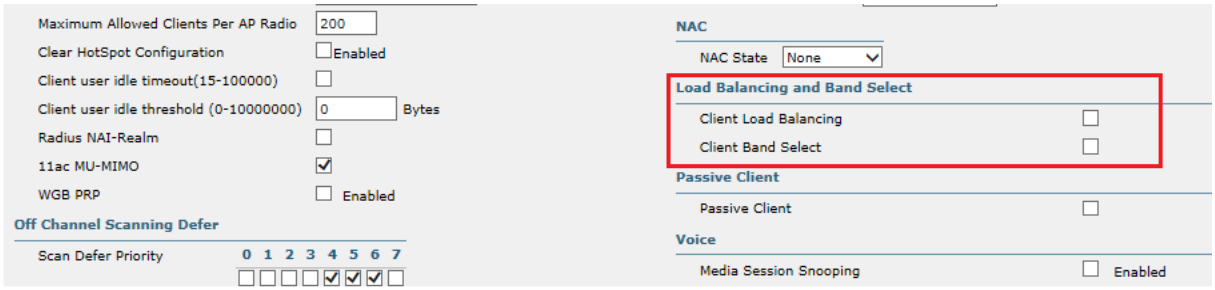

Set QoS to “Platinum (Voice)”



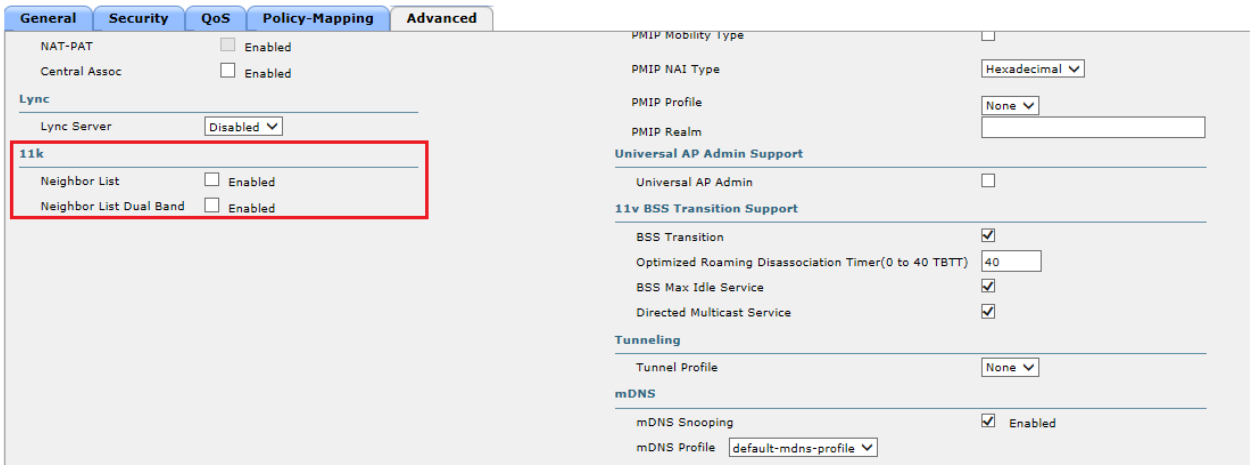

Make sure that WMM policy is set to “Required” or “Allowed”



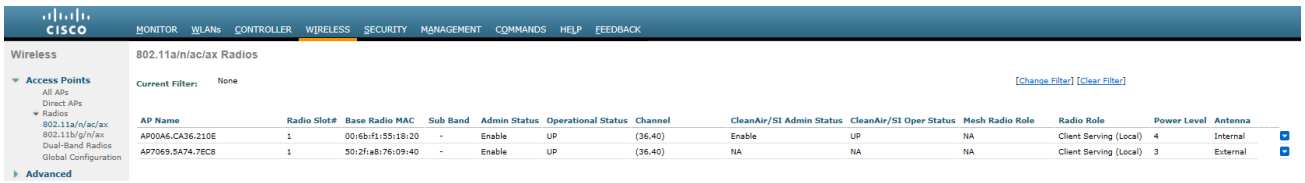

Make sure “Session timeout” is disabled. Coverage Hole Detection can be left enabled if RRM is used in the system. Set DTIM period to Ascom recommended value 5. DTIM value 5 values are recommended in order to allow maximum battery conservation without impacting the quality. Using a lower DTIM value is possible but will reduce the standby time.



