

# **BLiNQ Networks**

## **FW-300i Intelligent LTE Base Station**

### ***User Manual***

**Software Release 2.0.13**

**Oct 2020**

## Revision History

VERSION (YYMMDD)	REASON FOR ISSUE
201002	Initial User Manual release for SW 2.0.13

### Contact Information:

BLiNQ Networks (CCARI)  
140 Renfrew Drive, Suite 200  
Markham, ON L3R 6B3

### Web Site:

<http://www.blingnetworks.com>

### Sales Inquiries:

Email: [sales@blingnetworks.com](mailto:sales@blingnetworks.com)  
Telephone: 1-416-214-4204

### Customer Support:

Email: [support@blingnetworks.com](mailto:support@blingnetworks.com)  
Telephone: 1-416-214-4204

## Table of Contents

<b>1</b>	<b>About This Manual .....</b>	<b>1</b>
1.1	Manual Conventions.....	2
<b>2</b>	<b>FW-300i System Overview.....</b>	<b>3</b>
2.1	Technical Features.....	4
2.2	Network Management Features .....	6
2.2.1	FW-300i Security Protocols.....	8
2.2.1.1	Local Networking Protocols .....	8
<b>3</b>	<b>Technical Specifications .....</b>	<b>9</b>
3.1	System Parameters.....	10
3.2	System Enclosure.....	13
3.3	Antenna Patterns.....	14
<b>4</b>	<b>Getting Started with the FW-300i .....</b>	<b>15</b>
4.1	FW-300i Web User Interface (WebUI).....	16
4.1.1	Common Tools .....	17
4.1.1.1	Title Bar: Tool Area.....	17
4.1.1.2	Minimized and Maximized Menus.....	18
4.1.1.3	System Information Bar .....	19
4.1.2	System Status Messages .....	19
4.2	Default FW-300i Configuration.....	20
<b>5</b>	<b>Configuration.....</b>	<b>21</b>
5.1	System Configuration Process .....	22
5.2	Configuration with the WebUI .....	23
5.2.1	System.....	23
5.2.1.1	Configuring a System Name .....	24
5.2.1.2	System Synchronization .....	24
5.2.1.3	Network Connectivity Parameters.....	26
5.2.1.4	Advanced Options .....	27
5.2.2	Carriers.....	29
5.2.2.1	Setting up Carriers Baseline Parameters.....	29
5.2.2.2	Set Cells 0-2 RF Parameters .....	30
5.2.2.3	Advance Option.....	34
5.2.3	LTE Baseline .....	36
5.2.3.1	Configuring LTE Baseline Parameters .....	36
5.2.3.2	eNB Identifiers .....	40
5.2.3.3	EPC Settings.....	40
5.2.3.4	Advanced Options .....	42

5.2.4	Embedded EPC.....	44
5.2.4.1	APN Configuration.....	45
5.2.4.2	UE Templates .....	47
5.2.4.3	Embedded MAC Proxy .....	50
5.2.4.4	Subscriber Configuration.....	50
5.2.5	CBSD.....	55
5.2.5.1	Configure SAS Server Connectivity.....	55
5.2.5.2	ENB Settings .....	57
5.2.6	Management.....	58
5.2.6.1	SSH/Web Users .....	58
5.2.6.2	Syslog.....	61
5.2.6.3	SNMP.....	62
5.2.7	Verify, Save and Activate Current Running Configuration.....	67
5.2.7.1	Verify and Save Running Configuration .....	67
<b>6</b>	<b>Operation and Maintenance .....</b>	<b>68</b>
6.1	Operation and Maintenance with the WebUI.....	69
6.1.1	Administration .....	69
6.1.1.1	Software Manager.....	69
6.1.1.2	SAS Cert Download .....	72
6.1.1.3	IPSec Cert Download.....	73
6.1.1.4	Configuration Manager.....	74
6.1.2	Performance .....	76
6.1.2.1	eNB Stats Page .....	76
6.1.2.2	UE Stats Page.....	77
6.1.2.3	Core Connectivity Status.....	78
6.1.2.4	Trace Log Files .....	78
6.1.2.5	KPI Reports.....	79
6.1.3	Events.....	81
6.1.3.1	Alarms Page.....	81
6.1.3.2	History Page .....	82
6.2	Troubleshooting .....	82
<b>7</b>	<b>Customer Premise Equipment (CPE) .....</b>	<b>84</b>
<b>Appendix A</b>	<b>BLiNQ Wireless Devices and RF Safety/Les appareils sans fil BLiNQ et la sécurité RF ....</b>	<b>85</b>
A.1	Equipment Compliance .....	87
A.1.1	Federal Communications Commission (FCC) Notices.....	87
<b>Appendix B</b>	<b>PCI Planning Guidelines.....</b>	<b>88</b>
<b>Appendix C</b>	<b>Alarms and Events (Fault Management) .....</b>	<b>89</b>
<b>Appendix D</b>	<b>List of Acronyms .....</b>	<b>93</b>

## List of Figures

Figure 2-1	FW-300i Mounted on a Pole .....	3
Figure 2-2	FW-300i Sectors with Antenna Pattern .....	5
Figure 2-3	Antenna Sectors with Examples of CA Mapping.....	5
Figure 3-1	FW-300i (back and front respectively).....	13
Figure 3-2	Band 42, 43, 48 Antenna Patterns .....	14
Figure 4-1	Welcome FW-300i Screen.....	16
Figure 4-2	Title Bar – Tool Area Identification .....	18
Figure 4-3	View Maximized.....	18
Figure 4-4	FW-300i WebUI System Success Status Message.....	19
Figure 4-5	FW-300i WebUI Warning Message.....	19
Figure 4-6	FW-300i WebUI Error Message.....	19
Figure 5-1	FW-300i Configuration Process.....	22
Figure 5-2	FW-300i Sectors .....	31

## List of Tables

Table 3-1	FW-300i System Parameters.....	10
Table 3-2	FW-300i HP System Parameters .....	11
Table 4-1	FW-300i Default Configuration Values.....	20
Table 6-1	Troubleshooting Guide .....	82
Table 7-1	List of Alarms.....	91
Table 7-2	List of Events .....	92

# 1 About This Manual

This manual contains informational and overview chapters, and then continues as a guide to the recommended order that you configure and then monitor your FW-300i system. **It covers features from SW Version 2.0.13 onwards.** If a certain feature is specific to a software version, it will be indicated in the respective sections.

There are two methods to configure the FW-300i:

- FW-300i Web-based User Interface (WebUI) (recommended) or
- Command Line Interface (CLI)

This user manual contains step-by-step instructions for the FW-300i WebUI. For information about CLI configurations, please contact BLiNQ Technical Support Team.

The WebUI menu structure is the basis for the order of the chapters and the processes contained within those chapters:

- Initial system setup: See **Chapter 4, “Getting Started with the FW-300i”**
- Configuration: See **Chapter 5, “Configuration”** for configuring the FW-300i system using WebUI; See Section 5.2, “~~Configuration with the WebUI~~*Configuration with the WebUI*”
- Operation and Maintenance: See **Chapter 6, “Operation and Maintenance”**
  - Software upgrade
  - Performance containing eNB and Customer Premise Equipment (CPE) statistics plus trace log files and measurements
  - Events including alarms and past events (History)
  - Troubleshooting
- Management: See **Chapter 5.2.6, “Management”**
  - User operations (Local security)
  - Simple Network Management Protocol (SNMP)
  - Syslog server








## 1.1 Manual Conventions

**Bold** words indicate actual page names, fields or buttons within the software.

Examples:

- In the **LTE Baseline Parameters** section, set the **Cell range** to the desired kilometer range. The range is from 1 to 100 kilometers.

### LTE Baseline

 LTE Baseline Parameters					
Subframe Assignment	<input type="text" value="2"/>		Special Subframe	<input type="text" value="7"/>	
Baseline eNB ID	<input type="text" value="100"/>		PCI Seed Value	<input type="text" value="10"/>	
Cell range (km)	<input type="text" value="2"/>		Tracking Area Code	<input type="text" value="1"/>	

- Most FW-300i WebUI pages have a **Commit** button in the top right hand corner.

 Welcome, admin    

 System  

**Commit Button** 

## 2 FW-300i System Overview

BLiNQ Networks is a pioneer of next-generation wireless solutions that feature intelligent systems capable of adapting to the radio frequency environment to maximize capacity and performance.



**Figure 2-1 FW-300i Mounted on a Pole**

The BLiNQ FW-300i system is a tri-sector and tri-carrier Long-Term Evolution (LTE) Evolved Node B (eNB) with the capability to operate in the following bands: 42, 43, 46 and 48 (Citizens Broadband Radio Service (CBRS)). With a distinctive feature set and integration level, the FW-300i brings an ideal solution to an “install anywhere” micro-base transceiver station (micro-BTS) that fully serves private networks, fixed wireless access and mobility use cases.



## 2.1 Technical Features

---

Some of the main technical product characteristics are as follows:

- **‘All-In-One’ Fully Integrated Solution:** The FW-300i solution packs a three (3) sector 180-degree integrated antenna (60-degrees per sector) with an integrated Global Positioning System (GPS) sync source. There is also an additional option for an integrated Evolved Packet core (EPC), making deployment of the FW-300i as simple as deploying Wi-Fi.
- **Compact All-Outdoor and Zero-Footprint Form Factor:** The FW-300i packs three (3) carrier radios in one compact form. The FW-300i meets IP67 requirements for operation in tough environments with the capability to handle temperature variations from extreme cold to extreme heat. BLiNQ’s state-of-the-art and unique mounting design allows an unobtrusive deployment of multiple FW-300i systems on towers, poles, building sidewalls or rooftops with ease (See the “**FW-300i Installation Guide**” for more details).
- **For CBRS Band:** The FW-300i implements a native Spectrum Access System client that fully enables easy Citizens Broadband Radio Service (CBRS) deployments. With each cell designed to operate as an independent Type B CBSD, the FW-300i can operate on a Priority Access or General Authorized Access basis in the CBRS band consistent with Title 47 CFR Part 96.
- **Industry Standard TDD LTE-A Release 13 Radio Interface:** The FW-300i solution utilizes industry standard Time Division Duplexing (TDD) LTE-A Release 13 radio capabilities. This allows for robust wireless performance, with extremely cost-effective deployments of Customer Premise Equipment (CPE).
- **Configuration:** The FW-300i supports all LTE TDD frame configurations but focuses on Category 1 and Category 2.
- **Carrier Aggregation:** The FW-300i supports carrier aggregation (CA) with up to three (3) Component Carriers (3CC), allowing for increased throughput to support high bandwidth deployments in both dense suburban and rural environments.
- **Software Controlled Adaptive Carrier Steering:** The FW-300i is able to steer, with variable capacity, over different areas across 180 degrees of azimuth. The unit powers this steering ability by its integrated antenna system of three (3) sectors of 60 degrees each. This flexibility allows the FW-300i to support both large coverage models, as well as capacity driven models. The FW-300i supports three modes via software (SW) configuration:
  - 3 Sector covering 180 degrees each of 1 x 20 MHz carrier
  - 2 Sector covering 120 degrees (one sector with 2 x 20 MHz carriers and one sector with 1 x 20MHz carrier)
  - 1 Sector covering 60 degrees: one sector with 3 x 20 MHz carriers

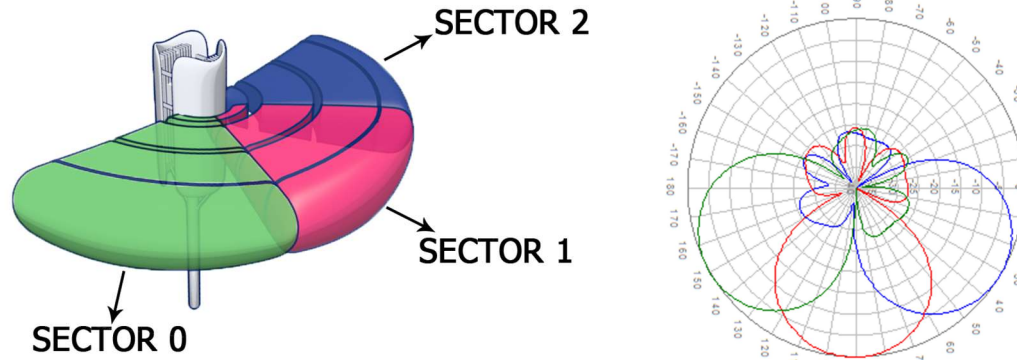


Figure 2-2 FW-300i Sectors with Antenna Pattern

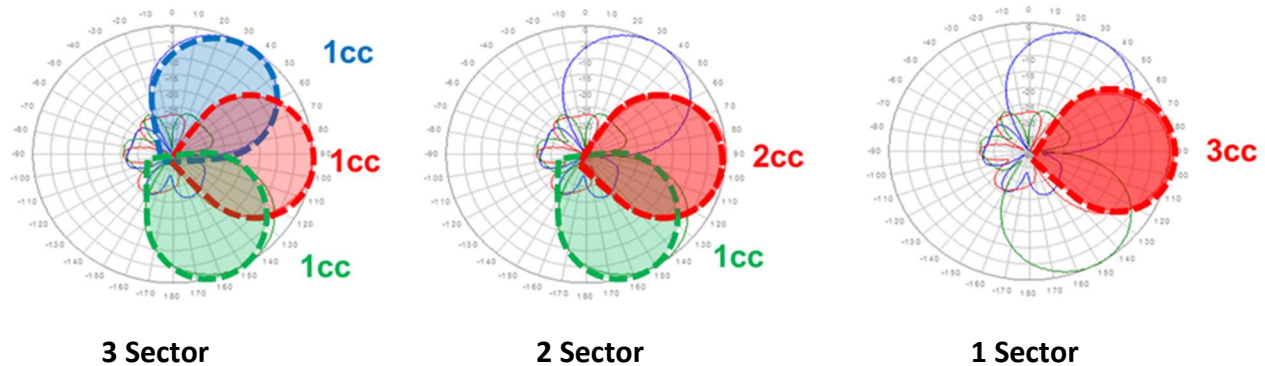


Figure 2-3 Antenna Sectors with Examples of CA Mapping

- **Multiple Input Multiple Output (MIMO):** The FW-300i system features standard 2x2 MIMO configurations in both downlink (DL) and uplink (UL) directions for each active sector.
- **High Modulation and Coding Scheme (MCS):** The FW-300i hardware supports high MCS:
  - Downlink (DL): 256 Quadrature Amplitude Modulation (QAM) and
  - Uplink (UL): 64 QAM
 Please refer to the latest SW release notes for the availability of these features.
- **Quality of Service (QoS):** The FW-300i system implements advanced features such Traffic Classification, Admission Control, Rate Shaping plus Active Scheduling and Queue Management in order to deliver the most optimal quality of service.

## 2.2 Network Management Features

---

The FW-300i implements complete web-based user interface (WebUI) and Command Line Interface (CLI) functionality, plus strong Element Management System (EMS) implementation that suits any type of customer needs.

- **FW-300i Web Interface (WebUI)** — Accessible via HTTP(S), the FW-300i WebUI provides an interactive visual toolset that allows you to modify the full configuration of the FW-300i system, as well as view state, fault and performance indicators. The FW-300i WebUI displays performance data using visual charts and provides applications to visualize up to 24 hours of historical performance data stored on the system.
- **FW-300i Command Line Interface (CLI)** — Accessible via Secure Shell protocol (SSH), the FW-300i CLI provides a well-structured command language in an industry standard idiom. The interface allows you (or third-party system) to manipulate the full configuration of the unit and examine state, performance and fault indicators.
- **Element Management System (EMS)** — The BLiNQ EMS system, enables a state-of-the-art Operations, Administration, Maintenance and Provisioning (OAM&P) feature set. The OAM&P possesses a strong set of interfaces to connect to northbound provision systems.

Providing comprehensive Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality, the FW-300i system uses standard networking protocols and tools that facilitate a full range of element and network management operations—from local craft configuration, to complex integration in Simple Network Management Protocol (SNMP) or script-based Element Management System (EMS) and Operations Support System (OSS) infrastructures.

- **Community-Based Simple Network Management Protocol version 2 (SNMPv2c)** — The SNMPv2c interface provide complete access to configuration, state, performance and fault information in the FW-300i system. This allows for high levels of integration in existing EMS/OSS infrastructure for monitoring, Service Level Agreement (SLA) assurance and administrative task automation.
- **Syslog** — The syslog interface allows the FW-300i system to send standard syslog fault management information (that is, syslog alarms, events and log entries) to external syslog servers.

The FW-300i system provides the following IP addresses for management purposes:

- **Local Craft IP Address** — A fixed, non-routable IP address: **169.254.1.1** which is always accessible without VLAN encapsulation. This address is always present on eNodeB. You use this address in situations where the Management IP Address (see below) is not configured or is unavailable, including initial commissioning and field troubleshooting scenarios. Typically, a technician accesses the Local Craft IP Address by plugging directly into the RJ45 Ethernet port of the eNodeB.
- **WAN IPv4 IP Address** — A user assigned, static or Dynamic Host Configuration Protocol (DHCP) IPv4 address. The device uses this IPv4 address to exchange traffic and control information with the network. The operator will use this IPv4 address to remotely manage the system. A user-configurable Virtual Local Area Network (VLAN) encapsulates all traffic to and from the WAN interface.

The FW-300i system provides the following network management functions:

- **Configuration Management** — The system configuration covers several functional areas:
  - *Radio Link Commissioning*  
Radio Link Commissioning parameters (for example, radio frequency, synchronization, TDD configuration) needs to be set *before* system deployment and are particular to the operator RF network.
  - *EPC Configuration*  
The Evolved Packet Core (EPC) Configuration parameters configure the EPC interface (e.g. Public Land Mobility Network Identifier (PLMN-ID), Mobility Management Entity (MME) interface, Serving Gateway (SGW) interface).
  - *Security Configuration*  
Security Configuration parameters allow you to secure access or disable specific management interfaces (add local user accounts) and perform various unit administrative operations.
  - *EMS Interfaces Configuration*  
Element Management Systems (EMS) enables you to configure SNMP, Syslog, plus the automatic upload of Performance Management (PM) files.

All parameters in these areas are accessible via all of the network management interfaces previously described.

- **Fault Management** — The FW-300i system provides fault management service via a comprehensive list of alarms and events. Some of the potential faults that the system detects and initiates alarms on include:
  - radio and Ethernet link failures
  - hardware module failures
  - synchronization faults
  - software module faults

SNMP traps or Syslog relays all alarms and events to higher level managers. The system also allows you to access active alarm and event history information using either the FW-300i CLI or WebUI.

- **Performance Management** — The FW-300i system maintains a comprehensive set of performance counters and indicators to facilitate:
  - performance monitoring
  - Service Level Agreement (SLA) monitoring
  - troubleshooting

The system provides a full set of Ethernet counters at the interface, module and service flow level, as well as radio quality indicators at the module level. The system makes all the counters available as either instantaneous values (via SNMP, CLI or WebUI) or historical performance files. The system maintains 24 hours of performance data at a 15 minute granularity. The eNodeB only stores performance files and can be extracted from the system on-demand.

- **Administrative Operations** — The FW-300i system provides tools that allow you to perform all standard unit administration operations using the provided remote network management interfaces. The system supports remote software upgrade operations using either a pull paradigm (that is, the system modules retrieve the software package files from external FTP servers) or a push scheme using the FW-300i WebUI (that is, you upload a software package file to the system modules using the FW-300i WebUI). The FW-300i system also supports remote configuration backups and backup restoration.

## 2.2.1 FW-300i Security Protocols

The FW-300i system supports local security access regarding system configuration and maintenance. With this model, you can, through CLI or WebUI, configure the user name, password and access level for the user. The configuration is stored on the FW-300i.

### 2.2.1.1 Local Networking Protocols

Local security protocol is the default protocol for the FW-300i modules. This means that you set each username, password and access level on each module. Each module stores the configuration data in its configuration database.

To configure the local security:

- with the WebUI see Section 5.2.6.1, “SSH/Web User~~SSH/Web User~~” or
- with CLI, please contact BLiNQ Technical Support for more details.

## 3 Technical Specifications

This chapter covers:

- System Parameters,
- System Enclosure and
- Antenna Patterns.

## 3.1 System Parameters

Table 3-1 lists the FW-300i system parameters for the North American (NA) product line.

Table 3-2 lists the FW-300i HP system parameters for the North America (NA) product line.

**Table 3-1 FW-300i System Parameters**

RADIO SPECIFICATIONS	
<b>Frequency Band</b>	3.55-3.70 GHz (LTE Band 48 - CBRS)
<b>Transmit Power</b>	32 dBm per sector of 60 degrees (deg) 29 dBm per antenna port 17 dBi Integrated Antenna → 52 dBm EIRP/Sector; 49 dBm EIRP/port
<b>Channel Bandwidth</b>	10, 20 MHz
<b>MIMO</b>	2TX x 2RX (several possible MIMO configurations)
<b>LTE Compliance</b>	3GPP Release 10 (SW upgrade to Release 13)
PERFORMANCE AND ATTRIBUTES	
<b>Connected/Active User Equipment (UE)</b>	Up to 96 active users per sector; 288 active users per box
<b>Carrier Aggregation</b>	Supports contiguous and non-contiguous 1CC, 2CC, 3CC, covers full CBRS band (150 MHz)
<b>Throughput DL TDD</b>	3GPP Release 10 (Software (SW) upgrade to Release 13)
<b>Throughput UL TDD</b>	3GPP Release 10 (SW upgrade to Release 13)
<b>Operating Mode</b>	TD-LTE
<b>Power Consumption</b>	150 W maximum
<b>Power</b>	48 VDC
<b>Connectivity</b>	Default: 1 x Copper 1000BaseT; Optional: 1 x SFP
<b>Synchronization</b>	Integral GPS antenna (GPS, GLONASS, BeiDou), Optional: External GPS, 1588v2
<b>Citizens Broadband Radio Service (CBRS)</b>	CBSD Type B SAS Support
<b>Embedded Evolved Packet Core (EPC)</b>	Software Option
OPERATIONS, ADMINISTRATION AND MAINTENANCE (OAM)	
<b>Configuration</b>	WebUI/CLI, radio and Ethernet performance monitoring
<b>EMS Integration</b>	SNMP v2c
<b>OAM Protocols</b>	NETCONF, HTTP(S), (S)FTP, SSH, TR-069/TR-196
ANTENNA SPECIFICATIONS CBRS BANDS 42/43 (48)	
<b>Gain</b>	17 dBi
<b>Azimuth Coverage (-5 dB)</b>	180 degrees
<b>Azimuth Beamwidth (-3 dB)</b>	45 degrees
<b>Azimuth Beamwidth (-5 dB)</b>	60 degrees
<b>Elevation Beamwidth (-3 dB)</b>	10 degrees
<b>Electrical Downtilt</b>	0 degree

ANTENNA SPECIFICATIONS CBRS BANDS 42/43 (48) (CONT.)	
<b>Azimuth Sidelobe</b>	< -25 dB (Typ.)
<b>Front-to-Back Ratio @180 Degrees</b>	> 30 dB (Typ.)
<b>Co-Polar Port-to-Port Isolation</b>	15 dB (Typ.)
<b>Cross-Polarization Port-to-Port Isolation</b>	> 20 dB (Typ.)
<b>Max. Voltage Standing Wave Ratio (VSWR)</b>	1.5:1
<b>Polarization</b>	Dual Pol 45 degrees
<b>Lightning Protection</b>	DC Ground
MECHANICAL	
<b>Dimensions (L x W x D)</b>	13.78" x 22.4" x 8.9" (350 x 570 x 227 mm)
<b>Survival Wind Speed</b>	> 124 mph (200 km/hour)
<b>Weight</b>	26.5 lbs. (12.0 Kg)
<b>Operational Temperature</b>	-40 to 60 degrees Celsius (-40 to 140 degrees Fahrenheit)
<b>Mechanical Uptilt/Downtilt</b>	0 - 10 degrees

Table 3-2 FW-300i HP System Parameters

RADIO SPECIFICATIONS	
<b>Frequency Band</b>	3.40-3.80 GHz (LTE Band 42/43) 3.55-3.70 GHz (LTE Band 48 - CBRS) 5.15-5.925 GHz (LTE Band 46)
<b>Transmit Power</b>	17 dBi Integrated Antenna → up to 53 dBm EIRP/Sector LTE Band 42/43: -10 dBm up to +36 dBm per TX port (add 3 dBm for aggregate power) LTE Band 48: -10 dBm up to +30 dBm (add 3 dBm for aggregate power)
<b>Channel Bandwidth</b>	3 x 10 MHz or 3 x 20 MHz (15 MHz*)
<b>MIMO</b>	2TX x 2RX (several possible MIMO configurations)
<b>LTE Compliance</b>	3GPP Release 10 (SW upgrade to Release 13)
PERFORMANCE AND ATTRIBUTES	
<b>Connected/Active User Equipment (UE)</b>	Up to 96 active users per sector; 288 active users per box
<b>Carrier Aggregation</b>	Supports contiguous and non-contiguous 1CC, 2CC, 3CC, covers full CBRS band (150 MHz)
<b>Throughput DL TDD Config 2-7 (default)</b>	105 Mbps
<b>Throughput UL TDD Config 2-7 (default)</b>	10 Mbps
<b>Operating Mode</b>	TD-LTE
<b>Power Consumption</b>	180 W maximum
<b>Power</b>	48 VDC
<b>Connectivity</b>	Default: 1 x Copper 1000BaseT; Optional: 1 x SFP
<b>Synchronization</b>	Integral GPS antenna (GPS, GLONASS, BeiDou), Optional: External GPS, 1588v2



<b>Citizens Broadband Radio Service (CBRS)</b>	CBSD Type B SAS Support
<b>Embedded Evolved Packet Core (EPC)</b>	Software Option
<b>OPERATIONS, ADMINISTRATION AND MAINTENANCE (OAM)</b>	
<b>Configuration</b>	WebUI/CLI, radio and Ethernet performance monitoring
<b>EMS Integration</b>	SNMP v2c
<b>OAM Protocols</b>	NETCONF, HTTP(S), (S)FTP, SSH, TR-069/TR-196
<b>ANTENNA SPECIFICATIONS BANDS 42/43, 48</b>	
<b>Gain</b>	17 dBi
<b>Azimuth Coverage (-5 dB)</b>	180 degrees
<b>Azimuth Beamwidth (-3 dB)</b>	45 degrees
<b>Azimuth Beamwidth (-5 dB)</b>	60 degrees
<b>Elevation Beamwidth (-3 dB)</b>	10 degrees
<b>Electrical Downtilt</b>	0 degree
<b>Azimuth Sidelobe</b>	< -25 dB (Typ.)
<b>Front-to-Back Ratio @180 Degrees</b>	> 30 dB (Typ.)
<b>Co-Polar Port-to-Port Isolation</b>	15 dB (Typ.)
<b>Cross-Polarization Port-to-Port Isolation</b>	> 20dB (Typ.)
<b>Max. Voltage Standing Wave Ratio (VSWR)</b>	1.5:1
<b>Polarization</b>	Dual Pol 45 degrees
<b>Lightning Protection</b>	DC Ground
<b>MECHANICAL</b>	
<b>Dimensions (L x W x D)</b>	13.78" x 22.4" x 8.9" (350 x 570 x 227 mm)
<b>Survival Wind Speed</b>	> 124 mph (200 km/hour)
<b>Weight</b>	26.5 lbs. (12.0 Kg)
<b>Operational Temperature</b>	-40 to 60 degrees Celsius (-40 to 140 degrees Fahrenheit)
<b>Mechanical Uptilt/Downtilt</b>	0 - 10 degrees

## 3.2 System Enclosure

---

The enclosure for the FW-300i is a rugged IP67 casing, supplied with an optional mounting bracket with both horizontal and vertical tilt capabilities to mount the unit on towers, poles and building side walls. These cases allow for full flexibility in the range of orientation to establish best connectivity between the FW-300i and Customer Premise Equipment (CPE).



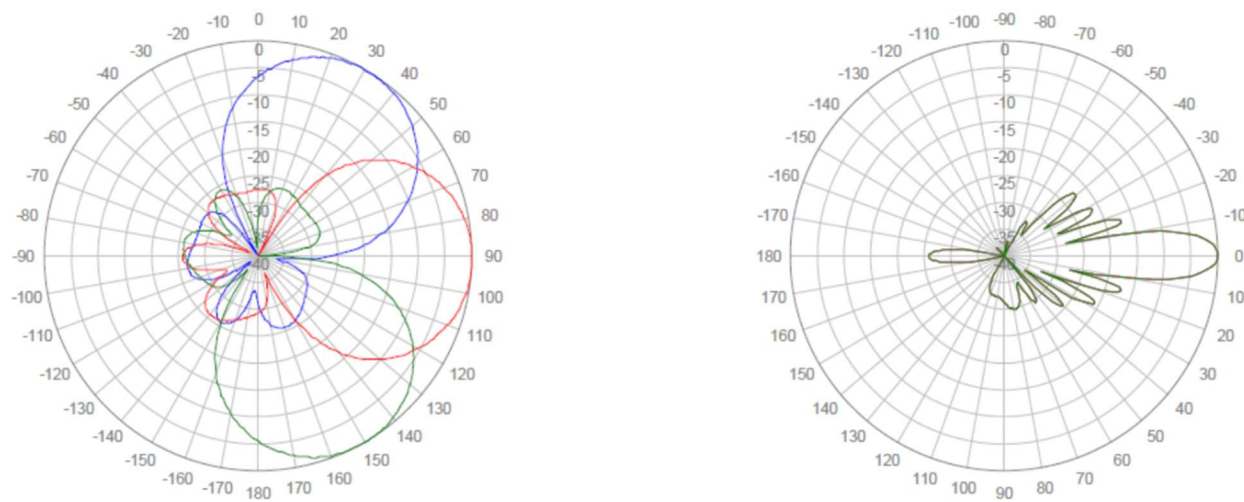
**Figure 3-1 FW-300i (back and front respectively)**

The mechanical enclosure for the FW-300i has an integrated antenna. There are two ports on the bottom of the FW-300i: a -48VDC power port and an Ethernet port for network connectivity. The Ethernet port comes pre-populated with 1 Gbps (100 Base-T) copper Small Form-factor Pluggable (SFP). If needed, you can replace this SFP with 1 Gbps fiber SFP.

An integrated Global Positioning System (GPS) antenna is included in the FW-300i antenna, yet if needed, the FW-300i has a SYNC port, to use for example, as an optional external GPS Pulse per Second (PPS) source. Therefore, there is no need for additional synchronization equipment which reduces total cost of ownership.

### 3.3 Antenna Patterns

The FW-300i covers up to 180 degree of azimuth which is powered by an integrated adaptive antenna system of 3 x 60 degree sectors. Following are the antenna patterns for Band 42, 43, 48 and then by the antenna patterns for Band 46.



**Figure 3-2 Band 42, 43, 48 Antenna Patterns**

## 4 Getting Started with the FW-300i

To initially log in to the FW-300i:



**Notes:**

- If required, consult the “**FW-300i Installation Guide**” for instructions on powering the unit.
- Connect your computer directly to the FW-300i through an Ethernet cable, and then check your connectivity by pinging the FW-300i using **169.254.1.1** (the Craft IP address that is always accessible).



**Note:** You need to statically set the IP address on the computer to 169.254.1.x subnet before pinging.

After successfully pinging the Craft IP address:

- Use a Secure Shell (SSH) client to log on to the FW-300i CLI using a SSH connection to the pinged 169.254.1.1 address. However, you must install SSH version 2.0 or higher client software on your host computer (you can use SSH version 1.0, but it is not recommended), or
- Open a web browser and navigate to the pinged 169.254.1.1 to bring up the FW-300i WebUI

To complete the initial system setup with the WebUI, follow the procedures under the desired chapter.

If you wish to complete the initial system setup with CLI, please contact BLiNQ Technical Support for more information.

## 4.1 FW-300i Web User Interface (WebUI)

### Login Credentials:

When prompted for login credentials, enter the default username and password: **admin/admin**.

On initial log in to the FW-300i Web User Interface (WebUI), you see an overview of the FW-300i details; BLINQ refers to these FW-300i details as the **Dashboard**. [Figure 4-1](#) ~~Figure 4-1~~, Welcome FW-300i Screen identifies the various elements of the FW-300i WebUI.

**Title Bar: Tool Area**

**Dashboard Navigation Bar**

**Increase Width Button**

**System Information Bar**

**System Overview**

System Name	Blinq eh8	Local Time	Sep 16, 2020 12:35:12 AM (UTC-04:00)
Device Model	RevC05	Uptime	5 days 10 hr 41 min 12 sec
Device Code	FW03004848NALzzzz	WAN IP Address	192.168.32.2
Serial Number	60101CS-18520037	WAN IPv6 Address	fe80::ea1:38ff:fe00:1
Software Version	2.0.12_1	WAN IF MAC Address	0ca1:38:00:00:01
GPS	Local (Free Run)	S1-MIME	Connected
Operational Status	Degraded, 3 major alarms active		
Licenses			

**Alarms**

ID	Alarm ID	Module ID	Alarm Time	Component	Severity	Type	Probable Cause	Description
6	11002	0ca1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#0	Major	Operational-status	Operating-mode	cell#0 has noise (-119.6) above normal level (-125)
7	11002	0ca1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#1	Major	Operational-status	Operating-mode	cell#1 has noise (-121.9) above normal level (-125)
8	11002	0ca1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#2	Major	Operational-status	Operating-mode	cell#2 has noise (-122.2) above normal level (-125)

Showing 3 of 3 entries

BLINQ Networks © 2020

Model: RevC05 Serial Number: 60101CS-18520037 Version: 2.0.12\_1 EEPROM Version: 3.2.54

**Figure 4-1 Welcome FW-300i Screen**

The dashboard gives you the summary of your system. This is the first page that you will land on after you log into the WebUI.

It shows you the **System Overview**, which includes the **System Name**, **Device Code**, **Serial Number**, **Software Version**, **Operational Status** just to name a few.

**System Overview**

System Name	Blinq eh8	Local Time	Sep 16, 2020 12:35:12 AM (UTC-04:00)
Device Model	RevC05	Uptime	5 days 10 hr 41 min 12 sec
Device Code	FW03004848NALzzzz	WAN IP Address	192.168.32.2
Serial Number	60101CS-18520037	WAN IPv6 Address	fe80::ea1:38ff:fe00:1
Software Version	2.0.12_1	WAN IF MAC Address	0ca1:38:00:00:01
GPS	Local (Free Run)	S1-MIME	Connected
Operational Status	Degraded, 3 major alarms active		
Licenses			

Please note that the serial number shown represents the serial number of your FW-300i Unit. It will come with the prefix of “FI03-YYWWNNNN”, where “YY” is the year, “WW” is the week and “NNNN” is the unit number produced in that particular year and week.


There are two tabs at the bottom: **Alarms** and **LTE Cells Status**


- **Alarms:** Errors on your system will appear in this section, giving you the **Alarm ID, Alarm Time, Component, Severity, Type, Probable Cause** and **Description** of the error.

Operational Status

Degraded, 3 major alarms active

Licenses

 Alarms

 LTE Cells Status

ID	Alarm ID	Module ID	Alarm Time	Component	Severity	Type	Probable Cause	Description
6	11002	0c:a1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#0	Major	Operational-status	Operating-mode	cell#0 has noise (-119.6) above normal level (-125)
7	11002	0c:a1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#1	Major	Operational-status	Operating-mode	cell#1 has noise (-121.9) above normal level (-125)
8	11002	0c:a1:38:00:00:01	Sep 10, 2020 1:55:39 PM (UTC-04:00)	Cell#2	Major	Operational-status	Operating-mode	cell#2 has noise (-122.2) above normal level (-125)

Showing 1 to 3 of 3 entries

First1Last

- **LTE Cells Status:** This is where you can monitor the LTE Cells' operational parameters.

Operational Status

Degraded, 3 major alarms active

Licenses

Alarms

LTE Cells Status

LTE Cell	Attached UEs	S1-MME	CBSD	eNBID	PCI	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Active Secondary Cells
0	0	Connected	Not Configured	33792	30	3580	23	None
1	1	Connected	Not Configured	33793	31	3680	23	None
2	1	Connected	Not Configured	33794	32	3685	23	None

## 4.1.1 Common Tools

Following are some common features of the FW-300i WebUI.

### 4.1.1.1 Title Bar: Tool Area

Most FW-300i WebUI pages have either a **Commit** button or a **Refresh** button or both in the top right hand corner.

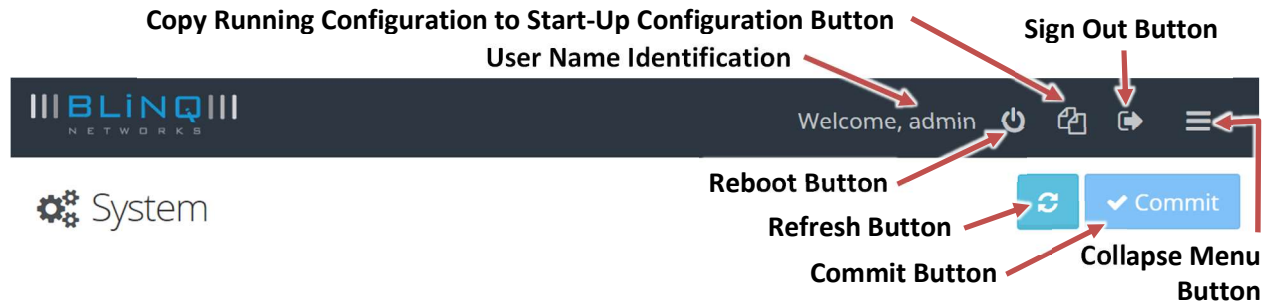


Figure 4-2 Title Bar – Tool Area Identification

- **Commit** button: If you change any settings on a page, select **Commit** *before* navigating to another page to save your changes.
- **Refresh** button: Updates any read-only data on a page or returns any altered settings to their original values.
- **Copy Running Configuration to Start-Up Configuration** button (📄): Makes any configuration changes persistent over system reboots.
- **Reboot** button (🔄): Reboot the FW-300i, at any time. It is available at the top of every page.

**Note:** Before a reboot, the FW-300i system performs a verification check between the running configuration and the startup configuration to determine if there are any changes. This is to prevent the loss of any changes. If there is a change, the system prompts you to save your changes.

- **Sign Out** button: Ends each session.
- **Collapse Menu** button (☰): Minimizes the **Dashboard Navigation Bar** on the left side. You can still access the menu by positioning your cursor over the thin visible portion of the **Dashboard Navigation Bar**. Select the **Collapse Menu** button again to make the menu visible again.

#### 4.1.1.2 Minimized and Maximized Menus

When a plus sign (+) is present beside a menu title, this indicates that you can minimize/maximize this area to reduce or see more options. To maximize an area, select the plus sign (+); the area expands so that all options are visible. To minimize, select the minus sign (-); the menu closes.

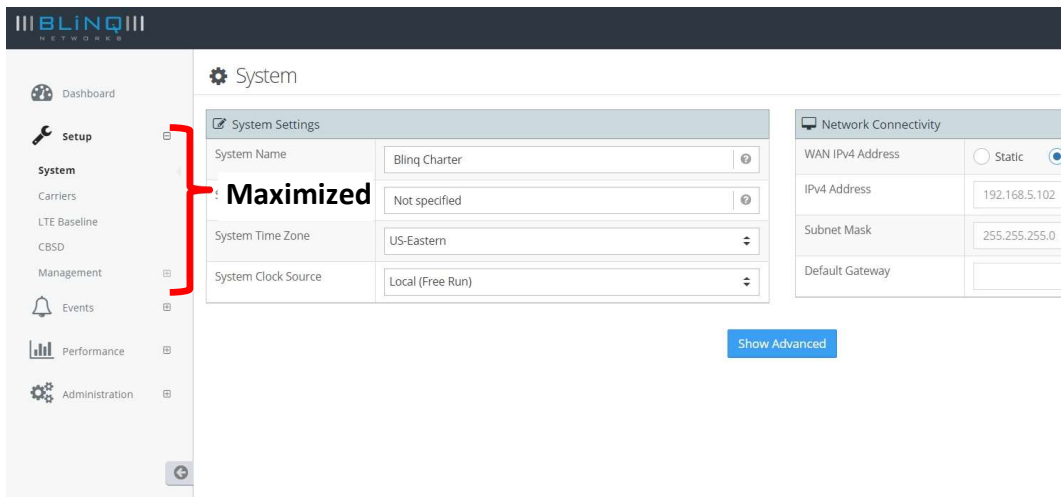


Figure 4-3 View Maximized

### 4.1.1.3 System Information Bar

The FW-300i system displays the model number, serial number, software version, EEPC version and current license (if applicable) status/number along the bottom of each main page. For example:

BLiNQ Networks © 2020

Model: RevC05 Serial Number: 60101C5-18520037 Version: 2.0.9\_1 EEPC Version: 3.2.54

## 4.1.2 System Status Messages

The FW-300i WebUI outputs the following types of real-time messages to report on the interaction and/or change results between you and the FW-300i system:

### Success Message (Green):

- A Success message in green advises, for example, of a successful data or configuration change.
- Success messages automatically disappear after about 4 seconds. You can dismiss them earlier by clicking on the message.



Figure 4-4 FW-300i WebUI System Success Status Message

### Warning Message (Yellow):

- A Warning message in yellow usually cautions of a validation error. For example, if there are problems with entered data, then a Warning message in yellow appears to explain the issue.
- You must click on a Warning message to dismiss it. They do not disappear automatically.



Figure 4-5 FW-300i WebUI Warning Message

### Error Message (Red):

- An Error message in red usually advises, for example, when the server is returning an error.
- Error messages signify syntactical issues (or a required field being left empty) with the settings you are trying to commit.
- You must click on an Error messages to dismiss it. They do not disappear automatically.



Figure 4-6 FW-300i WebUI Error Message



## 4.2 Default FW-300i Configuration

The following table contains the FW-300i default configuration:

**Table 4-1 FW-300i Default Configuration Values**

CONFIGURATION	DEFAULT SETTING
DHCP	ON
Fixed, Non-routable Local Craft IP Address	169.254.1.1
Management IP Address	Provided by DHCP
Gateway IP Address	Provided by DHCP
WebUI	Enabled (ON)
Channel Bandwidth	20 MHz
Operating Frequencies	<b>Band 42/43:</b> 3620MHz, 3640MHz, 3660MHz Corresponding eARFCN: 43790, 43990, 44190 <b>Band 48:</b> 3580MHz, 3600MHz, 3620MHz Corresponding eARFCN: 55540, 55740, 55940
TDD Frame Configuration	2 (Special Subframe: 7)
Cell State	Enabled
Transmit Power	30 dBm
Clock Source	GPS
CBSD	Certificates installed, parameters not configured

## 5 Configuration

This chapter describes the tasks associated with preparing an FW-300i system to provide network services to its users using the FW-300i WebUI.

The FW-300i system allows efficient installation processes by supporting full pre-configuration of equipment in the warehouse and a field installation process that does not require other installation tools other than the ones needed for the physical installation.

To configure your system using the FW-300i WebUI (recommended), see Section 5.2, “[Configuration with the WebUI](#)”.