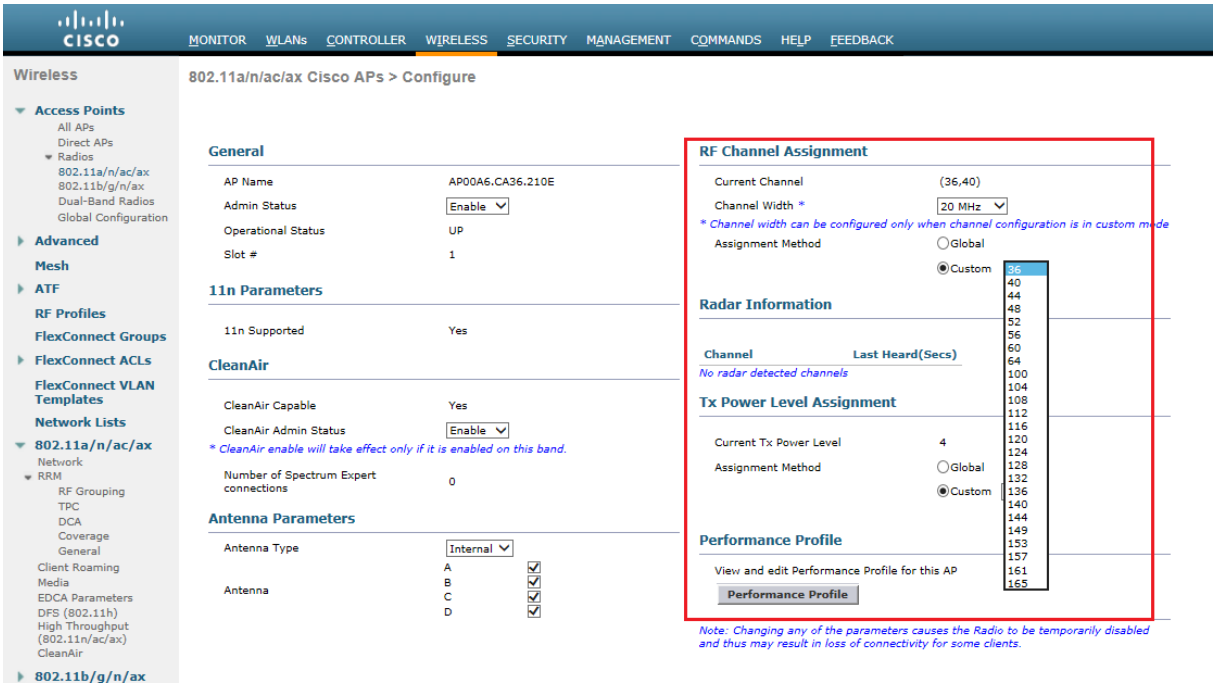

Make sure Client Load Balancing and Client Band select is disabled.




Even though 11k features are not supported Ascom i62 it can coexist in a network were it is enabled.




Channel configuration. See next picture for additional information.