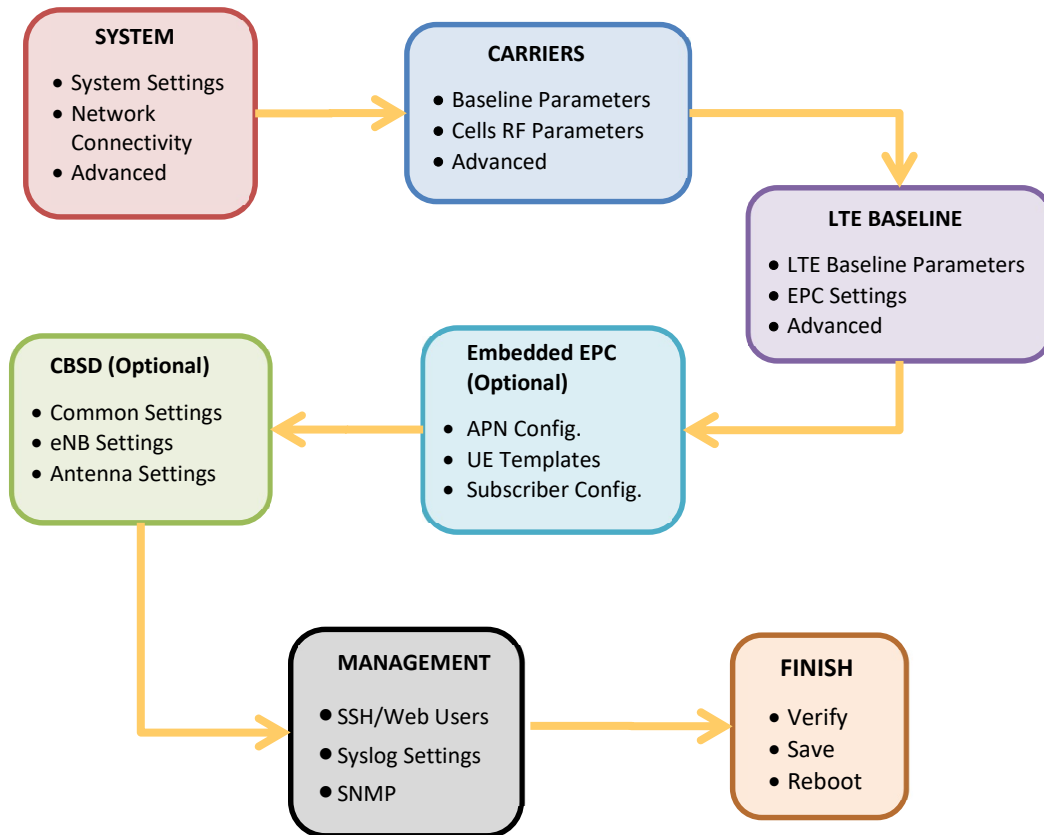
If you want to perform the configuration process using a CLI, please contact BLiNQ Technical Support.

The recommended FW-300i system commissioning process includes the following steps:

- Pre-Configuration in the Warehouse
- Field Installation (See the “*FW-300i Installation Manual*”)

## 5.1 System Configuration Process

The FW-300i WebUI menu structure is the basis for the configuration process. This means that the configuration steps are set up so that you logically input all of the related parameters on a page before you move to the next page/step in the configuration process.



**Figure 5-1 FW-300i Configuration Process**



### Notes:

- Perform these steps in the order presented.
- Once you complete the pre-configuration, ensure that you save the current running configuration to the start-up configuration. This ensures that any changes are persistent over reboots.
- See Section 5.2.7, “Verify, Save and Activate Current Running Configuration”

## 5.2 Configuration with the WebUI

---

This section describes the tasks associated with preparing an FW-300i system to provide network services to its users using the FW-300i WebUI. If needed, see Figure 5-1, FW-300i Configuration Process for a visual overview of the configuration process.

The recommended FW-300i system commissioning process includes the following steps:

- Pre-Configuration in the Warehouse
- Field Installation (See the “*FW-300i Installation Manual*”)

### 5.2.1 System

On the WebUI (under “**Setup**”) **System** page you set a few parameters:


- System Name and Description
- System Time Zone and Clock Source
- Network Connectivity parameters
- Advanced (IPv6, DNS, NTP, MTU, VLAN)

### 5.2.1.1 Configuring a System Name

When pre-configuring the FW-300i, it is highly recommended that you set a unique hostname to differentiate it from other devices.

- Navigate to the **Setup > System** page of the FW-300i WebUI.
- Under the **System Settings** area, assign a descriptive name to the module in the **System Name** field.

If desired, assign more identifying information via the **System Description** field. Use **System Time Zone** and **System Clock Source** to set your time zone and clock source.



System Settings	
System Name	Blinq eNB
System Description	Not specified
System Time Zone	US-Eastern
System Clock Source	GPS

System Settings	
System Name	Blinq Networks Link 12
System Description	Corner of 1st and 2nd Street - Test
System Time Zone	US-Eastern
System Clock Source	GPS

Select **Commit** in the top right corner to save the changes or select the **Refresh** (↺) button to cancel and return to the previous settings.

Repeat as needed for each device in your system.

Please note that most configuration changes are only applied after system reboot. To ensure that all of your pre-configuration changes are saved to the start-up configuration file and to activate all of your current configuration settings, see Section 5.2.7, “Verify, Save and Activate Current Running Configuration”.

### 5.2.1.2 System Synchronization

The FW-300i system is a Time Division Multiplexed (TDM) radio system. Therefore, FW-300i networks require proper synchronization of the air interface to provide optimal service. The FW-300i system provides flexible synchronization options as well as providing a high-performance extension to existing synchronization networks which delivers quality clock services to downstream devices such as small cells.

The eNodeB synchronizes using the Global Positioning System (GPS).

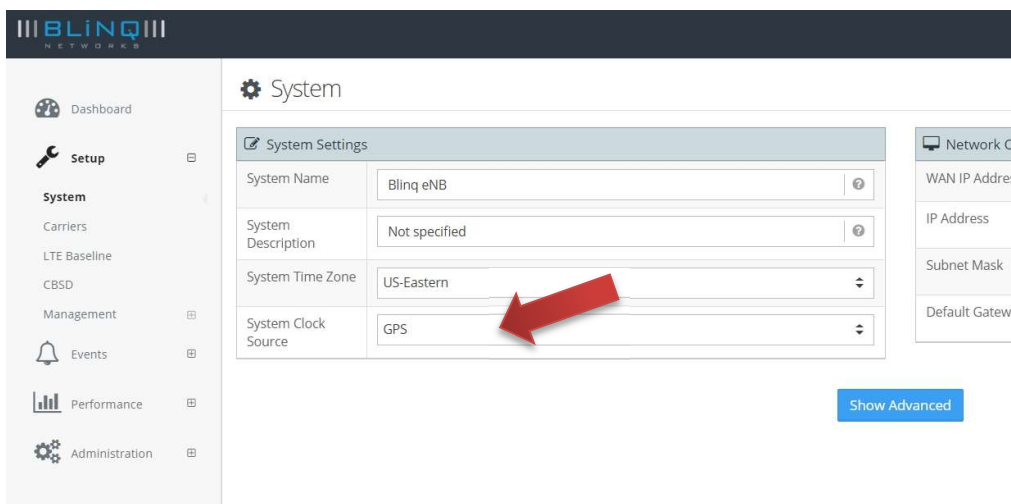
When configured to synchronize via GPS, the FW-300i system uses its internal GPS antenna and receiver module to synchronize to the GPS network. This allows all network deployed FW-300i eNodeBs to

accurately synchronize their transmit and receive operations on the air interface. The GPS system also allows the FW-300i system to determine accurate time of day and date information. This time information, together with a user configured time zone setting, tells time across the system and is essential in functions such as fault management (for example, event and alarm time stamping) and historical performance (for example, performance indicator processing and performance file creation). If needed, there is also an optional external GPS source available.

The FW-300i system includes a high performance crystal oscillator that allows it to maintain its clock properties (Holdover) even if the primary clock reference (that is, GPS) is no longer available. The system provides a Holdover period of 5 minutes. During this time the radio is operational and the system attempts to recover its primary clock source. If the system does not reacquire the clock source after the Holdover period expires, the system is deemed “Not synchronized” and therefore ceases radio operation so as to not interfere with other deployed FW-300i systems.

On the WebUI, to set the system synchronization:

- Navigate the **Setup > System** page on the FW-300i WebUI.
- In the **System Settings** area, you set the system synchronization via the **System Clock Source** option. Select your system clock source to **GPS**.



#### Notes:

- Networks of FW-300i systems depend on proper synchronization through GPS clock references to operate optimally, and may experience significant performance degradation or even outage if not deployed accordingly.
- The system allows you to use local clock as a clock source. This parameter is meant for lab testing only.
- A change in clock source requires a reboot!  
When you change the system time, you need to commit, save the change and then perform a FW-300i reboot in order for the change to take effect.

Before moving to a new page, select **Commit** in the top right corner to save your changes or select the **Refresh** button to cancel and return to the previous settings.

To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



Reboot the system to activate all of your saved changes, by selecting the **Reboot System** button () in the top right corner.

### 5.2.1.3 Network Connectivity Parameters

Once logged on to the FW-300i, you can change the IP address of the WAN interface under **Network Connectivity**. There are two possible methods of assigning IP address to the system. You can choose either:

- **Static:** statically assign the IP address for the WAN interface. If set to **Static:** you must configure the IP address, subnet mask and default gateway, or
- **DHCP:** use the Dynamic Host Configuration Protocol (DHCP) to configure this IP address.

**Note:** To have DHCP properly assign an address to your FW-300i system, the system must have network access to a DHCP server on your local network. This DHCP server must have available addresses in its address pool, which are in the desired subnet you wish to assign to the system.

By default, the FW-300i WAN IPv4 address is assigned via DHCP.

In order to set the IPv4 address, please follow these steps:

- Navigate to the **Setup > System** page of the FW-300i WebUI.
- Under **Network Connectivity**, you find all the configurable options.

Network Connectivity	
WAN IPv4 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv4 Address	<input type="text" value="192.168.5.102"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.5.1"/>

- Ensure the **WAN IPv4 Address** option is set to **Static**.
- Enter an IPv4 address, subnet mask and optionally an address for the default gateway (local router) using the applicable fields:
  - **IPv4 Address,**
  - **Subnet Mask,**
  - **Default Gateway**
- Select **Commit** in the top right corner to save your changes.

#### Notes:

- At any time during configuration changes and before clicking the **Commit** button, use the **Refresh** () button to return to the previous settings and/or to update the information on the screen.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** () button – located on the top right corner.

- The changes do not take effect until you reboot the system. Reboot the system by selecting the **Reboot System** button (🔄) in the top right corner.

#### 5.2.1.4 Advanced Options

When you click on the **Show Advanced** button, more configurable fields (**IPv6** and **Advanced Network Connectivity**) will appear. This is where you will go to configure **IPv6** and your **DNS, NTP, IP MTU** and **VLAN**.

The diagram illustrates the process of accessing advanced network settings. It starts with the 'Network Connectivity' section, which includes fields for WAN IPv4 Address, IPv4 Address, Subnet Mask, and Default Gateway. A red arrow points to the 'Show Advanced' button, which is circled in red. A large red arrow points down to the 'Advanced Network Connectivity' section, which includes fields for DNS1, DNS2, NTP1, NTP2, IP MTU, and VLAN. Below this section is a 'Reset Advanced' button.

System Settings	
System Name	Bling Charter
System Description	Not specified
System Time Zone	US-Eastern
System Clock Source	Local (Free Run)

Network Connectivity	
WAN IPv4 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv4 Address	192.168.5.102
Subnet Mask	255.255.255.0
Default Gateway	192.168.5.1

**Show Advanced**

IPv6	
WAN IPv6 Address	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IPv6 Address	fc00:192:168:5::18e
IPv6 Prefix Length	128
Default Gateway	

Advanced Network Connectivity	
DNS1	8.8.8.8
DNS2	8.8.4.4
NTP1	
NTP2	
IP MTU	
VLAN	<input type="checkbox"/> OFF <input checked="" type="checkbox"/> ON

**Reset Advanced**

##### 5.2.1.4.1 Setting up IPv6

1. Ensure the **WAN IPv6 Address** option is set to **Static**. (**WAN IPv4 Address** needs to be set to **Static** for this section to be fillable.)
2. Enter an IPv6 address, IPv6 Prefix Length and optionally an address for the default gateway (local router) using the applicable fields:
  - **IPv6 Address,**
  - **IPv6 Prefix Length,**
  - **Default Gateway**



3. Select **Commit** in the top right corner to save your changes.

IPv6	
WAN IPv6 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv6 Address	<input type="text"/> ?
IPv6 Prefix Length	<input type="text"/> ?
Default Gateway	<input type="text"/> ?



IPv6	
WAN IPv6 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv6 Address	<input type="text" value="2600:6ce6:4400:35::e"/> ?
IPv6 Prefix Length	<input type="text" value="64"/> ?
Default Gateway	<input type="text" value="2600:6ce6:4400:35::1"/> ?



#### Notes:

- With the current SW release, the IPv4 address and IPv6 address are either both statically assigned, or both obtained through DHCP. This behavior will be modified in the future software release such that methods for obtaining IP addresses are independent of each other.
- At any time during configuration changes in advanced mode and before clicking the **Commit** button, use the **Reset Advanced** button (at the bottom) to return to the previous/default settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

#### 5.2.1.4.2 Advanced Network Connectivity

This is where you can configure your **DNS1, DNS2, NTP1, NTP2, IP MTU** and **VLAN** settings.

1. Enter your desired **DNS1, DNS2, NTP1, NTP2, IP MTU** and **VLAN** values into each of the applicable fields.
2. Select **Commit** in the top right corner to save your changes.

Advanced Network Connectivity	
DNS1	8.8.8.8
DNS2	8.8.4.4
NTP1	
NTP2	
IP MTU	
VLAN	OFF



Advanced Network Connectivity	
DNS1	8.8.8.8
DNS2	8.8.4.4
NTP1	192.168.6.15
NTP2	192.168.6.16
IP MTU	1500
VLAN	ON



#### Notes:

- At any time during configuration changes and before clicking the **Commit** button, use the **Reset Advance** button to return to the previous settings and/or to update the information on the screen.
- All of these advanced parameters (DNS, NTP, MTU and VLAN) are optional settings and are not critical for the system to be working.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

## 5.2.2 Carriers

On the WebUI **Carriers** page you set the following parameters:

- Carriers Baseline Parameter (such as Channel Bandwidth and Frequency Setting Mode)
- Cell 0, 1 and 2 RF Parameters

### 5.2.2.1 Setting up Carriers Baseline Parameters

This is where you can set the parameters that are common for all the cells:

- Set the channel size,
- Assign the operating frequency mode (EARFCN or Frequency)

- Along with the option of muting the carriers
- The system supports 10MHz and 20MHz bandwidth configuration. Select the desired bandwidth via the **Channel Size (MHz)** drop-down menu: **10 MHz** or **20 MHz** (default).
- Set the frequency mode for your carrier from the **Frequency Setting Mode** drop-down list. The options are: **EARFCN** (E-UTRA Absolute Radio Frequency Channel Number) or **Frequency**. The default is set to EARFCN.



**Note:** If you select **EARFCN**, configure each **Cell x Carrier EARFCN** (where x is the desired cell number) to the EARFCN licensed for your operation.

### Carriers

Carriers Baseline Parameters	
Channel Frequency	20 MHz
Frequency Setting Mode	EARFCN
Mute all Carriers	<input type="radio"/> NO <input checked="" type="radio"/>


### Carriers

Carriers Baseline Parameters	
Channel Frequency	20 MHz
Frequency Setting Mode	Frequency
Mute all Carriers	<input type="radio"/> NO <input checked="" type="radio"/>

You also have the option of muting all Carriers in this section, should you desire to. All carriers are not muted by default.

### Carriers

Carriers Baseline Parameters	
Channel Frequency	20 MHz
Frequency Setting Mode	EARFCN
Mute all Carriers	<input checked="" type="radio"/> YES <input type="radio"/>

Click **Commit** in the top right corner to save the changes on this page or select the **Refresh** () button to cancel and return to the previous settings.



#### Notes:

- The EARFCN or RF frequency parameter **must match** between an FW-300i and the CPE to create a link.

### 5.2.2.2 Set Cells 0-2 RF Parameters

This is where you can set the parameters that are unique for each cell:

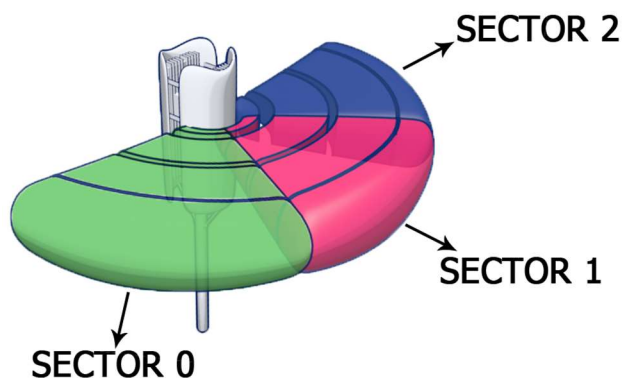
1. Make sure that the box under “**Enable Cell**” is checked for each of the cell that you are configuring.

Cells	
Cell Number	Enable Cell
Cell 0	<input checked="" type="checkbox"/>
Cell 1	<input checked="" type="checkbox"/>
Cell 2	<input checked="" type="checkbox"/>

2. Assign Sector x (where “x” is the desired sector antenna number) to each cell using the drop-down list.\*

Cells		Antenna	RF Parameters			
Cell Number	Enable Cell	Sector Antenna	Carrier Frequency (MHz)		Carrier TX Power (dBm)	
Cell 0	<input checked="" type="checkbox"/>	Sector 0	3580	?	29	?
Cell 1	<input checked="" type="checkbox"/>	Sector 0	3600	?	29	?
Cell 2	<input checked="" type="checkbox"/>	Sector 2	3620	?	29	?
Carrier Aggregation Disabled						

As a reference as to how the sectors are labelled, see [Figure 5-2](#) [Figure 5-2](#), “FW-300i Sectors”.



**Figure 5-2 FW-300i Sectors**

As seen in [Figure 5-2](#) [Figure 5-2](#), the cells can be programmed to transmit out of different antenna sectors. A typical use for this is carrier aggregation, where for 2CC, two cells typically transmit out of the same sector antenna (*Please refer to the latest software release notes to see if carrier aggregation is supported*).

3. Next, depending on the frequency mode (EARFN or Frequency) that you have selected previously under “Carriers Baseline Parameters”, set up the **Carrier Frequency** for each cell. Here are the default values for each cell:
- For Band 42/43 units:
    - 3620 MHz (Cell 0)
    - 3640 MHz (Cell 1)

- 3660 MHz (Cell 2)
- For Band 48 units:
  - 3580 MHz (Cell 0)
  - 3600 MHz (Cell 1)
  - 3620 MHz (Cell 2)

Cells		Antenna	RF Parameters	
Cell Number	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]
Cell 0	<input checked="" type="checkbox"/>	Sector 0 ▾	3620 ⓘ	23 ⓘ
Cell 1	<input checked="" type="checkbox"/>	Sector 1 ▾	3640 ⓘ	23 ⓘ
Cell 2	<input checked="" type="checkbox"/>	Sector 2 ▾	3660 ⓘ	23 ⓘ

**OR**

Set up the **Carrier EARFCN** values for each cell. Here are the default values for each cell:

- For Band 42/43 units:
  - 55940 (Cell 0)
  - 56140 (Cell 1)
  - 56340 (Cell 2)
- For Band 48 units:
  - 55540 (Cell 0)
  - 55740 (Cell 1)
  - 55940 (Cell 2)

Cells		Antenna	RF Parameters	
Cell Number	Enable Cell	Sector Antenna	Carrier EARFCN	Carrier TX Power [dBm]
Cell 0	<input checked="" type="checkbox"/>	Sector 0 ▾	56290 ⓘ	23 ⓘ
Cell 1	<input checked="" type="checkbox"/>	Sector 1 ▾	56090 ⓘ	23 ⓘ
Cell 2	<input checked="" type="checkbox"/>	Sector 2 ▾	56290 ⓘ	23 ⓘ



**Note:** The FW-300i and CPE **MUST** have matching EARFCN or frequencies (that are within the range of usable frequency for the FW-300i system) to create a link.

4. The software recognizes different product codes and will adjust the **Carrier TX Power** (Carrier Transmit Power) limit accordingly. However, the default value is set at 23 dBm
5. Lastly, the drop-down list for **Carrier Aggregation** gives you the option of “**Disabled**” or “**2 CC**”. Starting with SW v2.1, FW-300i supports DL Carrier Aggregation with 2 component carriers. That means that the FW-300i can use two 20 MHz channels to transmit up to 200 Mbps towards a single CPE that also support Carrier Aggregation.

In order to enable this function, select option “**2CC**” from **Carrier Aggregation** drop-down list. With this option selected, the system automatically selects Cells 0 and 1 and disables Cell 2. The system is certified for carrier aggregation out of central (sector 1) antenna; the action of 2CC selection will automatically reconfigure cells 0 and 1 to transmit using central antenna. In addition, if the transmit power for either of cells is set to a value higher than 30 dBm, the system will automatically limit the TX power to 30 dBm.

Cells 0-2 RF Parameters				
Antenna Name		Integrated		
Antenna Model		FW-300i Integrated		
Cells		Antenna	RF Parameters	
Cell Number	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]
Cell 0	<input checked="" type="checkbox"/>	Sector 0	3620	29
Cell 1	<input checked="" type="checkbox"/>	Sector 1	3640	29
Cell 2	<input checked="" type="checkbox"/>	Sector 2	3660	29
		Carrier Aggregation	<div> <div>Disabled</div> <div>Disabled</div> <div>2CC</div> </div>	
<div>Show Advanced</div>				

6. Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (↺) button to cancel and return to the previous settings.