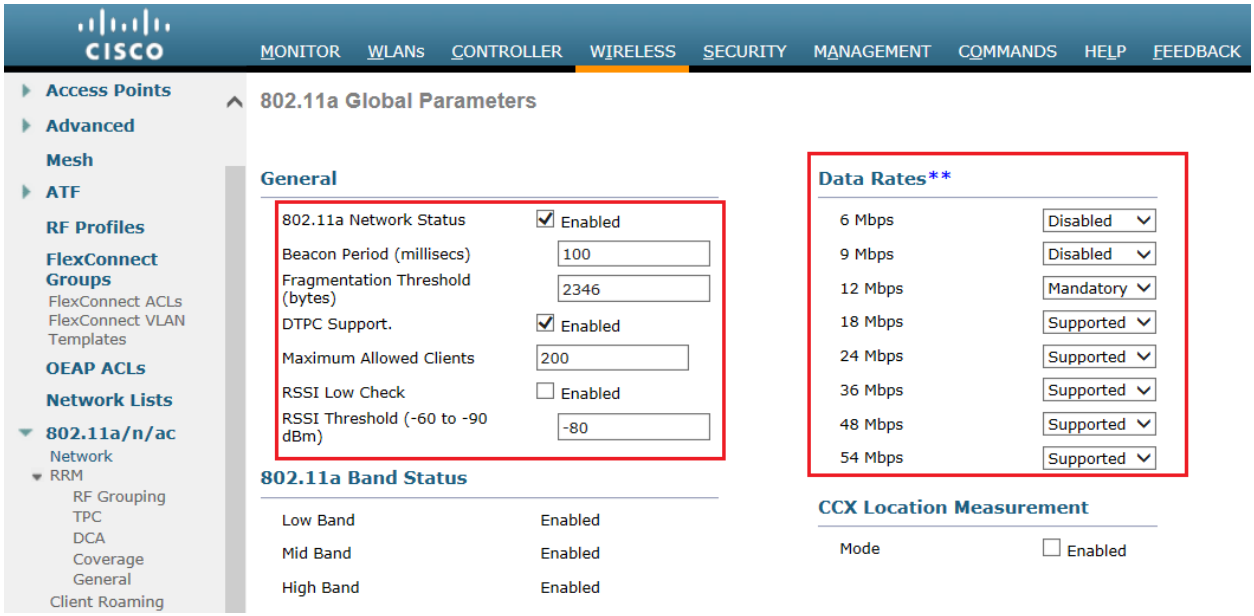

Ascom recommended settings for 802.11b/g/n are to only use channel 1, 6 and 11. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.

**Note that Tx power level and channel was manually set for test purpose.**

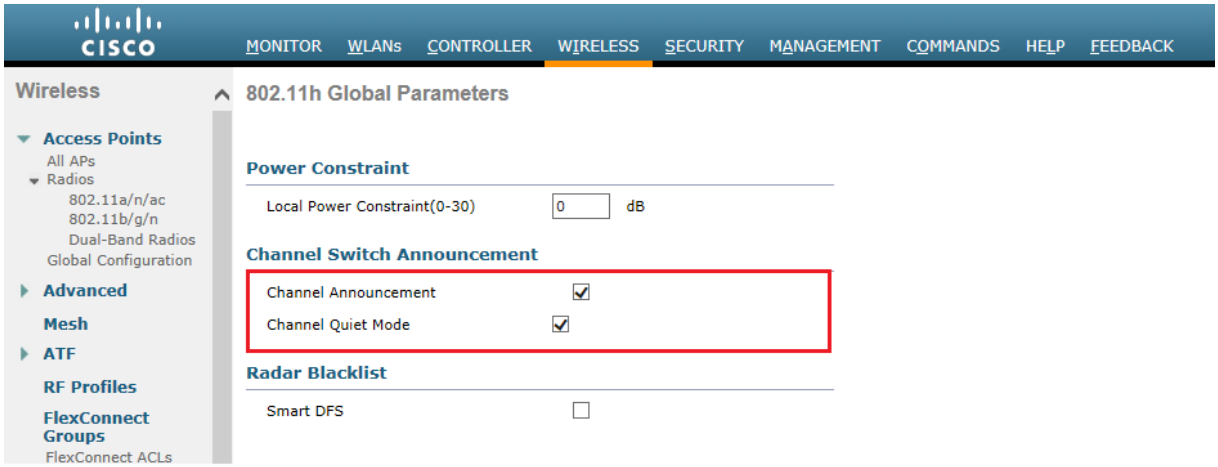
***General guidelines when deploying Ascom i62 handsets in 802.11a/n/ac environments:***

1. ***Enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed.***
   ***Ascom does not recommend exceeding this limit.***
2. ***Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 20MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.***
3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***
4. ***Make sure that all non-DFS channel 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 VoWIFI deployments.***

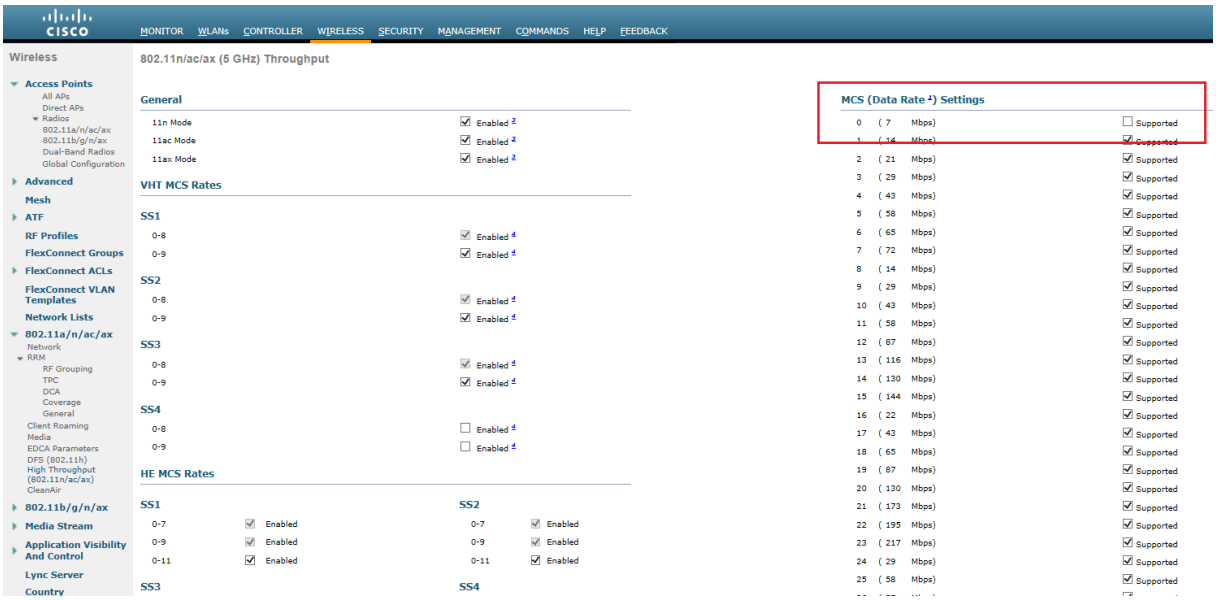
***) Dynamic Frequency Selection (radar detection)**




The default data rate set will work just fine, however Ascom recommends disabling the lowest speeds and have 12Mbps as lowest supported speed.

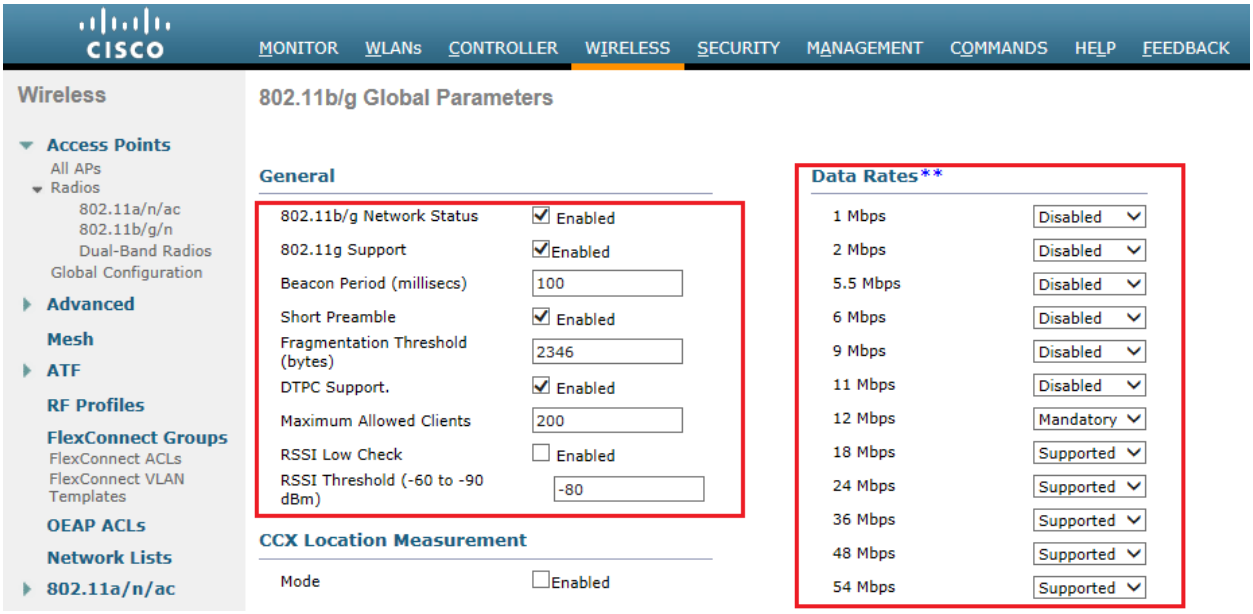



As Ascom i62 do support Channel Switch Announcement it's recommended to have this setting enabled in the system (only applicable when DFS channels are used)