**Note:**

- You configure transmit power *per cell*
- The following maximum values are limited via software:

FW-300i	Band 48	
	➤	20 MHz Bandwidth: 29 dBm for any operational frequency within 3565 MHz to 3685MHz
	➤	10 MHz Bandwidth: 27 dBm for any operational frequency within 3555 MHz to 3695 MHz
	Band 42	
	➤	20 MHz Bandwidth: 29 dBm for any operational frequency within 3410 MHz to 3590MHz
	➤	10 MHz Bandwidth: 27 dBm for any operational frequency within 3405 MHz to 3595 MHz
	Band 43	
	➤	20 MHz Bandwidth: 29 dBm for any operational frequency within 3610 MHz to 3790MHz
	➤	10 MHz Bandwidth: 27 dBm for any operational frequency within 3605 MHz to 3795 MHz

FW-300i HP	<b>Band 48</b>	
	➤	20 MHz Bandwidth: 30 dBm for any operational frequency within 3565 MHz to 3685MHz (33 dBm for Sector 1)
	➤	10 MHz Bandwidth: 30 dBm for any operational frequency within 3555 MHz to 3695 MHz
	<b>Band 42</b>	
	➤	20 MHz Bandwidth: 30 dBm for any operational frequency within 3410 MHz to 3590MHz (37 dBm for Sector 1)
	➤	10 MHz Bandwidth: 30 dBm for any operational frequency within 3405 MHz to 3595 MHz (37 dBm for Sector 1)
	<b>Band 43</b>	
	➤	20 MHz Bandwidth: 30 dBm for any operational frequency within 3610 MHz to 3790MHz (37 dBm for Sector 1)
	➤	10 MHz Bandwidth: 30 dBm for any operational frequency within 3605 MHz to 3795 MHz (37 dBm for Sector 1)

\*One of the unique features of the FW-300i is the ability to steer, with variable capacity, over different areas across 180 degrees of azimuth. This flexibility allows the FW-300i to support both large coverage models, as well as capacity driven models. As a result of this feature, you are able to configure the FW-300i to cover 60 degrees (3 x 20MHz), 120 degrees (2 x 20MHz) or 180 degrees (1 x 20MHz). Please note that the max. Carrier Transmit Power will vary based on your configuration. Please speak with BLiNQ Technical Support for the correct values based on your configurations.

### 5.2.2.3 Advance Option

When you click “Show Advanced” button at the bottom of the page, you will reveal more configurable parameters – **Cell Advanced Parameters** (where the Multiband feature is revealed) and **Band Scan**.

**Carriers**

**Carriers Baseline Parameters**

Channel Size: 20 MHz

Frequency Setting Mode: Frequency

Mute all Carriers: ☐ No ☒ Yes

**Cells 0-2 RF Parameters**

Antenna Name: Integrated

Antenna Model: FW-300i Integrated

Cell Number	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]
Cell 0	<input checked="" type="checkbox"/>	Sector 0	3620	29
Cell 1	<input checked="" type="checkbox"/>	Sector 1	3640	29
Cell 2	<input checked="" type="checkbox"/>	Sector 2	3660	29

Carrier Aggregation: Disabled

**Show Advanced**

Carrier Aggregation: Disabled

**Hide Advanced**

**Cell Advanced Parameters**

Enable Multiband: ☒ YES ☐ NO

**Band Scan**

Scan Band at Boot: ☒ YES ☐ NO

Noise Threshold: -125

Significant Noise Threshold: -115

### 5.2.2.3.1 Cell Advance Parameters

Band 48 overlaps with Band 42 and 43 (3550-3700MHz). The Multiband feature allows CPE that do not support Band 48 to connect to the FW-300i operating on Band 48. (ie. Backwards compatibility) To enable this feature, make sure that the “**Enable Multiband**” is turned to “**YES**”.

**Cell Advanced Parameters**

Enable Multiband: ☒ YES ☐ NO

#### Note:

- CPE’s support for multiband feature (MFB) is also required. Please consult your CPE manual to verify this.
- All BLiNQ CPEs support multiband feature.



- By default, “**Enable Multiband**” is set to “**YES**”.

#### 5.2.2.3.2 Band Scan

You can set the FW-300i to scan the frequency band automatically when it is booting up. This is a functionality that has been added from SW 2.0.12 onwards. When this feature is on, the FW-300i will scan and register noise levels across the entire span of the band (150 MHz) in 5 MHz steps for all 3 cells.

Band Scan	
Scan Band at Boot	<input checked="" type="radio"/> YES
Noise Threshold	<input type="text" value="-125"/> ?
Significant Noise Threshold	<input type="text" value="-115"/> ?

- Under **Carriers > Show Advanced > Band Scan**, click on the button to toggle between “YES” and “NO”. Select the option you desire.
- If you have selected “YES”, please set up the **Noise Threshold** and **Significant Noise Threshold** levels for the scan. The eNB will register anything from -130 dBm to 90 dBm.

### 5.2.3 LTE Baseline

On the **LTE Baseline** page, you configure the following parameters for all modes of operation:

- The baseline parameters (such as eNB ID and Cell Range)
- EPC settings

LTE Baseline

LTE Baseline Parameters

Subframe Assignment

2

Special Subframe

7

Baseline eNB ID

133

PCI Seed Value

133

Cell range [km]

5

Tracking Area Code

1

EPC Settings

PLMN Id

99999

EPC

External

Embedded

Enable MME Pool

MME Name

Embedded

MME Host

Local

eNB Identifiers

LTE Cell	eNB ID	PCI
LTE Cell 0	34048	399
LTE Cell 1	34049	400
LTE Cell 2	34050	401

Show Advanced

### 5.2.3.1 Configuring LTE Baseline Parameters

In this section, you can assign values to **Subframe Assignment**, **Special Subframe**, **eNB ID**, **PCI Seed Value**, **Cell Range** and **Tracking Area Code**.

Based on **Baseline eNB ID** and **PCI Seed Value**, the system will calculate **eNB Identifiers** and **PCIs** for each of the cells and display these values in the read-only **eNB Identifiers** table.

eNB Identifiers		
LTE Cell	eNB ID	PCI
LTE Cell 0	25600	30
LTE Cell 1	25601	31
LTE Cell 2	25602	32


### 5.2.3.1.1 Subframe Assignment and Special Subframe

The advantage of using TDD is that it is possible to change the up and downlink balance and characteristics to meet the load conditions. Please refer to [ETSI TS 136 211 Chapter 4.2](#) to properly configure your subframes.

1. Navigate to the **Setup > LTE Baseline** page of the FW-300i WebUI
2. In the **LTE Baseline Parameters** section, enter a value between 0-6 for the **Subframe Assignment** field. As a default, it has the value of 2.
3. Under the **Special Subframe** field, set a value between 0-8. It is set at 7 by default.

#### LTE Baseline

LTE Baseline Parameters			
Subframe Assignment	2	Special Subframe	7
Baseline eNB ID	100	PCI Seed Value	10
Cell range (km)	2	Tracking Area Code	1

4. Select **Commit** in the top right corner to save the changes on this page or select the **Refresh**  button to cancel and return to the previous settings.

### 5.2.3.1.2 Assign a Baseline eNodeB ID

You use the eNodeB ID to identify each cell when establishing a connection with the Evolved Packet Core (EPC). The system automatically generates three IDs from the baseline value of this parameter for each cell respectively, using the following logic:

- {[eNB Id]\*256},
- {[eNB Id]\*256+1},
- {[eNB Id]\*256+2}.








This setting **must** match with the configured value in the EPC.

To setup the Baseline eNodeB ID:

- Navigate to the **Setup > LTE Baseline** page of the FW-300i WebUI.

Under the **LTE Baseline Parameters** section, assign the eNodeB identification in the **Baseline eNB ID** field. The default value for this parameter is 100.

### LTE Baseline

 LTE Baseline Parameters					
Subframe Assignment	<input type="text" value="2"/>		Special Subframe	<input type="text" value="7"/>	
Baseline eNB ID	<input type="text" value="100"/>		PCI Seed Value	<input type="text" value="10"/>	
Cell range (km)	<input type="text" value="2"/>		Tracking Area Code	<input type="text" value="1"/>	

- Before going to another section, select **Commit** in the top right corner to save your changes or select the **Refresh** button to cancel and return to the previous settings.

#### 5.2.3.1.3 Entering PCI Seed Value

The **Cell ID** and **PCI Seed Value** define each cell's Physical Cell ID (PCI) which the system uses to decode data transmission.








- PCI calculation:  $3 * [\text{PCI Seed Value}] + [\text{Cell Id}]$
- Cell IDs are fixed at 0, 1 and 2 respectively.
- BLiNQ recommends to pre-draft a PCI assignment strategy carefully to avoid interference due to PCI reuse; you can use preconfigured default values
- Refer to **Appendix B, "PCI Planning Guidelines"** for more information on creating a PCI assignment strategy


To enter PCI Seed Value:

- Navigate to the **Setup > LTE Baseline Parameters** page of the FW-300i WebUI.

Under the **LTE Baseline Parameters** area, assign the PCI Seed Value in the **PCI Seed Value** field (You can enter any value between 0-167). It is set to 10 by default.

### LTE Baseline

 LTE Baseline Parameters					
Subframe Assignment	<input type="text" value="2"/>		Special Subframe	<input type="text" value="7"/>	
Baseline eNB ID	<input type="text" value="100"/>		PCI Seed Value	<input type="text" value="10"/>	
Cell range (km)	<input type="text" value="2"/>		Tracking Area Code	<input type="text" value="1"/>	

- Before going to another section, select **Commit** in the top right corner to save your changes or select the **Refresh** () button to cancel and return to the previous settings.


### 5.2.3.1.4 Assigning Cell Range

Configuring the cell range parameter automatically sets the parameters that the CPE requires to establish the link.

To assign the cell range:

- Navigate to the **Setup > LTE Baseline** page of the FW-300i WebUI.
- In the **LTE Baseline Parameters** section, set the **Cell range** to the desired kilometer range. The range is from 1 to 100 kilometers. 20 km is the default value.

LTE Baseline Parameters			
Subframe Assignment	2	Special Subframe	7
Baseline eNB ID	100	PCI Seed Value	10
Cell range [km]	20	Tracking Area Code	1



- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (↺) button to cancel and return to the previous settings.


### 5.2.3.1.5 Setting Tracking Area Code

The Tracking Area Code identifies the tracking area within a particular network. You need to set the same code that matches the settings on your EPC.

- Navigate to **Setup > LTE Baseline** page to set the tracking area code under LTE Baseline Parameters section.
- Set the Tracking Area code via the **Tracking Area Code** field. By default, the value is set at 1.

#### LTE Baseline

LTE Baseline Parameters			
Subframe Assignment	2	Special Subframe	7
Baseline eNB ID	100	PCI Seed Value	10
Cell range (km)	2	Tracking Area Code	1




- Before going to another section on the page, select **Commit** in the top right corner to save your changes or select the **Refresh** (↺) button to cancel and return to the previous settings.

### 5.2.3.2 eNB Identifiers


The values in this section are read only and will change based on the values inserted in the **LTE Baseline Parameters** section.

To configure this section, manipulate the values (see [Section 5.2.3.1.2 Assign a Baseline eNodeB ID](#) and [Section 5.2.3.1.3 Entering PCI Seed Value](#)) in **LTE Baseline Parameters**.

eNB Identifiers		
LTE Cell	eNB ID	PCI
LTE Cell 0	25600	30
LTE Cell 1	25601	31
LTE Cell 2	25602	32



Varies with  
Baseline eNB ID



Varies with PCI  
Seed Value

### 5.2.3.3 EPC Settings

In the Evolved Packet Core (EPC) Settings section, you will configure the system to use either Embedded EPC or External EPC.

This is also the section where you configure the PLMN ID.

The Public Land Mobile Network Identifier or PLMN ID defines the network. The PLMN ID consists of a 3-digit mobile country code (MCC) and a 2 (or 3)-digit mobile network code (MNC), thus PLMN-ID = MCC + MNC. You **must** enter the value that matches the one in the EPC.

To configure the Evolved Packet Core (EPC) for the FW-300i:

1. Navigate to the **Setup > LTE Baseline** page of the FW-300i WebUI.
2. Under the **PLMN Id** area of the **EPC Settings** section, assign the Public Land Mobile Network identification in the **PLMN Id** field. The default value is 00101 (test network)

EPC Settings		
PLMN Id	<input type="text" value="00101"/> ?	
<input type="radio"/> Use Embedded EPC		
<input checked="" type="radio"/> Use External EPC	MME IPv4 Address	<input type="text" value="10.110.0.100"/> ?

3. Select either **“Use Embedded EPC”** or **“Use External EPC”**.
4. If you select **“Use Embedded EPC”**, please refer to Section 5.2.4, “Embedded EPC” to configure your EPC with the WebUI.
5. If you are using external EPC, use the drop-down list to select either **“MME IPv4 Address”** or **“MME IPv6 Address”** and set your IP address. This only applies for SW Versions prior to 2.1.1. For SW Versions 2.1.1 onwards, please see Section 5.2.3.3.1 “MME Pool” below.

6. Select **Commit** in the top right corner to save your changes or select the **Refresh** (🔄) button to cancel and return to the previous settings



**Note:** EPC Provisioning - You use WebUI or CLI for setting up the optional embedded EPC on the FW-300i system. See Section 5.2.4 “Embedded EPC” for WebUI configuration or contact BLiNQ Technical Support if you want to set up with CLI.

#### 5.2.3.3.1 MME Pool

Mobile Management Entity (MME) plays an import role in LTE EPC architecture. MME is the main signalling node in the EPC. Multiple MMEs can be grouped together in a pool to meet increasing signalling load in the network.

From SW Version 2.1.1 onwards, you will be able to take advantage of this functionality for the FW-300i.

1. Navigate to the **Setup > LTE Baseline** page of the FW-300i WebUI.
2. Under **EPC Settings**, choose **“Use External EPC”** and check the **“Enable MME Pool”** box.

3. Now you can fill in the **MME Names** as well as the **MME Host** IPv4 or IPv6 Addresses.
4. Select **“Commit”** in the top right corner to save your changes or select the **Refresh** (🔄) button to cancel and return to the previous settings

### 5.2.3.4 Advanced Options

The **Show Advanced** Option in the **LTE Baseline** page opens up three more sections where you can set different values for each cell. The sections are **LTE Advanced – General**, **PDSCH/PDDCH** and **RACH/PRACH**.

The screenshot shows the 'LTE Baseline' configuration page. At the top, there are tabs for 'LTE Baseline Parameters' and 'EPC Settings'. The 'LTE Baseline Parameters' tab is active, showing fields for Subframe Assignment (2), Special Subframe (7), Baseline eNB ID (100), PCI Seed Value (10), Cell range (km) (2), and Tracking Area Code (1). Below this is a table for 'eNB Identifiers' with columns for LTE Cell, eNB ID, and PCI. The table shows three cells: LTE Cell 0 (eNB ID 25600, PCI 30), LTE Cell 1 (eNB ID 25601, PCI 31), and LTE Cell 2 (eNB ID 25602, PCI 32). A red arrow points from the 'Show Advanced' button to the expanded advanced settings section below.

The expanded advanced settings section includes three tabs: 'LTE Advanced - General', 'PDSCH / PDCCH', and 'RACH / PRACH'. The 'LTE Advanced - General' tab is active, showing a table for LTE Cell parameters (Max Number of UEs, Pmax value, Q Rx Rev Min) for three cells. The 'PDSCH / PDCCH' tab is also visible, showing a field for PDCCH CFI (1). The 'RACH / PRACH' tab is visible at the bottom, showing a checkbox for 'Use RACH/PRACH to configure Cell Range' and a table for RACH and PRACH parameters for three cells.

LTE Cell	Max Number of UEs	Pmax value (dBm)	Q Rx Rev Min (dBm)
LTE Cell 0	96	23	-65
LTE Cell 1	96	23	-65
LTE Cell 2	96	23	-65

eNB	RACH Poweramping Step	RACH Poweramping Preemblem Initial RTP	RACH Preemblem Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
LTE Cell 0	4 dB	90 dBm	3	3	5
LTE Cell 1	4 dB	90 dBm	3	3	5
LTE Cell 2	4 dB	90 dBm	3	3	5

#### 5.2.3.4.1 LTE Advanced – General Settings

1. Set the **max. number of UEs** (between 0-96) of the respective cells.
2. Enter the **P-max Value**. This is the maximum power the CPE is allowed to transmit. The maximum value for this parameter is 23dBm.

- Lastly, configure the **Q Rx Lev Min** value, which is the minimum signal strength that the CPE needs to see in order for it to connect. Care must be taken when modifying this parameter. Please note that a value of -65 dBm configured on the FW-300i translates to a min. threshold of -130 dBm (ie. Multiplied by 2). If the CPE measures the signal strength lower than -130 dBm, then it will not attempt to connect. Increasing the value of this parameter will severely impact the cell range.

LTE Advanced - General			
LTE Cell	Max Number of UEs	P-max value (dBm)	Q Rx Lev Min (dBm)
LTE Cell 0	96	23	-65
LTE Cell 1	96	23	-65
LTE Cell 2	96	23	-65

- Select **Commit** in the top right corner to save your changes or select the **Reset Advanced** button to cancel and return to the previous advanced settings.

#### 5.2.3.4.2 Setting Up RACH/PRACH Values

Setting up the right values for RACH is critical to achieve up link synchronization between UE and eNB. The default parameters are carefully selected by BLiNQ. Please do not modify unless instructed by BLiNQ Support.

- Choose a value from the drop-down list in the **RACH Powerramping Step** field. This is the amount of power that will be added onto the Initial RTP (which you will be configuring next) after each connection attempt.

RACH / PRACH					
<input type="checkbox"/> Use RACH/PRACH to configure Cell Range					
eNB	RACH Powerramping Step	RACH Powerramping Preamble Initial RTP	RACH Preamble Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
LTE Cell 0	4 dB	90 dBm	3		
LTE Cell 1	4 dB	90 dBm	3		
LTE Cell 2	4 dB	90 dBm	3		

- The next column is **RACH Powerramping Preamble Initial RTP**. Similarly, select a value from the drop-down list to set the initial power to use for connection to the CPE.
- Select the maximum number of connection attempts from the drop-down list under **RACH Preamble Trans Max** field.
- The next two columns (**PRACH Config Idx** and **PRACH Zero Corr Zone**) are used only if you wish to use RACH/PRACH to configure your cell range instead of setting it up in the previous section (**LTE Baseline Parameters**).
  - Check off the box at the top left corner of this section.



- b. Set your **PRACH Config Idx** and the **PRACH Zero Corr Zone** to establish your cell range.

RACH / PRACH

☒ Use RACH/PRACH to configure Cell Range

eNB	RACH Poweramping Step	RACH Poweramping Preamble Initial RTP	RACH Preamble Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
LTE Cell 0	4 dB	90 dBm	3	3	5
LTE Cell 1	4 dB	90 dBm	3	3	5
LTE Cell 2	4 dB	90 dBm	3	3	5

5. Once you are satisfied with your values, select **Commit** in the top right corner to save your changes or select the **Reset Advanced** button to cancel and return to the previous advanced settings.

#### 5.2.3.4.3 PDSCH/PDCCH

This section sets up the PDCCH (Physical Downlink Control Channel) CFI (Control Format Indicator) value. It defines the amount of symbols in each subframe allocated to PDCCH. The default is set at 1.

BLiNQ Networks recommends keeping this value at 1.

PDSCH / PDCCH

PDCCH CFI:

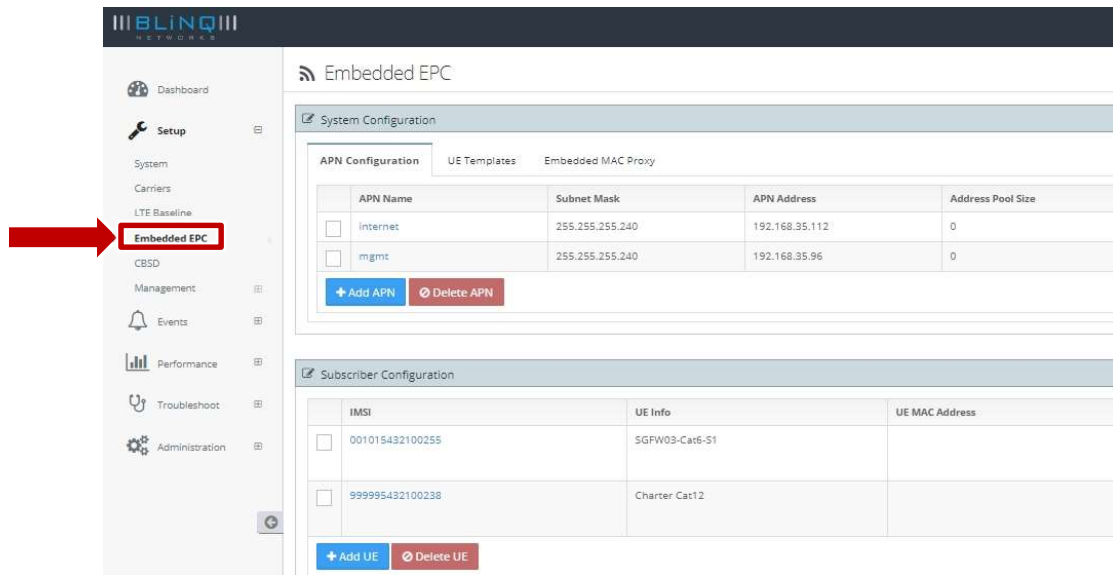
### 5.2.4 Embedded EPC

From Release 2.0.3 onwards, you can configure the following items on the WebUI for your embedded EPC:

- System Configuration (APN Configuration, UE Templates and Embedded MAC Proxy)
- Subscriber Configuration

Please note that the **Embedded EPC** option will only appear on the side menu when **Embedded EPC** is selected under **LTE Baseline > EPC Settings**. Clicking the **Commit** button on the top right will then bring up the **Embedded EPC** option on the side menu. (See 5.2.3.3 EPC Settings)

The EEPC app and license has to be installed for this section to be working/show up on the WebUI.