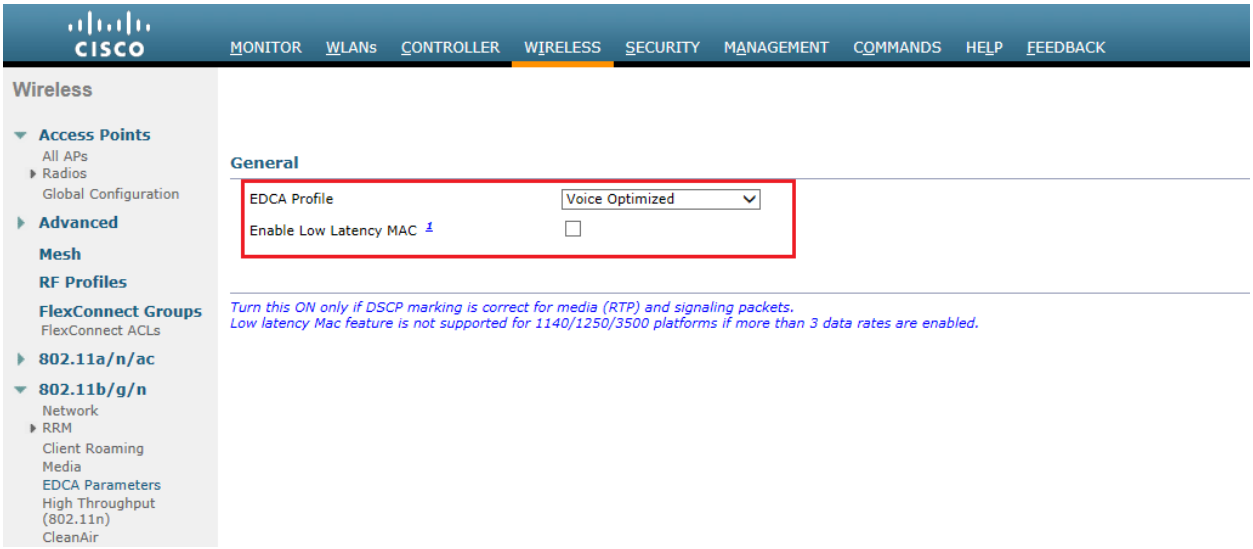



Ascom i62 is an .11n device but can coexist in .11ac and 11ax systems with both 40 MHz and 80 MHz channel width. We recommend disabling the lowest data rates including MCS0

**Follow the recommendations "*General guidelines when deploying Ascom i62 handsets in 802.11a/n/ac environments*" on Page 16**



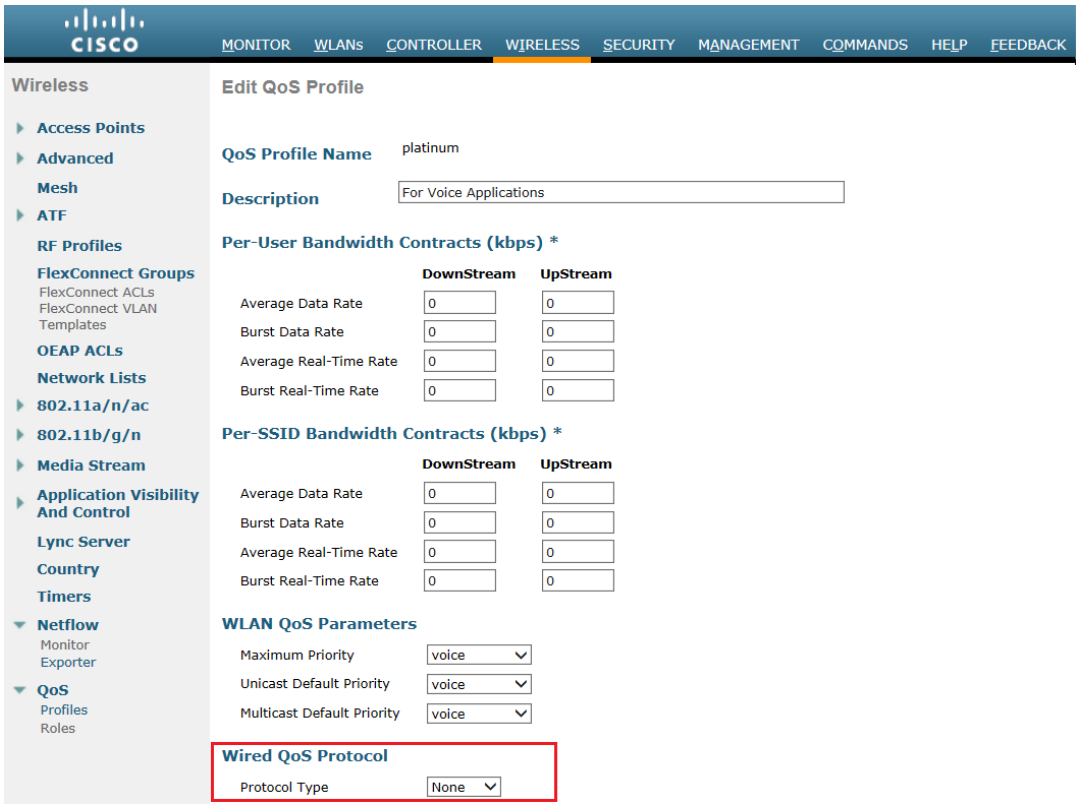

The default data rate set will work fine, however for optimization Ascom recommends disabling the lowest data rates and have 12Mbps as lowest mandatory rate.