### 5.2.4.1 APN Configuration

Currently, a maximum of two APN is supported on the FW-300i embedded EPC.

#### 5.2.4.1.1 Adding APN

To add an APN:

- Navigate to **Setup > Embedded EPC** and choose the **APN Configuration** tab under **System Configuration**.
- Click on **+Add APN**. This will open a window to configure the APN.


- Enter the values for the following fields:
  - **Name:** Configure a name for the APN
  - **Subnet Mask:** The subnet mask for the APN network
  - **APN Address:** The IP address for APN network

- **Address Pool Size:** This field configures the dynamic IP range within the APN IP pool. This is the number of dynamic IP addresses that will be available for dynamic allocation. If we set this to zero, then it means that the IP addresses will be statically assigned in the configuration. You can check via the WebUI to ensure that the static IPs are not assigned from the dynamic range.

Example 1:



Your network 192.168.35.96, with subnet mask 255.255.255.224, and address pool size is 6. Then your tap interface IP will 192.168.35.97, dynamically assigned IPs will range from 192.168.35.98 to 192.168.35.103, and the first static IP address will be 192.168.35.104.

Example 2:

When...		Then...
<ul style="list-style-type: none"> <li>• Network: 10.0.110.0</li> <li>• Subnet: 255.255.255.0</li> <li>• Address pool: 16</li> </ul>		<ul style="list-style-type: none"> <li>• Tap Interface IP: 10.0.110.1</li> <li>• 16 addresses (dynamically assigned): 10.0.110.2 to 10.0.110.17</li> <li>• Static IP address will start at 10.0.110.18</li> </ul>



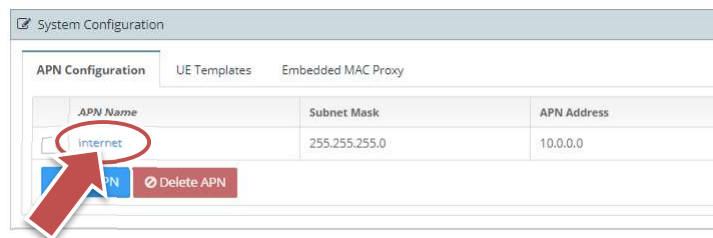
**NOTE:** Alternatively, you can set Address Pool Size to 0, which is essentially saying “all UEs will have static IP addresses”, and then the first static IP address can be 10.0.110.2.

- **DNS1 IP:** The first DNS IP Address
- **DNS2 IP:** The second DNS IP Address
- **NAT:** You can **enable** or **disable** NAT for this APN but **checking** or **unchecking** the box.
- Once you have filled up the respective fields, click the **+ Add APN** button to add APN.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** () button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** () button – located on the top right corner.

### 5.2.4.1.2 Updating APN

To update an existing APN:

- Navigate on the WebUI to **Setup > Embedded EPC**
- Under **System Configuration**, select the **APN Configuration** tab
- Find the **APN Name** that you are looking to update and click on it.



- A pop-up window will appear, and you can now update the APN's values.

Name	Internet
Subnet Mask	255.255.255.0
APN Address	10.0.0.0
Address Pool Size	0
DNS1 IP	8.8.8.8
DNS2 IP	8.8.4.4
NAT	<input checked="" type="checkbox"/>

Cancel + Update APN

- Click the **+ Update APN** button at the bottom of the window.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.

#### 5.2.4.1.3 Deleting APN

To delete an existing APN:

- Navigate on the WebUI to **Setup > Embedded EPC**
- Under **System Configuration**, select the **APN Configuration** tab
- Select the APN that you want to delete by checking the box on the left column.

APN Name	Subnet Mask	APN Address	Address Pool Size	DNS1 IP	DNS2 IP	NAT
<input checked="" type="checkbox"/> internet	255.255.255.0	10.0.0.0	0	8.8.8.8	8.8.4.4	Yes

+ Add APN Delete APN

- Then click on **Delete APN** to delete the desired APN.
- Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

#### 5.2.4.2 UE Templates

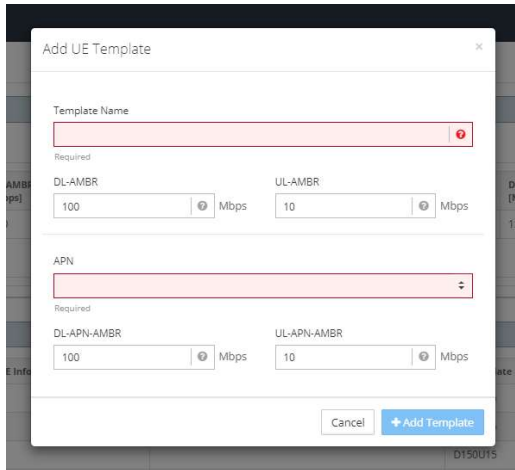
Under the **UE Templates** tab (**Setup > Embedded EPC, System Configuration** section), you can add, delete or updated UE templates.

Using the template-based approach, you can create different templates based on the uplink and downlink speeds to which you want to limit the customers.

### 5.2.4.2.1 Adding UE Templates

To add a UE Template:

- Click on **+ Add Template** under the **UE Templates** tab.
- A pop-up window will appear with various fields that you will need to fill in.

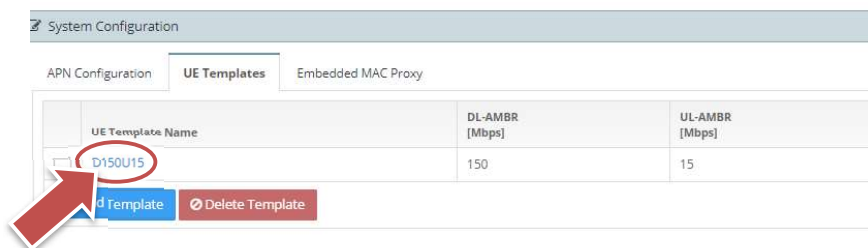


- Enter the values for the following fields:
  - **Template Name:** A name for the template that will be easy to identify
  - **DL-AMBR:** The download aggregate maximum bit rate
  - **UL-AMBR:** The upload aggregate maximum bit rate
  - **APN:** You can assign one of the existing APN to this template by using the drop-down menu in this field.
  - **DL-APN-AMBR:** The download aggregate maximum bit rate for the APN
  - **UL-APN-AMBR:** The upload aggregate maximum bit rate for the APN
- Once you are satisfied with your values, click + Add Template to add the template.
- You should see this new template on the UE Templates List.
- Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

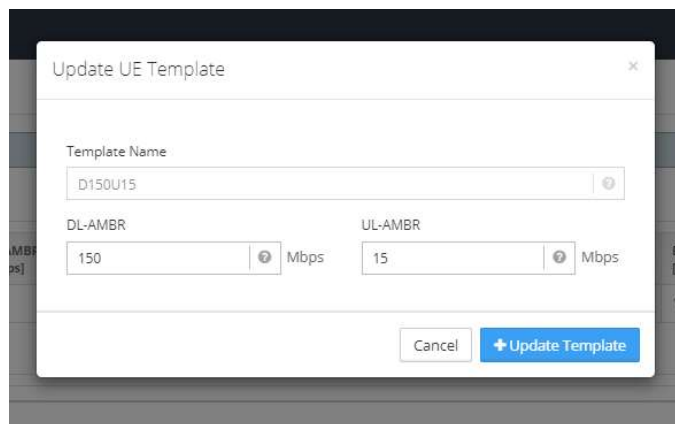
### 5.2.4.2.2 Updating UE Templates

To update an existing UE Template:

- Navigate on the WebUI to **Setup > Embedded EPC**.
- Under **System Configuration**, select the **UE Templates** tab.
- Find the **Template Name** that you are looking to update and click on it.



- A pop-up window will appear, and you can now update the UE Template's values.

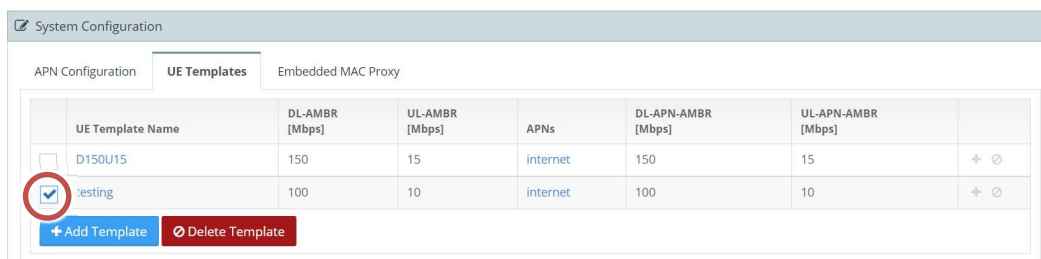


- Click the **+ Update Template** button at the bottom of the window.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

### 5.2.4.2.3 Deleting UE Templates

To delete an existing UE Template:

- Navigate on the WebUI to **Setup > Embedded EPC**.
- Under **System Configuration**, select the **UE Templates** tab.
- Select the Template that you want to delete by checking the box on the left column.



- Then click on **Delete Template** to delete the desired APN.
- Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

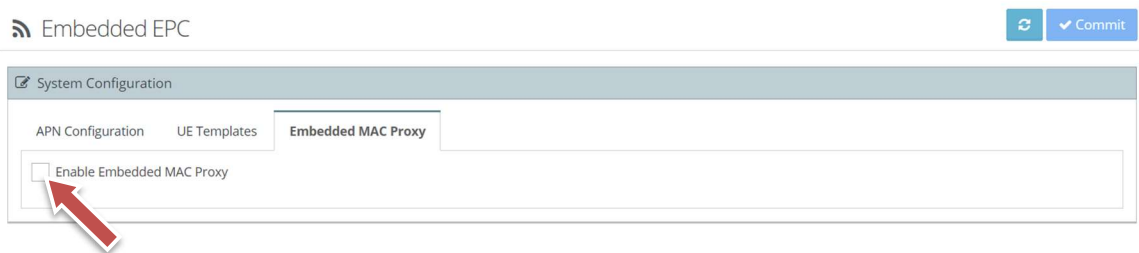
### 5.2.4.3 Embedded MAC Proxy

If you want to create MAC addresses for each of your subscribers, you can enable the **Embedded MAC Proxy** feature. This feature will allow you to create a unique MAC address for each UE.

This allows the router connected to the eNodeB to identify the UE based on its MAC address.

To enable embedded MAC Proxy:

1. Navigate to **Setup > Embedded EPC**
2. Under **System Configuration**, select the **Embedded MAC Proxy** tab
3. **Enable or Disable** the **Embedded MAC Proxy** option by checking or unchecking the box respectively.



4. Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
5. To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

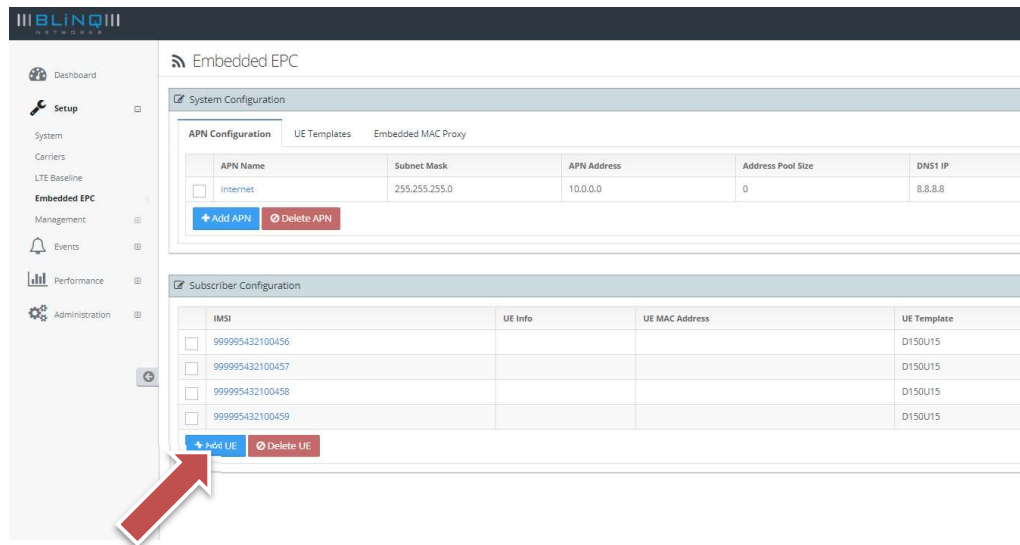
### 5.2.4.4 Subscriber Configuration

You can configure the security parameters (K, OPC and AMF values) for each of your UEs via the WebUI. The ability to do add UEs in bulk will be a feature in the WebUI in a later software release.

#### 5.2.4.4.1 **Adding UE**

To add a UE:

- Go to **Setup > Embedded EPC**
- Under **Subscriber Configuration**, click on the blue **+ Add UE button**.



- A popup window will appear.

- Enter the values for each of the fields:
  - **IMSI:** IMSI is used as a unique attribute to identify each SIM card within a CPE. IT is also used to define the subscriber on the embedded EPC.
  - **K, OPC and AMF:** The K, OPC and AMF parameters form the security keys which are used for authenticating the user when the CPE attempts to connect with the X-300i. These values may be unique for each SIM cards. Please contact BLiNQ Networks Support to obtain this information.
  - **UE Template:** Select the UE template that you want to be associated with this UE
- Once you have entered all the values, click on the **+ Add UE button** at the bottom of the popup window to add the UE. You should be able to see the newly added UE in the **Subscriber Configuration**.
- Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.



### 5.2.4.4.2 Updating UE

There are a few things that you can do for modifying/updating the UE. You can:

- Change its **K**, **OPC**, **AMF** values
- Change its **UE Template**
- Assign a **Static IP**
- Assign a **MAC Address**

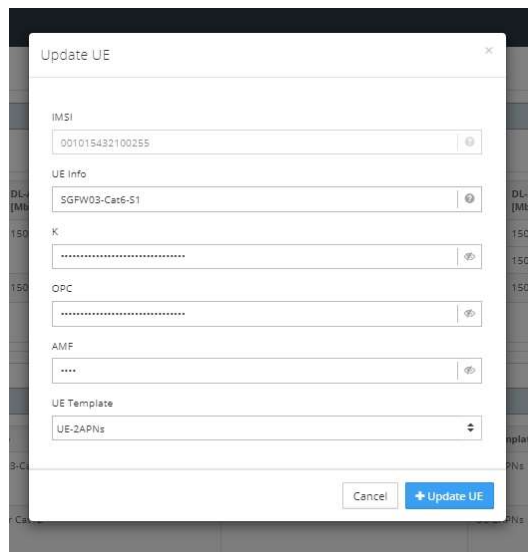
To update/change the values of an existing UE:

- Go to **Setup > Embedded EPC**

Under **Subscriber Configuration**, find the UE that you are looking to update and click on its **IMSI** number



- A window will pop up with all the details.



- Make the changes in their respective fields and then click on the + **Update UE** button at the bottom of the window to save your changes.
- Please note that the only field that you would not be able to change is the UE's **IMSI**.
- Remember to select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

You also have the option to assign a static IP for a particular UE.

To assign a static IP for a UE:

- Locate the UE that you want to assign a static IP address to.
- Click on its **APN**

Subscriber Configuration

	IMSI	UE Info	UE MAC Address	UE Template	APNs	Static IPv4
<input type="checkbox"/>	999995432100456			D150U15	internet	10.0.0.56
<input type="checkbox"/>	999995432100457			D150U15	internet	10.0.0.57
<input type="checkbox"/>	999995432100458			D150U15	internet	10.0.0.58
<input type="checkbox"/>	999995432100459			D150U15	internet	10.0.0.59

+ Add UE    - Delete UE

- A window will pop up which will allow you to make changes only to its **Static IPv4** option.

Update UE APN

IMSI: 999995432100456

UE Info:

UE Template: D150U15

APN: internet

Static IPv4: 10.0.0.56

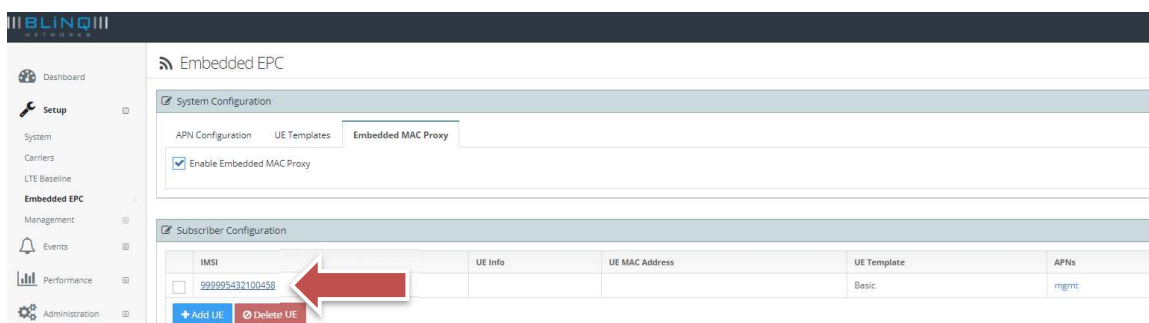
Cancel    + Update UE APN

- Enter the static IP that you want to use then click on + **Update UE APN** to save the change.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (↺) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

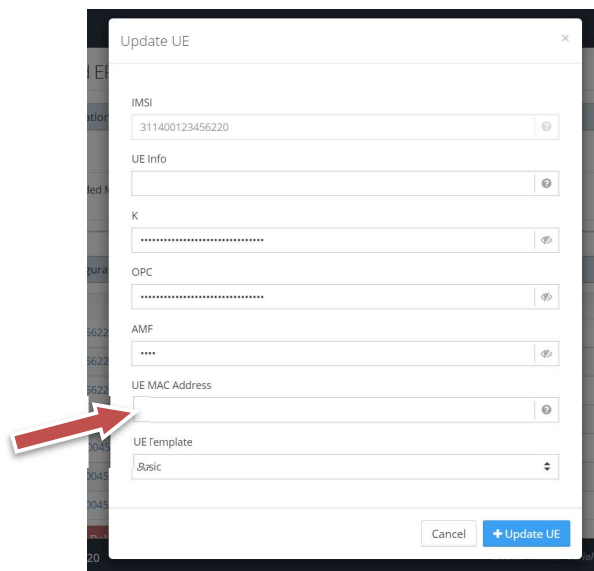
Lastly, you are also able to assign a MAC address for a particular UE.

To assign a MAC address for a UE:

- Make sure that you have enabled the Embedded MAC Proxy option before the next step. (See Section 5.2.4.3 Embedded MAC Proxy)
- Locate the UE **IMSI** that you want to assign a MAC address to.
- Click on its **IMSI**



- A window will pop up which will allow you enter the **UE MAC Address**.



- Enter the **UE MAC Address** that you want to use then click on + **Update UE** to save the change.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

**NOTE:** Reboot is not required in case of adding new APN, templates or UEs. The reboot is not required as long as we do not change existing templates after having used them for some UEs. Otherwise, the changes for existing UEs will only occur after reboot

#### 5.2.4.4.3 Deleting UE

To delete a UE:

- Locate the UE that you want to delete in the **Subscriber Configuration (Setup > Embedded EPC)** section.
- Check the box that is at the beginning of the row and click on the red **Delete UE** button in the same section.

Subscriber Configuration

	IMSI	UE Info	UE MAC Address	UE Template	APNs	Static IPv4
<input type="checkbox"/>	001015432100255	SGPW03-Card-01		UE-2APNs	internet	192.168.35.118
<input type="checkbox"/>	999995432100238	Charter-Card12		UE-2APNs	internet	192.168.35.117
					mgmt	192.168.35.102
					mgmt	192.168.35.101

- The UE will then be deleted.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.
- To make your changes permanent (same configuration after a reboot), select the **Copy Running Configuration to Start-Up Configuration** (📄) button – located on the top right corner.

## 5.2.5 CBSD

CBSD option is only available for frequency band 48 (B48)..

When the WebUI loads, it will recognize the eNodeB is operating in B48 and make **CBSD** option available for configuration.

On the WebUI, you use the Citizens Broadband (radio) Service Device (CBSD) page for the Spectrum Access System (SAS) server connectivity. When using the LTE Band 48, eNodeB requires Spectrum Access System (SAS) server connectivity for operation. The eNodeB will automatically configure the operating frequency and transmit power per sector based on the grants received by the SAS server.

Perform these steps in the order presented below.



### Notes:

- You need to select the **Commit** button *before* you move to a new page to save your configuration changes.
- *Before* exiting from the SAS configuration, you must save the current configuration to the startup configuration with the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar. This ensures that your current configuration is the configuration after a reboot of the unit.

### 5.2.5.1 Configure SAS Server Connectivity

- On the WebUI, navigate to **Setup > CBSD**.

The screenshot shows the BLiNQ Networks FW-300i user interface. The top navigation bar includes a logo, a 'Welcome, admin' message, and a 'Commit' button. The left sidebar contains a 'Setup' menu with options for System, Carriers, LTE Baseline, CBSD, Management, Events, Performance, and Administration. The main content area is titled 'CBSD Settings' and is divided into two sections: 'Common Settings' and 'eNB Settings'. The 'Common Settings' section includes fields for User ID (blinq), FCC ID (ROR00000005), SAS Server URL (https://), CPI Id, CPI Name, and Full Spectrum Request (YES). The 'eNB Settings' section includes fields for Category (B), Multi Step Reg (YES), Latitude (41.012345), Longitude (-89.054321), Height (8.5), Height Type (AGL), Horizontal Accuracy (1), Vertical Accuracy (1), and Measurement Capability 0. There is also an 'Antenna Settings' section with Azimuth and Downtilt fields.

- Under the **Common Settings** area, use the following options to set up your SAS server connectivity:

This is a close-up view of the 'Common Settings' section. It contains the following fields: User ID, FCC ID, SAS Server URL (pre-filled with https://), CPI Id, CPI Name, and Full Spectrum Request (set to NO with a red indicator).