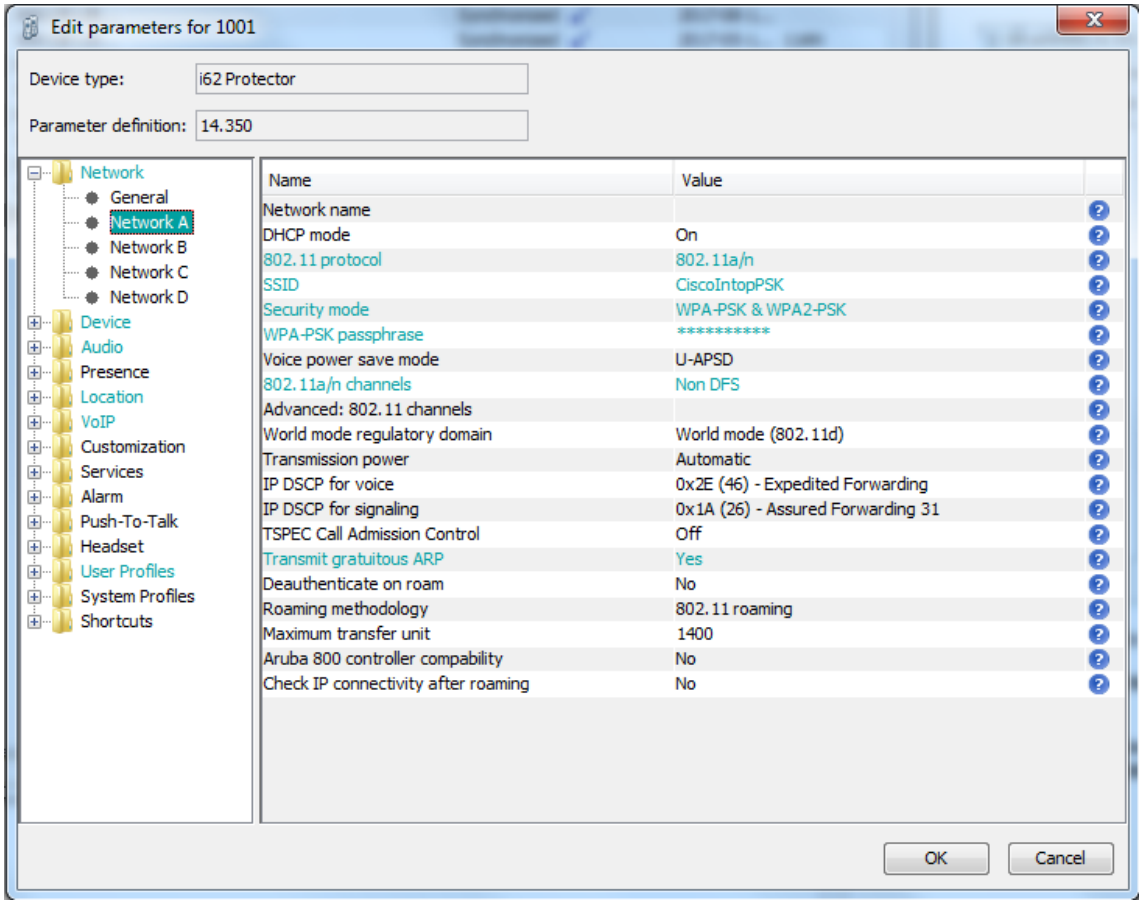

Ascom recommends “EDCA Profile”: Voice Optimized

Make sure Low Latency MAC is disabled. (Both 802.11a/n/ac and 802.11b/g/n)

**Note. Using EDCA Profile “WMM” is acceptable but “Voice Optimized” is to prefer when voice clients are present in the system.**