- User ID:** Input the CBSD User identification number
- FCC ID:** Federal Communications Commission (FCC) identification (ID) number. This value is automatically populated by the system. For FW-300i, the value is ROR00000005.
- SAS Server URL:** Input the Spectrum Access System (SAS) database server Universal Resource Locator (URL), for example: <https://testexample.com>
- CPI ID:** Certified Professional Installer ID is to be provided by the user who is certified to install and perform necessary changes to the CBSD device.  
Note: Only user with valid CPI ID is allowed to install the CBSD class B as SAS verifies the CPI ID. Failure to provide valid CPI ID will lead to installation parameter errors.
- CPI Name:** CPI Name is name of the user who holds valid CPI ID.
- Full Spectrum Request:**
  - When full spectrum request is **enabled** the CBSD asks SAS for all the available channels by sending a spectrum inquiry request and if SAS responds back with more than 60 MHz available channels, all the three sectors will use different channels of 20 MHz each. If only 40 MHz is available then, sector 0 and sector 2 will share the same channel or reuse the frequency and sector 1 will use the rest 20 MHz. If channel availability is less than 40 MHz then all three sectors will be disabled and CBSD needs to wait until the channel is available.

- When full spectrum request is **disabled** the CBSD requests for the carrier frequency that is configured under carriers and if any sector gets error all the sectors will disabled and CBSD will not start the transmission until all three sectors are receive authorized grant.

### 5.2.5.2 ENB Settings

In the **eNB Settings** area, enter the information for each field to connect your eNodeB:

eNB Settings	
Category	B
Multi Step Reg	<input checked="" type="radio"/> YES
Latitude	41.012345
Longitude	-89.654321
Height	8.5
Height Type	AGL
Horizontal Accuracy	1
Vertical Accuracy	1
Measurement Capability 0	Select Meas Cap
Measurement Capability 1	Select Meas Cap
Group Type	None

- **Category:** CBSD units are classified category A or category B device. You will not be able to make any changes in this field as it is a set value.
- **Multi Step Reg:** CBSD device can register itself to SAS server either by using a multi-step registration or single step-registration. Currently, we support only multi-step registration. Additionally, single step registration would require your CPI signed installation parameters to be in the registration request. But a multi-step registration would allow for those parameters to be provided via the SAS portal. Use the toggle button to turn on (**YES**) or off (**NO**) this feature.
- **Latitude:** Input the eNB latitude as per the current location of the unit.
- **Longitude:** Set the eNB longitude as per the current location of the unit.
- **Height:** Input the height (feet) of the eNB based on the type of height selected
- **Height Type:** Set the type of height; options are: above ground level (**AGL**) or altitude/elevation above mean sea level (**AMSL**)
- **Horizontal Accuracy:** Set the horizontal accuracy
- **Vertical Accuracy:** Set the vertical accuracy
- **Measurement Capability:** Assign the measurement capability; you can leave this blank or choose from the following options: **Power Without Grant** and **Power With Grant**
- **Group Type:** Set the type of group; options are: **None** or **Interference Coordination**  
When set to **Interference Coordination** the CBSD will co-ordinate with neighbouring units and report to the SAS.

Under the **Antenna Settings** area, use the following options to set up the antennas:

Antenna Settings	
Azimuth	<input type="text" value="0"/>
Downtilt	<input type="text" value="0"/>

- **Azimuth:** Set the antenna azimuth
- **Downtilt:** Input the antenna downtilt

Select the **Commit** button at the top of the screen to save your changes.

To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



Reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔌) in the top right corner.

## 5.2.6 Management

The following sections only deal with using the FW-300i WebUI. If you want to use the CLI, contact BLiNQ Technical Support for more details.

### 5.2.6.1 SSH/Web Users

Configure the username, password and access level for the local security of each unit. The **SSH/Web Users** feature allows you to add, modify (update password and read/write privileges level) or delete system users from the FW-300i WebUI. Each unit's configuration database stores the user configuration data on the FW-300i.

To add users to (or modify an existing user on) the system using the FW-300i WebUI:

- Navigate to the **Setup > Management > UI & Reporting** page of the FW-300i WebUI.



NOTE: Please note that **KPI Reporting** is a feature for SW 2.1 onwards.

- Select the **Add User** button to add a user in the **SSH / Web Users** section. An **Add User** dialog box appears.

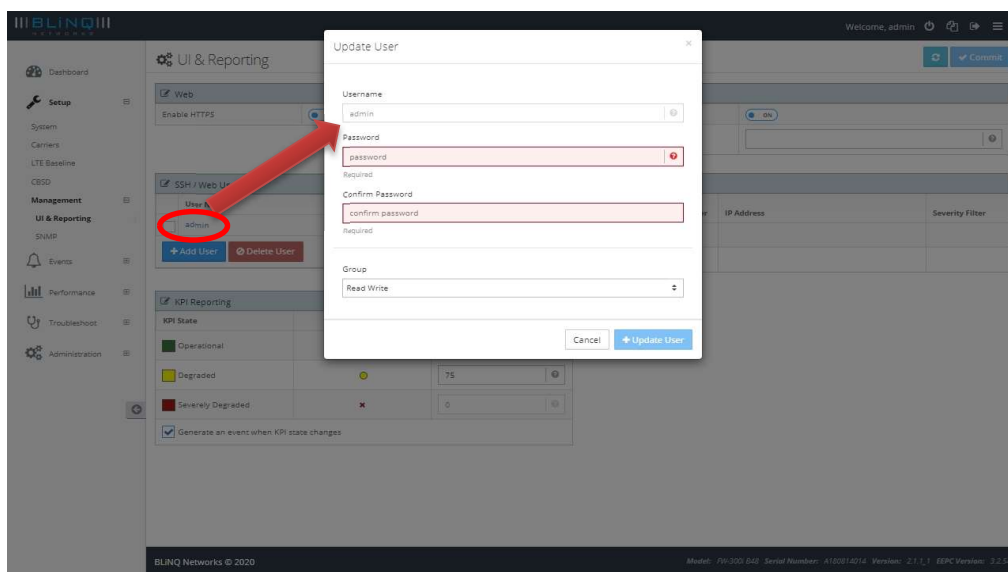
- From the **Add User** dialog box, you can enter a username, password and choose the access level of that user (**Group**) -- either **Read Only** or **Read Write**.



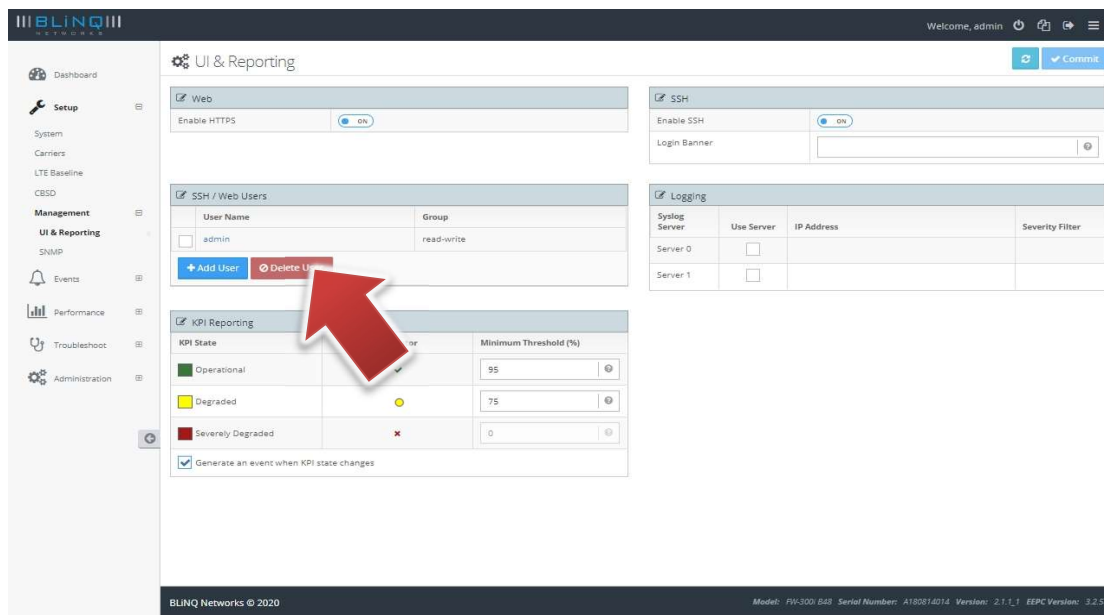
**Note:**

- Usernames must start with a letter and may be composed of alphanumeric characters only.
  - Passwords are case sensitive, may be composed of alphanumeric characters including special characters and must contain at least one (1) letter and one (1) digit.
  - At least one user with read/write privileges needs to exist in the FW-300i system.
  - The system will lock out specific user after 6 unsuccessful login attempts.
- You can edit existing FW-300i users by selecting the hyperlinked name of the user you want to modify. This will bring up the **Update User** dialog box.
  - To reset a password, type in the new password and select the **Update User** button to confirm the new password. Inform the user of the new password.
  - You can also adjust the user's access level – either **Read Only** or **Read Write**.





- To change a username, you must delete this user and create the user under a new name.
- To delete a user: select the check box beside the user that you want to delete. Select the **Delete User** button. The selected user's **User Name** will disappear from the list.



**Note:** If you cannot login due to a forgotten username or password, contact another user with read/write access privileges to have them reset your login credentials. If you have lost all read/write login credentials, contact your supplier.

For any of the actions, select **Commit** for the changes to save your changes or **Cancel** to abandon this action.

Ensure that you save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.

## 5.2.6.2 Syslog

The syslog interface allows the FW-300i system to send standard syslog fault management information (that is, syslog alarms, events and log entries) to external syslog servers.

On the **Setup > Management > UI & Reporting** page, you can set or change their operational status.

### 5.2.6.2.1 Using/Editing Syslog Server

To use/edit a syslog server:

- Navigate to the **Management > UI & Reporting** page.
- Select the server you wish to use in the **Logging** section.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	<input type="text" value="Required"/>	Info
Server 1	<input type="checkbox"/>		

- Enter either an IPv4 or an IPv6 address in the **IP Address** field.
- Select a **Severity Filter** by using the drop down list to set the type of information collected.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	192.168.5.102	Info
Server 1	<input type="checkbox"/>		

- Select the **Commit** button at the top of the screen to save your changes.
- To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



### 5.2.6.2.2 Delete a Syslog Server

To delete a server:

- Navigate to the **Management > UI & Reporting** page.
- From the **Logging** section, uncheck the box next to the syslog server that you want to delete.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	192.168.5.102	Debug
Server 1	<input type="checkbox"/>		

- Select the **Commit** button at the top of the screen to save your changes.
- The syslog server would then be deleted.
- To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



### 5.2.6.2.3 KPI Reporting

This section allows you to set up custom thresholds for your reporting/analysis/monitoring purposes. This feature is available from software 2.1.1 version onwards.

- Go to **Management > UI Reporting > KPI Reporting**

KPI Reporting		
KPI State	Indicator	Minimum Threshold (%)
Operational		95
Degraded		75
Severely Degraded		0

☒ Generate an event when KPI state changes

- Set up the **Minimum Threshold** (in percentage) for each of the three **KPI State** – **Operational**, **Degraded** and **Severely Degraded**.
- Check the box at the bottom if you wish to generate an event when the **KPI State** changes. For example, an event will then be generated if the unit's performance changed from **Degraded** to **Operational**.

### 5.2.6.3 SNMP

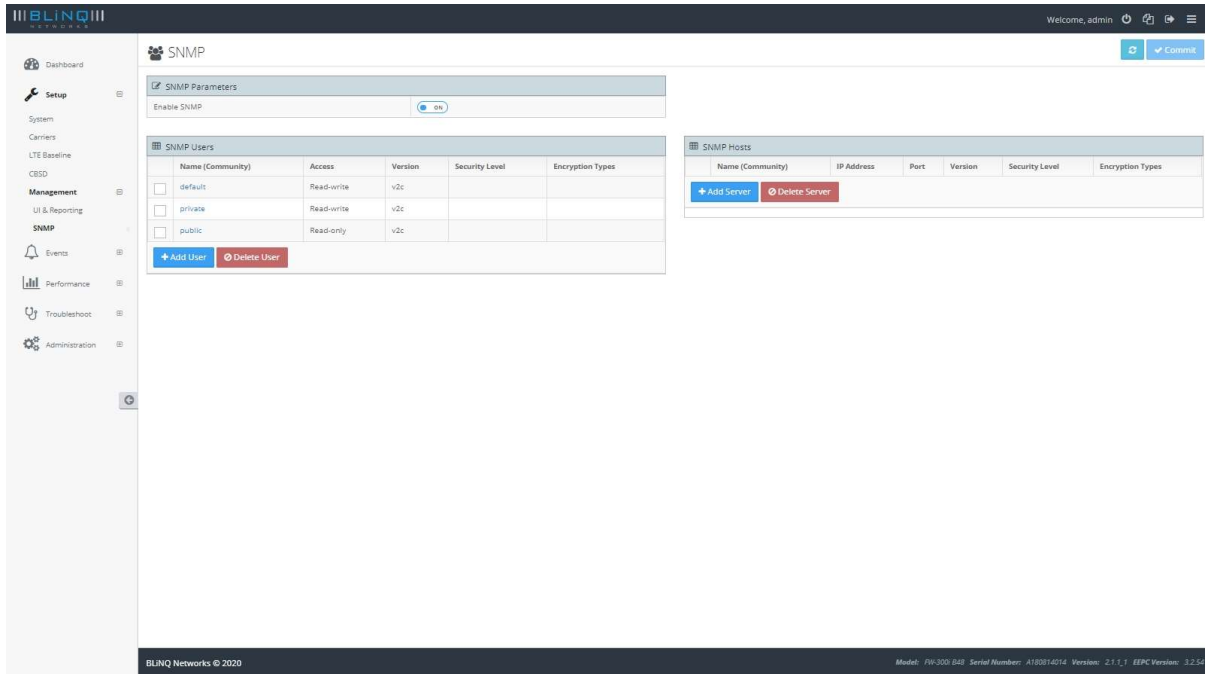
The Simple Network Management Protocol (SNMP) feature allows you to add, delete or edit SNMPv2c or SNMPv3 users and hosts. These interfaces provide complete access to configuration, state, performance and fault information in the FW 300i system.

The WebUI SNMP page allows you to set up Simple Network Management Protocol (SNMP) users and host servers, plus add, edit and remove SNMP users and host servers.

### 5.2.6.3.1 Add or Remove SNMP User

To add or remove an SNMP user:

- Access the **Management > SNMP** page.

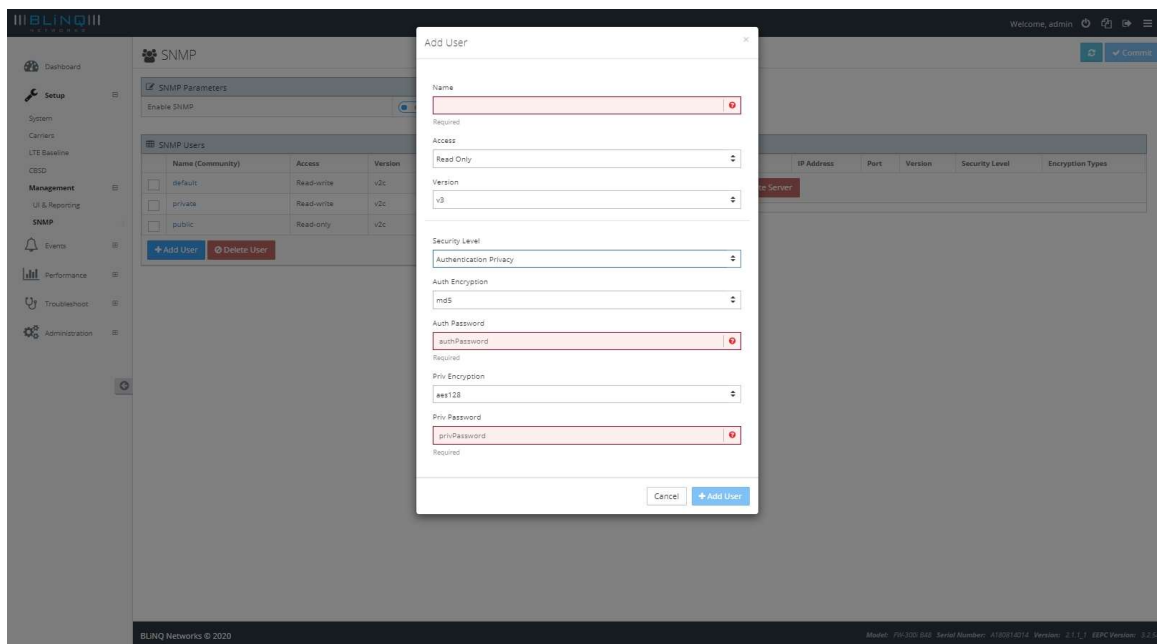


- To add an SNMP user: select the **Add User** button under the **SNMP Users** section. An **Add User** dialog appears. Input the name of the user in the **Name** field. Use the **Access** option to designate the user access level by selecting either the **Read Only** or **Read Write** option.

**Version** refers to the security protocol level for that user: **v2c** (default) or a higher level security protocol of **v3**. If you select **v3**, more options appear. Within the **SNMPv3 Security** area, you can choose higher levels of security depending on the needs of your user and network.

- Security Level** — sets the level of security: **None** (no options available), **Authentication**, **Authentication Privacy**.
- Auth Encryption** — sets the type of authentication encryption protocol: **md5** or **sha**; only visible when **Security Level** set to **Authentication**.

- **Auth Password** — sets the authentication password; only visible when **Security Level** set to **Authentication**.
- **Priv Encryption** — sets the privacy encryption: **aes128** or **des56**; available only when **Authentication Privacy** option selected; only visible when **Security Level** set to **Authentication Privacy**. (aes128 - The system automatically establishes encryption keys and changes them periodically.)
- **Priv Password** — sets the privacy encryption password; available only when **Authentication Privacy** option selected; only visible when **Security Level** set to **Authentication Privacy**.



- Select the **Add User** button to add your user or the **Cancel** button to abandon the addition.
- If you need to edit an existing user, select the hyperlinked name of the desired user, an **Update User** dialog appears. When you finish your edits, select the **Update User** button to save your changes or **Cancel** to abandon these changes.



**Note:** You cannot change the name field. If you do need to change the user name, delete that user and repeat the above steps with a new name.

- To remove an SNMP user: select the check box beside the user you want to delete. Select the **Delete User** button. The user disappears from the list.
- Select the **Commit** button at the top of the screen to save your changes.
- To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.

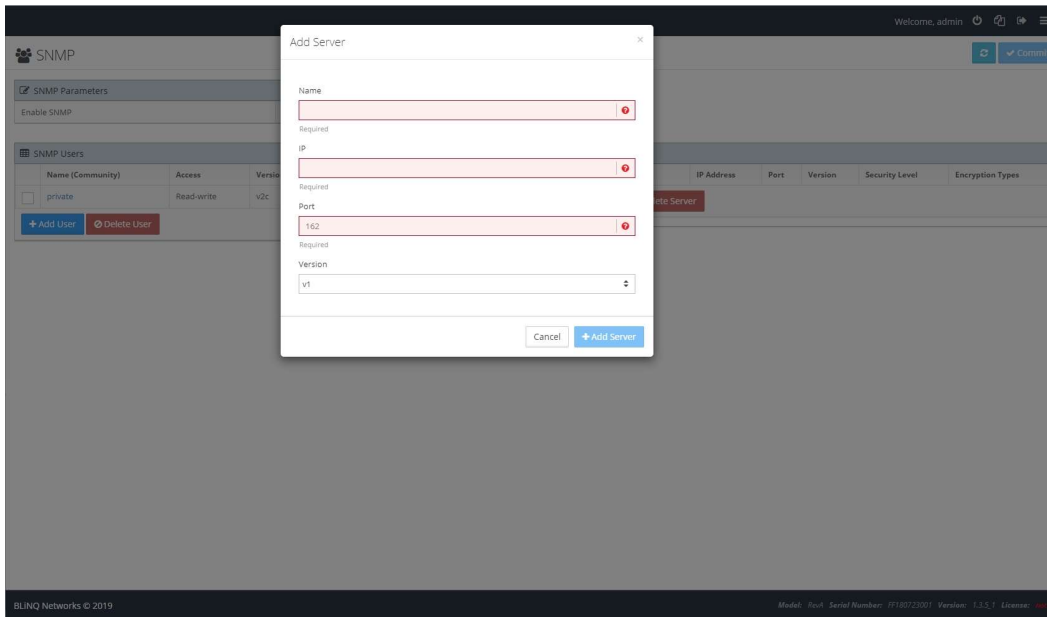


- If this is your last change/update, reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔌) in the top right corner.

### 5.2.6.3.2 Add or Remove SNMP Host

To add or remove an SNMP host:

- Access the **Management > SNMP > SNMP Hosts** area.
- To add an SNMP host: select the **Add Server** button. An **Add Server** dialog appears. You need to know the **Name**, **IP Address** and **Port** for your SNMP host.



**Version** refers to the security protocol level for that host: **v1** (default), **v2** or the higher level security protocol of **v3**. If you select **v3**, more options appear. Within the **SNMPv3 Security** area, you can choose higher levels of security depending on the needs of your host.

- **Security Level** — sets the level of security: **None** (no options available), **Authentication**, **Authentication Privacy**
- **Auth Encryption** — sets the type of authentication encryption protocol: **md5** or **sha**; only visible when **Security Level** set to **Authentication**.
- **Auth Password** — sets the authentication password; only visible when **Security Level** set to **Authentication**.
- **Priv Encryption** — sets the privacy encryption: **aes128** or **des56**; only visible when **Security Level** set to **Authentication Privacy**. (**aes128** - The system automatically establishes encryption keys and changes them periodically.)

- **Priv Password** — sets the privacy encryption password; only visible when **Security Level** set to **Authentication Privacy**.