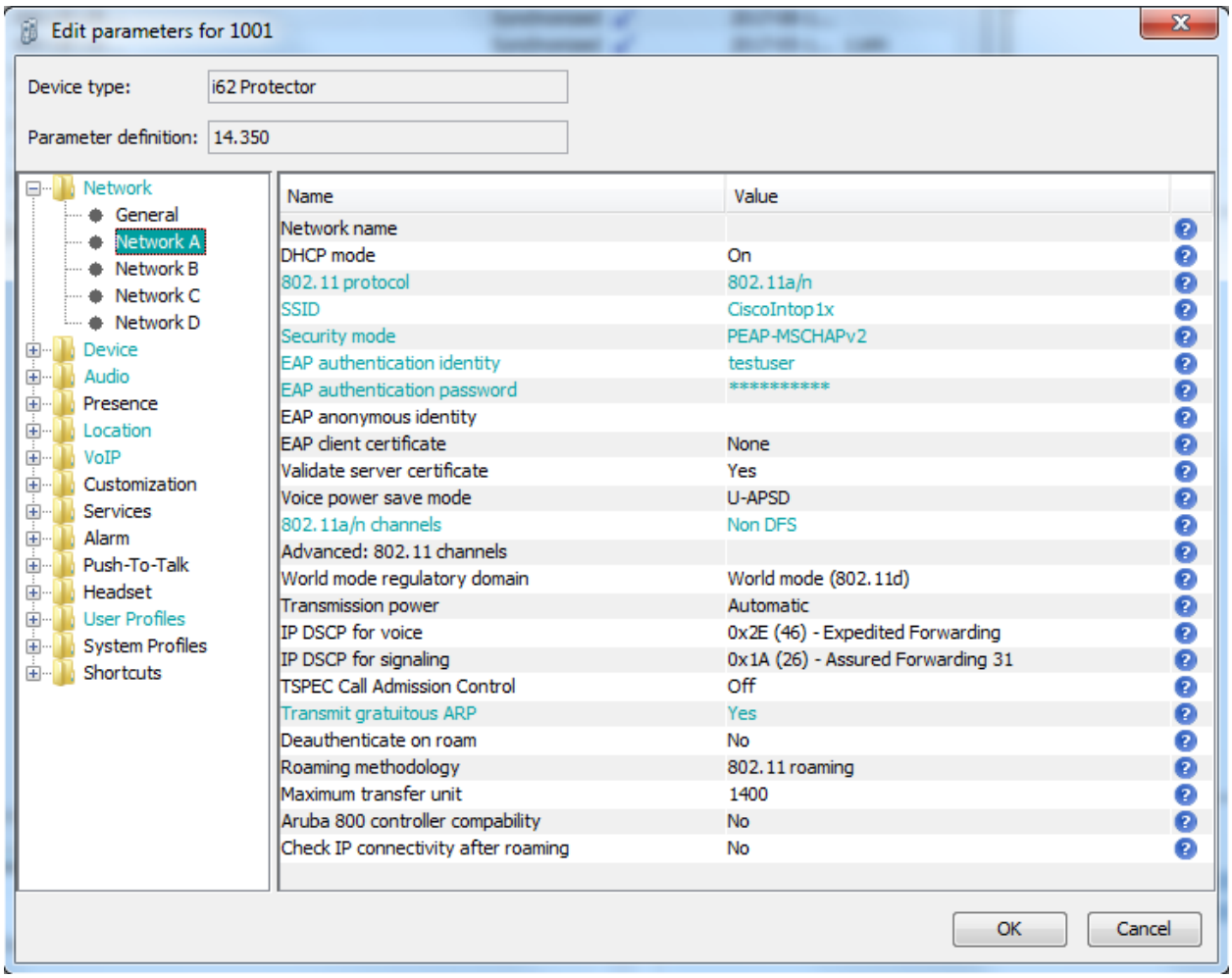

Depending on the infrastructure (switches) ”Protocol Type” may have to be disabled.



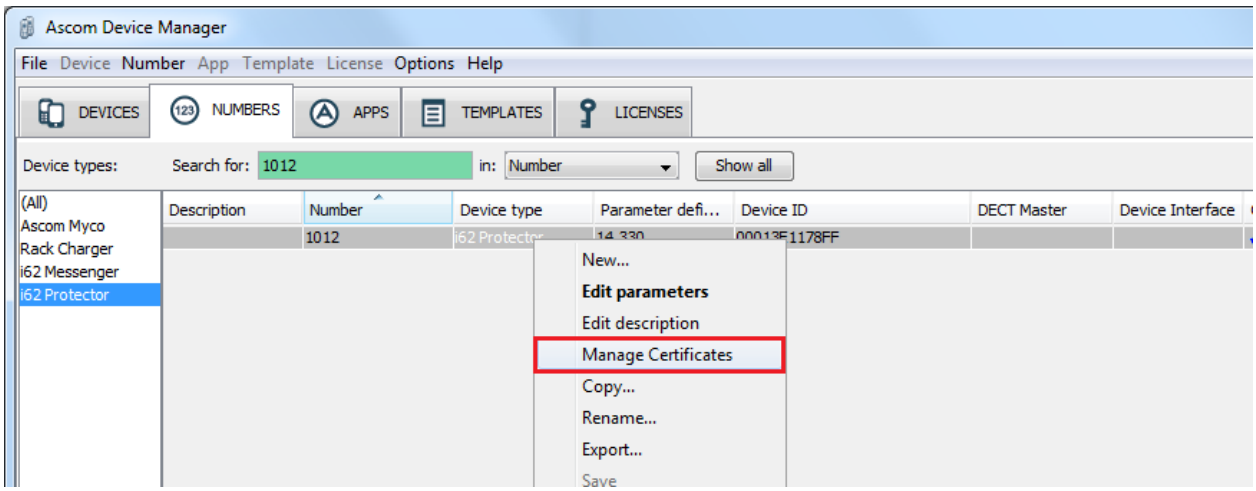

Network settings for WPA2-PSK

**Note. Make sure that the enabled channels in the i62 handset match the channel plan used in the system.**

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




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




802.1X Authentication requires a CA certificate to be uploaded to the phone by “right clicking” - > Edit certificates. EAP-TLS will require both a CA and a client certificate.

***Note that both a CA and a client certificate are needed for TLS. Otherwise only a CA certificate is needed. Server certificate validation can be overridden in version 4.1.12 and above per handset setting.***

# Appendix B: Interoperability Validation Records

| | |
|---|---|
| Pass | 17 |
| Fail | 0 |
| Comments | 0 |
| Not validated | 6 |
| **Total** | 23 |

Refer to the attached file for detailed validation results.

Refer to the validation specification for explicit information regarding each validation case.
The specification can be found here (requires login):
https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/

# Document History

| Rev | Date | Author | Description |
|---|---|---|---|
| P1 | 9-June-20 | SEKMO | Draft |
| R1 | 17-June-20 | SEKMO | Internal review. R1 status. |
| | | | |
| | | | |