- Select the **Add Server** button to add your server or the **Cancel** button to abandon this addition.
- If you need to edit an existing SNMP host, select the hyperlinked name of the desired host, an **Update Server** dialog will appear. When you finish your edits, select the **Update Server** button to save your changes or **Cancel** to abandon these changes.



**Note:** If you do need to change the Host name, delete that host and repeat the above steps with a new name.

- To remove an SNMP host: select the check box beside the host you want to delete. Select the **Delete Server** button. The host disappears from the list.
- Select the **Commit** button at the top of the screen to save your changes.
- To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



- If this is your last change/update, reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔌) in the top right corner.

## 5.2.7 Verify, Save and Activate Current Running Configuration

Before exiting from the pre-configuration setup:

- Verify that the currently running configuration meets all of the configuration system setup requirements. If the configuration matches the expected configuration, you **must** save the currently running configuration to the start-up configuration. This ensures that any changes are saved after a reboot. To activate and see your configuration changes, reboot the system.

### 5.2.7.1 Verify and Save Running Configuration

To verify and save the currently running configuration:

- Verify the currently running configuration to ensure that it matches the expected configuration. For instance, check that the EARFCN or radio frequencies match on the FW-300i and CPE.

Select the **Commit** button at the top of the screen to save your changes.

To save your changes to the startup configuration, select the **Copy Running Configuration to Start-Up Configuration** button (📄) in the title bar.



Reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔌) in the top right corner.



## 6 Operation and Maintenance

This section contains the following additional FW-300i operation and maintenance features:

- Software Upgrade
- Performance monitoring statistics for:
  - eNB
  - CPE
  - Trace Log Files
  - Measurements (per Sector)
- Fault management via the Events:
  - Alarms page
  - Events history

## 6.1 Operation and Maintenance with the WebUI

The following sections only deal with using the FW-300i WebUI. If you want to use the CLI, please contact BLiNQ Technical Support.

### 6.1.1 Administration

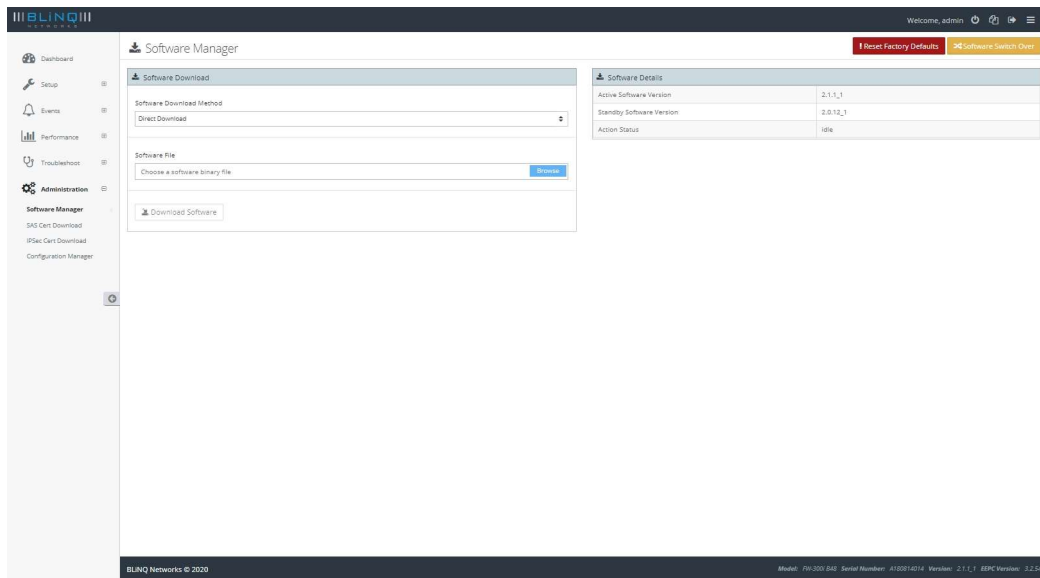
Under “**Administration**”, you can manage the following:

- Software Version
- Download SAS Certificate
- Download IPsec Certificate
- Generate/Restore from Configuration backup files

#### 6.1.1.1 Software Manager

To perform system software upgrade activities, you must have read-write privileges to access this functionality.

Software upgrades occur either from an FTP server, SFTP server or from your hard disk. Navigate to **Administration > Software Manager** to upgrade system software or to view details on the current software.



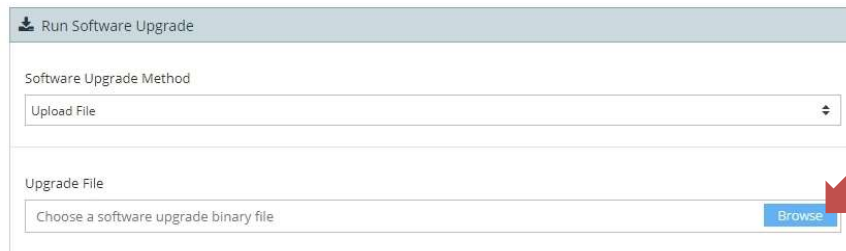
The read-only **Software Details** area informs you of the device’s currently running software (active), the available standby software and the current upgrade status.

Software Details	
Active Software Version	2.1.1_1
Standby Software Version	2.0.12_1
Action Status	idle

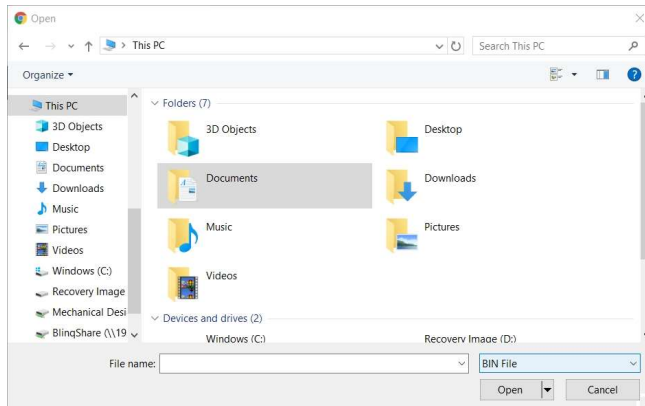
NOTE: You can also see the running software version from the **Dashboard** when you first log into the system.

#### 6.1.1.1.1 System Software Upgrade

- Navigate to the **Administration > Software Manager** in the FW-300i WebUI.
- Within the **Software Download** area, from the **Software Download Method**, select either **Direct Download**, **FTP** or **sFTP** from the dropdown menu.
- For **Direct Download** (for software files located on your hard drive or available network drive):
  - Click on the **Browse** button under the **Software File** field.

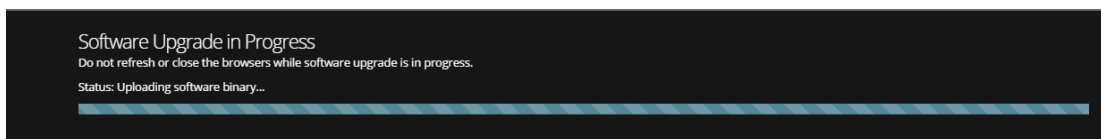


- A File Manager window will pop up. Browse for the binary file to be used for the upgrade and click **“Open”**.

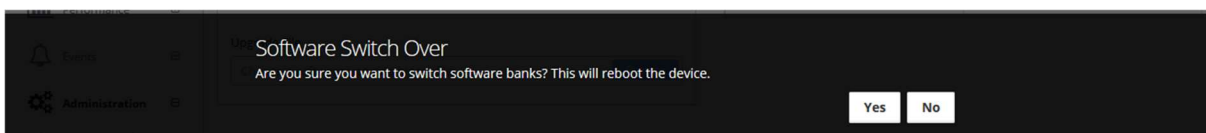


- The file name should appear in the Software File. Click on **Download Software** to download the software.
- For **FTP** or **sFTP**:
  - Enter the details (**Host Address (IPv4 or IPv6)**, **Username**, **Password** and **File Path**) to locate the file.

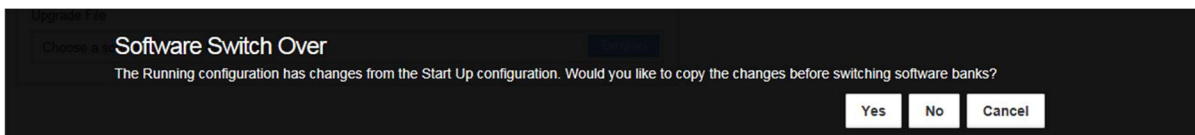
- Click on **Download Software** to download the software onto the eNB.
- Regardless of your download method, once you click on **Download Software**, a progress bar should appear.



- A green status message at the top of the page will indicate if the software download succeeds (see Section 4.1.2).
- The **Standby Software Version** field then shows the new software load version
- To load the standby software, select the **Software Switch Over** button at the top of the page.
  - A **Software Switch Over** query window appears. Select the **Yes** button at the prompt. The system restarts using the new software image. If the banner at the top indicates that this was successful, you have finished this software upgrade procedure. Select the **No** button if you want to abandon this update.



- If there is a difference between the currently running configuration and the saved configuration, a query window appears. Select **Yes** to save your configuration changes and continue with the switch over or **No** to continue with the software switch over and lose your configuration changes. You can select **Cancel** to stop the switch over completely, for instance to verify the configuration changes.



- If the software upgrade fails (for example, due to a corrupt load), the banner at the top of the page will indicate that the upgrade was unsuccessful. The system tries three (3) times to restart with the new software version; if the software upgrade attempts fail, the system reverts to the previous software version. In this case, select a different version of the new software and repeat this procedure from Step 1.

**Notes:**

- You can only upgrade the FW-300i system software from one active browser session. This means you can not open another browser session and start another upgrade process in parallel with the first. If you try this, you get a warning message and the system does not let you continue. Further, do not close the browser once you start the upgrade; if you do or if your computer crashes, you must reset the FW-300i system that was being upgraded and start the upgrade process over.
- To ensure a fresh installation, after switching over to new software, please clear your browser history cache before launching a new WebUI session!



Warning..

⚠ Please ensure the history browser cache is cleared, prior to sign in.



WebUI Sign In

Username

Password

Sign in

ONLY USE the **! Reset Factory Defaults** button, at the top of the page, when you want to return *all* of the configuration settings to the factory defaults. You must have read-write privileges to access this button. When you select the **! Reset Factory Defaults** button, the Login screen appears.

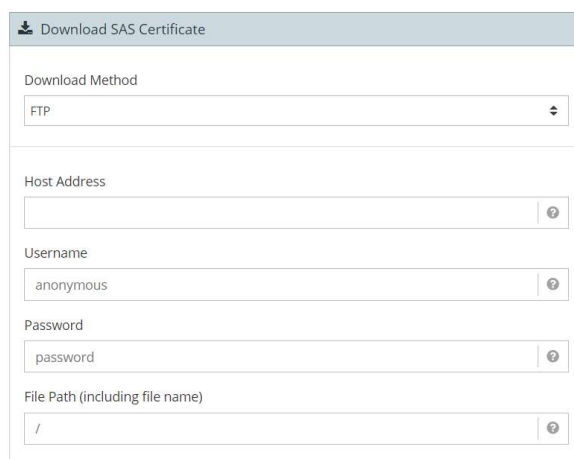
### 6.1.1.2 [SAS Cert Download](#)

To successfully authenticate and establish a TLS connection with the SAS server – CBSD SAS certificate must be installed on the unit. CBSD SAS certificates are generated using the MAC address of the CBSD device and the file format would look like *CBSD-OCA1380004E2-instal\_rsa.certs.tgz*

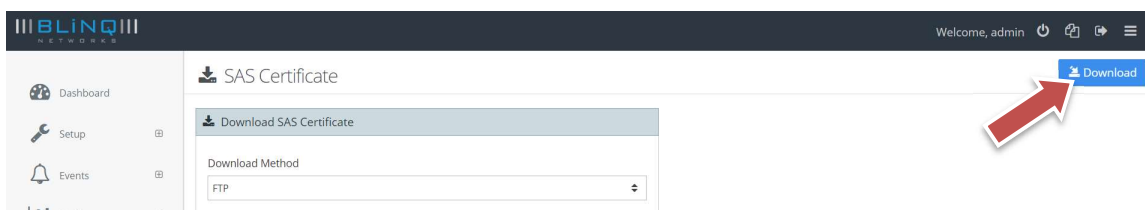
**NOTE:** Certificate package is installed at factory and no operator action is required by default. The operator would need to upload new certificate only in rare scenario (e.g. certificate becomes corrupted).

You can download SAS Certificate from either from an FTP server or SFTP server. To download the SAS Certificate, do the following:

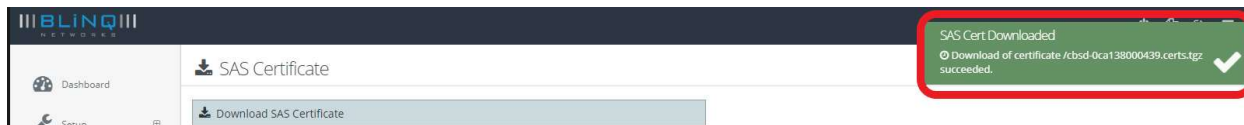
- Navigate to the **Administration > SAS Cert Download** in the FW-300i WebUI.
- Within the **Download SAS Certificate** area, select **Download Method: FTP** or **sFTP**
- Enter the details (**Host Address** (IPv4 or IPv6), **Username**, **Password** and **File Path**)



- Once you have selected the file that you need, click on the **Download** button at the top right of the page.



- A green status window will appear at the top right corner of the WebUI if download is successful.



**NOTE:** A system reboot is required after the SAS Certificate has been downloaded.

### 6.1.1.3 IPSec Cert Download

**NOTE:** IPsec Certificate is needed for communication with Secure Gateway.

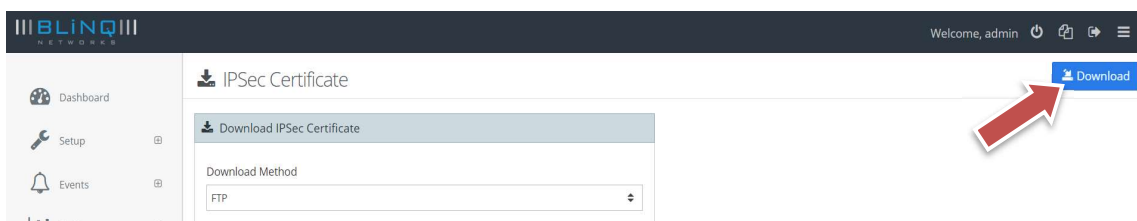
You can download IPsec Certificate from either from an FTP server or SFTP server. To download the IPsec Certificate, do the following:

- Navigate to **Administration > IPSec Cert Download** in the FW-300i WebUI.

- Within the **Download IPSec Certificate** area, select **Download Method: FTP** or **sFTP**
- Enter the details (**Host Address (IPv4 or IPv6)**, **Username**, **Password** and **File Path**)



- When you have selected the correct file, click on the **Download** button at the top right of the page.



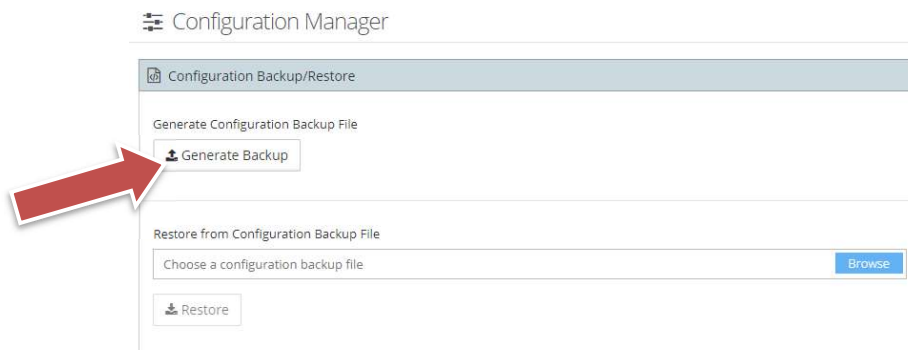
- If download is successful, you will see a green status bar appearing at the top right corner of the WebUI.

#### 6.1.1.4 Configuration Manager

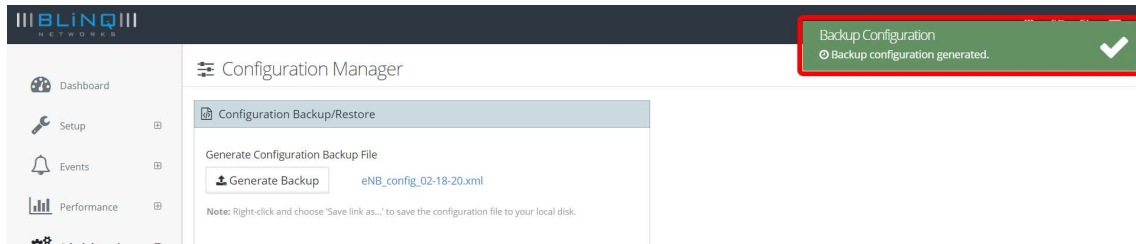
This is the page you can go to **Generate a Configuration Backup File** or to **Restore** from a previous **Configuration Backup File**.

To generate a configuration backup file:

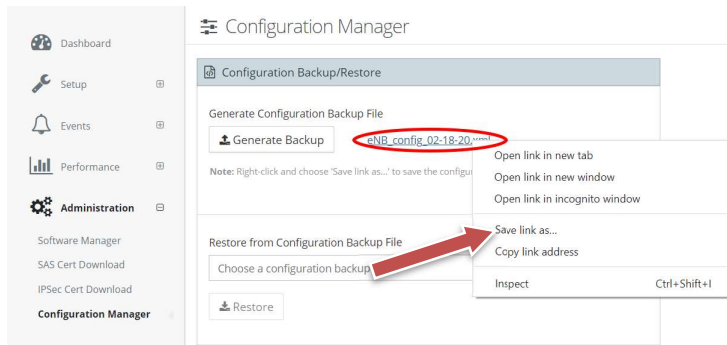
- Navigate to **Administration > Configuration Manager** in the WebUI.
- Within the **Configuration Backup/Restore** section, click on the **“Generate Backup”** button.



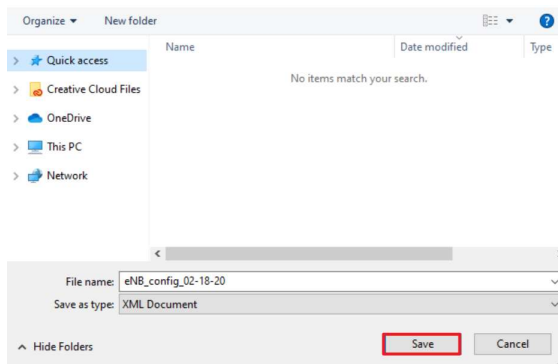
- A green status bar will appear at the top right corner of the WebUI, informing you that the backup file has been successfully generated.



- Right click on the **blue** .xml file link to reveal a popup window. Select “**Save link as...**” to save the configuration file to your local disk.



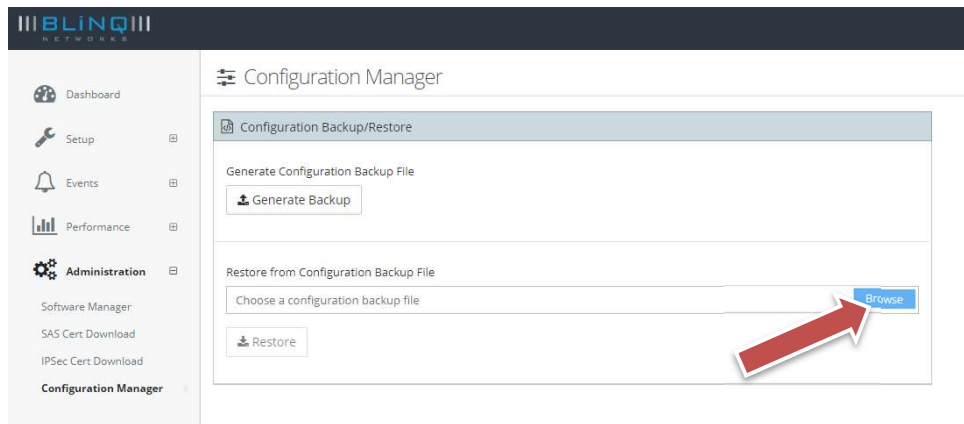
- A **File Manager** window will appear. Choose the location where you want to save the backup file in and click “**Save**”.



To restore from a Configuration Backup file:

- Navigate to **Administration > Configuration Manager** on the WebUI
- Within the **Configuration Backup/Restore** section, click on the “**Browse**” button in the **Restore from Configuration Backup File** field





- A **File Manager** window will popup. Please select the configuration backup file that you desire and hit the **Restore** button.
- A **green status** message will appear at the top right corner of the page if the restoration has been successful.

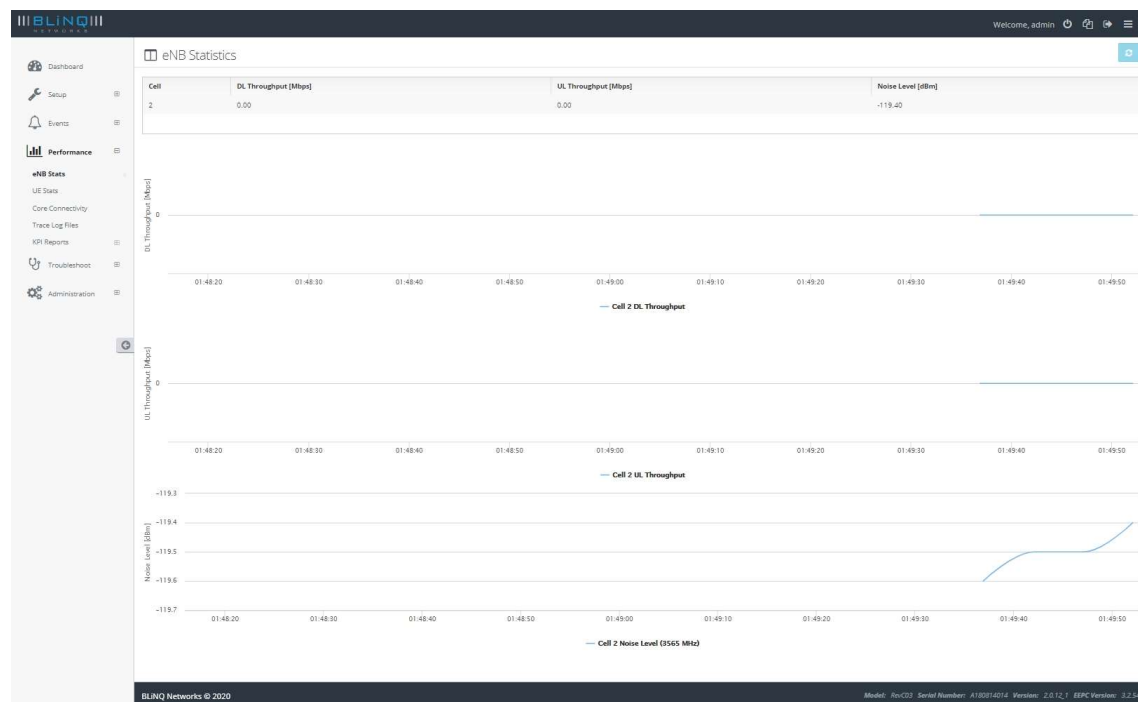
## 6.1.2 Performance

The FW-300i monitors the performance statistics for the eNB and the linked CPE(s).

### 6.1.2.1 eNB Stats Page

The eNodeB Statistics or **eNB stats** page is a read-only page that displays accumulated eNB throughput statistics for how the FW-300i and the associated sectors have been performing for the past 24 hours.

The FW-300i stores a maximum of 96 performance history files over 24 hours before overwriting—one file for every 15 minutes of performance data. Each performance history file contains all of the performance data for every active, linked CPE during the associated 15 minute period.



## 6.1.2.2 UE Stats Page

The Customer Premise Equipment Statistics or **UE stats** page is a performance read-only page that visualizes the incoming and outgoing traffic for the interface connections between the CPE and the FW-300i. This allows you to see traffic and bandwidth usage for the interfaces in real-time and monitor the current download/upload throughput speeds. It also lists the current throughput performance statistics for the interfaces.



**Note:** The screen refresh interval is every 5 seconds.

If needed, the **Refresh** button allows you to refresh the data; it takes approximately 5 seconds to refresh.

LTE Cell	IMSI	RNTI	Carrier Frequency [MHz]	UL-SINR [dB]	UL-RSRP [dBm]	UL-MCS	DL-MCS	UL-BLER [%]	DL-BLER [%]	DL/UL Throughput [Mbps]	Reattach Count	Trace
2	999995452100251	100	3565	36.0	-82.18	10	21	12.50(4.78)	0.00(0.00)	0.0 / 0.0	2	Start

Showing 1 to 1 of 1 entries.

First 1 Last

BLiNQ Networks © 2020

Model: RevC33 Serial Number: A100014014 Version: 2.0.12.7 EEPC Version: 3.2.54

The **CPE Statistics** covers:

- **IMSI:** IMSI is used as a unique attribute to identify each SIM card within a CPE
- **RNTI:** denotes the Radio Network Temporary Identifier (RNTI) of a connected UE
- **Carrier Frequency:** The frequency that the LTE cell is transmitting on
- **UL-SINR:** Uplink Signal to Interference and Noise Ratio
- **UL-RSSI:** Uplink Received Signal Strength Indicator
- **UL MCS:** Indicates the uplink Modulation and Coding Scheme (MCS)
- **DL MCS:** Indicates the downlink Modulation and Coding Scheme (MCS)
- **UL-BLER:** Uplink Block Error Rate – the ratio of the number of erroneous blocks to the total number of blocks transmitted on a digital circuit.
- **DL-BLER:** Downlink Block Error Rate
- **DL/UL Throughput:** shows the downlink (DL) and uplink (UL) throughput (Tput)
- **Reattach Count:** designates the Physical Uplink Shared Channel (PUSCH) Signal to Interference plus Noise Ratio (SINR)
- **Trace:** Starts and then stops the creation of a Trace Log file on this specific CPE

### 6.1.2.3 Core Connectivity Status

This is a read-only page that displays all the CBRS Connectivity information for the ease of monitoring. That includes the **SAS information**, **CBSD State**, **Certificate Status** and the **Valid Until** date of the certificate.

Core Connectivity Status

CBRS Connectivity

SAS Info

Cell	FCC ID-CBSD ID	CBSD State	Certificate Status	Valid Until
Cell 0	N/A	Not Configured	N/A	N/A
Cell 1	N/A	Not Configured	N/A	N/A
Cell 2	N/A	Not Configured	N/A	N/A

BLINQ Networks © 2020

Model: RevA Board Identifier: FF180911001 Version: 2.0.13.1 EPC Version: 3.2.54

### 6.1.2.4 Trace Log Files

The Trace Log Files page offers access to XML trace log files which provide detailed information on one or more UEs. You can use this information for monitoring and optimizing operations and/or to aid in troubleshoot issues.

Trace log files

Filename
trace_1246.xml

Showing 1 to 1 of 1 entries

First Last

To obtain a trace file:

- Navigate to the **Performance > UE Statistics > Trace** column; then select the **Start** button under the desired CPE, this activates the trace file. The button label changes to say **Stop** and the button background changes from blue to red. Each CPE creates a separate trace file.

## UE Statistics

LTE Cell	IMSI	RNTI	Carrier Frequency [MHz]	UL-SINR [dB]	UL-RSRP [dBm]	UL-MCS	DL-MCS	UL-BLER [%]	DL-BLER [%]	DL/UL Throughput [Mbps]	Reattach Count	Trace
2	999995432100251	100	3565	36.0	-91.92	10	21	12.50(4.76)	0.00(0.00)	0.0 / 0.0	2	<a href="#">Stop</a>

Showing 1 to 1 of 1 entries

First 1 Last

- To stop the trace, click on the **Stop** button. This deactivates the trace on this CPE.

To view the file(s), go to **Performance > Trace Log Files**:

- Select the desired XML file hyperlink. The names are based on the CPE's RNTI. The file opens in a separate tab in your web browser.

### 6.1.2.5 KPI Reports

**Cell x Measurements** page, where x represents the sector number, covers Key Performance Indicators (KPI) subcategories: accessibility, retainability, availability and mobility measurements for that sector.

### Part 1 of Sector 0 Measurements page

BLINQ

NETWORKS

Dashboard

Setup

Events

Performance

enB stats

UE stats

Trace log files

KPI Reports

Cell 0

Cell 1

Cell 2

Administration

Welcome, admin

Cell 0 measurements

ERAB.EstabAddAttNbr.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ERAB.EstabAddSuccNbr.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Retainability

ERAB Releases per QCI															
	QCI 1	QCI 2	QCI 3	QCI 4	QCI 5	QCI 6	QCI 7	QCI 8	QCI 9	QCI 65	QCI 66	QCI 69	QCI 70	QCI 75	QCI 79
ERAB.RelActNbr.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ERAB.RelEnbNbr.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ERAB Session time															
ERAB.SessionTimeUE	0														

Availability

RRU Unavailable time per Cause															
	manual intervention								fault						
RRU.CellUnavailableTime.Cause	0								0						

Mobility

HO Preparations per QCI															
	QCI 1	QCI 2	QCI 3	QCI 4	QCI 5	QCI 6	QCI 7	QCI 8	QCI 9	QCI 65	QCI 66	QCI 69	QCI 70	QCI 75	QCI 79
HO.PrepareAtt.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HO.PrepareSucc.QCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

HO Executions															
HO.ExecAtt	0														
HO.ExecSucc	0														

BLINQ Networks © 2020

Model: X-300 (4x4 Outdoor) Serial Number: 60101CS18320037 Version: 2.0.6.1 EEPIC Version: 2.2.52

## Part 2 of Sector 0 Measurements page

### 6.1.2.5.1 Accessibility

- **RRC Establishments per Cause:** details Radio Resource Control (RRC) established connections per cause
  - **RRC.ConnEstabAtt.Cause:** shows established RRC connections attempts per cause
  - **RRC.ConnEstabSucc.Cause:** demonstrates successful RRC connections established per cause
- **RRC Reestablishments per Cause:** details Radio Resource Control (RRC) re-established connections per cause
  - **RRC.ConnReEstabAtt.Cause:** shows re-established RRC connections attempts per cause
  - **RRC.ConnReEstabSucc.Cause:** demonstrates successful RRC connections re-established per cause
- **S1SIG Establishments:** details established S1 signalling
  - **S1SIG.ConnEstabAtt:** shows S1 signalling established connections attempts per cause
  - **S1SIG.ConnEstabSucc:** demonstrates successful S1 signalling connections established per cause
- **ERAB Establishments per QCI:** details the number of established E-UTRAN Radio Access Bearers (E-RAB) per Quality of Service (QoS) Class Identifier (QCI)
  - **ERAB.EstabInitAttNbr.QCI:** shows the number of established initial attempts E-RAB per QCI
  - **ERAB.EstabInitSuccNbr.QCI:** shows the number of successfully established initial attempts E-RAB per QCI
  - **ERAB.EstabAddAttNbr.QCI:** shows the number of additional established attempts E-RAB per QCI
  - **ERAB.EstabAddSuccNbr.QCI:** shows the number of additional successfully established attempts E-RAB per QCI

### 6.1.2.5.2 Retainability

- **ERAB Releases per QCI:** details the number of E-UTRAN Radio Access Bearer (E-RAB) releases per Quality of Service (QoS) Class Identifier (QCI)
  - **ERAB.RelActNbr.QCI:** shows the actual release number of E-RAB per QCI
  - **ERAB.RelEnbNbr.QCI:** shows the eNB release number of E-RAB per QCI
- **ERAB Session time:** details the E-RAB active session time
  - **ERAB.SessionTimeUE:** shows the active session time between the UE and the E-RAB

### 6.1.2.5.3 Availability

- **RRU Unavailable time per Cause:** provides percentage of time that the remote radio unit (RRU) is unavailable per cause (0 and 1)
  - **RRU.CellUnavailableTime.Cause**

### 6.1.2.5.4 Mobility

- **HO Preparations per QCI:** provides handover(HO) preparations per standardized Quality of Service (QoS) Class Identifier (QCI) characteristics (release 12)
  - **HO.PrepAtt.QCI:** specifies the attempted handover preparations per standardized QCI
  - **HO.PrepSucc.QCI:** states the successful handover preparations per standardized QCI
- **HO Executions:**
  - **HO.ExeAtt:** identifies the number of handover execution attempts
  - **HO.ExeSucc:** details the number of handover execution successes

## 6.1.3 Events

The system events are broken down into two sections:

- Alarms and
- History

### 6.1.3.1 Alarms Page

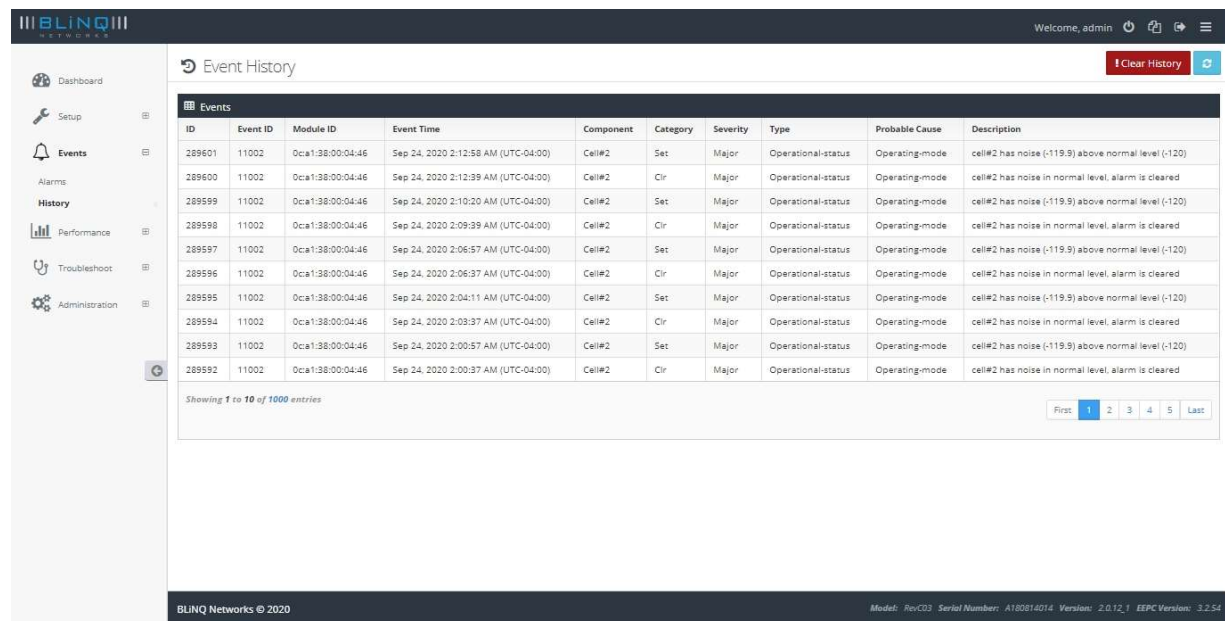
This read-only page lists active alarms (set alarms). Once you clear the Alarm, it appears on the Alarm and History pages along with its details. For a list of alarms, see **Appendix C, “Alarms and Events (Fault Management)”**.

The screenshot displays the 'Alarms' page in the BLiNQ Networks interface. The page title is 'Alarms' and it shows a table of active alarms. The table has the following columns: ID, Alarm ID, Module ID, Alarm Time, Component, Severity, Type, Probable Cause, and Description. A single alarm is listed with ID 159, Alarm ID 11002, Module ID Dca1:38:00:04:46, Alarm Time Sep 24, 2020 2:10:20 AM (UTC-04:00), Component Cell#2, Severity Major, Type Operational-status, Probable Cause Operating-mode, and Description cell#2 has noise (-119.9) above normal level (-120). The page also includes a sidebar with navigation links like Dashboard, Setup, Events, Alarms, History, Performance, Troubleshoot, and Administration.

ID	Alarm ID	Module ID	Alarm Time	Component	Severity	Type	Probable Cause	Description
159	11002	Dca1:38:00:04:46	Sep 24, 2020 2:10:20 AM (UTC-04:00)	Cell#2	Major	Operational-status	Operating-mode	cell#2 has noise (-119.9) above normal level (-120)

### 6.1.3.2 History Page

This read-only page lists a chronological history of alarms and events along with their details. For a list of alarms and events see **Appendix C, “Alarms and Events (Fault Management)”**. The most recent events appear first, to view older events use the page buttons or to quickly access the oldest events, use the **Last** button.



ID	Event ID	Module ID	Event Time	Component	Category	Severity	Type	Probable Cause	Description
289601	11002	0ca1:38:00:04:46	Sep 24, 2020 2:12:58 AM (UTC-04:00)	Cell#2	Set	Major	Operational-status	Operating-mode	cell#2 has noise (-119.8) above normal level (-120)
289600	11002	0ca1:38:00:04:46	Sep 24, 2020 2:12:39 AM (UTC-04:00)	Cell#2	Clr	Major	Operational-status	Operating-mode	cell#2 has noise in normal level, alarm is cleared
289599	11002	0ca1:38:00:04:46	Sep 24, 2020 2:10:20 AM (UTC-04:00)	Cell#2	Set	Major	Operational-status	Operating-mode	cell#2 has noise (-119.8) above normal level (-120)
289598	11002	0ca1:38:00:04:46	Sep 24, 2020 2:09:39 AM (UTC-04:00)	Cell#2	Clr	Major	Operational-status	Operating-mode	cell#2 has noise in normal level, alarm is cleared
289597	11002	0ca1:38:00:04:46	Sep 24, 2020 2:06:57 AM (UTC-04:00)	Cell#2	Set	Major	Operational-status	Operating-mode	cell#2 has noise (-119.8) above normal level (-120)
289596	11002	0ca1:38:00:04:46	Sep 24, 2020 2:06:37 AM (UTC-04:00)	Cell#2	Clr	Major	Operational-status	Operating-mode	cell#2 has noise in normal level, alarm is cleared
289595	11002	0ca1:38:00:04:46	Sep 24, 2020 2:04:11 AM (UTC-04:00)	Cell#2	Set	Major	Operational-status	Operating-mode	cell#2 has noise (-119.8) above normal level (-120)
289594	11002	0ca1:38:00:04:46	Sep 24, 2020 2:03:37 AM (UTC-04:00)	Cell#2	Clr	Major	Operational-status	Operating-mode	cell#2 has noise in normal level, alarm is cleared
289593	11002	0ca1:38:00:04:46	Sep 24, 2020 2:00:57 AM (UTC-04:00)	Cell#2	Set	Major	Operational-status	Operating-mode	cell#2 has noise (-119.8) above normal level (-120)
289592	11002	0ca1:38:00:04:46	Sep 24, 2020 2:00:37 AM (UTC-04:00)	Cell#2	Clr	Major	Operational-status	Operating-mode	cell#2 has noise in normal level, alarm is cleared

Showing 1 to 10 of 1000 entries

First 1 2 3 4 5 Last

BLiNQ Networks © 2020 Model: RevC3 Serial Number: A10014014 Version: 2.0.12.1 EEPROM Version: 3.2.54



**Note:** Clicking Clear History completely clears the current alarms and events history from the FW-300i event logging infrastructure.

Use the **Refresh** button to update the information on the screen.

## 6.2 Troubleshooting

Following is a quick troubleshooting guide:

**Table 6-1 Troubleshooting Guide**

SYMPTOM	POSSIBLE CAUSE	SOLUTION
State LED stuck continuously on red or amber	OS or configuration mismatch preventing the unit from entering functional state	Reboot unit. If problem persists over multiple reboots, contact BLiNQ Networks Support.

<b>FW-300i cannot be accessed</b>	VLAN mismatch	Connect computer to the FW-300i Ethernet port, open <a href="https://169.254.1.1">https://169.254.1.1</a> and verify configured VLAN (exchange with the craft IP is always untagged)
	Wrong IP is set	Connect computer to the FW-300i Ethernet port, open <a href="https://169.254.1.1">https://169.254.1.1</a> and verify that configured IP address, subnet mask and default gateway are set properly
	No dynamic IP address on FW-300i	If the FW-300i is configured for DHCP, verify your network and DHCP Server configuration
	Browser uses HTTP instead of HTTPS	Connect to the FW-300i using <a href="https://&lt;FW-300i_IP_Address&gt;">https://&lt;FW-300i_IP_Address&gt;</a>
	Forgotten username/password	Contact Blinq Support for recovery credentials
<b>FW-300i unable to form S1 link with EPC</b>	GPS is not synchronized	Make sure that the system clock source has been selected to GPS under Setup > Systems > System settings. If the unit is being set up for the first time, please ensure that it has outside visibility and the top of the unit is not heavily obstructed. Please keep in mind that after power disruption that is longer than 10 minutes, GPS synchronization may take up to 45 minutes.
	Wrong MME IP address set	Verify the MME IP address on FW-300i
	MME unreachable	Verify that there is network connectivity between FW-300i and MME
	SCTP/GTP filtering	Verify that firewall along the path does not filter SCTP or GTP traffic
	eNB related misconfiguration on EPC	Verify on EPC that eNB is allowed to connect to it (typically EPC will either work in unrestricted mode that allows any eNB to connect, or each eNB has to be allowed explicitly)
<b>CPE unable to form link with FW-300i</b>	Link is down due to loss of GPS sync	Reboot the FW-300i.
	Wrong RF channel number	Verify the RF channel number configured on CPE to confirm that it matches to FW-300i
	APN misconfiguration	Verify the APN configured on CPE is the same as in the CPE profile on EPC
	Cell range misconfiguration	Verify FW-300i cell range parameter is larger or equal to the distance of the furthest CPE
<b>CPE unable to pass data traffic</b>	Link is down	Confirm that the RF channel number is correctly configured on CPE. Restart CPE to trigger network entry again
	Link quality is poor	Analyze the link performance metrics (RSRP, CINR, Tx Pwr) on the CPE to determine if it's being served by the best available sector. Antenna orientation optimization may be required.
	APN misconfiguration	If CPE is operating in bridge mode, ensure that on EPC there is an APN defined for user traffic.



## 7 Customer Premise Equipment (CPE)

BLiNQ Networks offers a wide variety of CPEs, designed to meet your needs. Please contact BLiNQ for more information.

You can also use a third party CPE to connect to the FW-300i. If so, please consult your third party CPE manual for details on this equipment or the relevant CPE Configuration Manual.

## Appendix A BLiNQ Wireless Devices and RF Safety/Les appareils sans fil BLiNQ et la sécurité RF

**REMARQUE:** La traduction française suit le texte anglais.

BLiNQ Networks evaluates all of its products to ensure that they conform to the Radio Frequency (RF) energy emission safety limits adopted by the Federal Communications Commission (FCC). BLiNQ Networks conducts these evaluations using the compliance rules and guidelines adopted by both the FCC and Industry Canada. They are based on the results of the Maximum Permissible Exposure (MPE) studies by the FCC for mobile or fixed devices, which dictate MPE limits for human exposure to RF energy.

Before selling any wireless networking device to the public, BLiNQ Networks submits its devices to the FCC and Industry Canada for MPE (that is, RF emissions) studies and evaluation. These studies must demonstrate that the device meets the accepted regulatory limits for safe RF emissions, or it is not approved for sale by the FCC and thus cannot be sold to the public. This means that when wireless networking devices, purchased from BLiNQ Networks, are installed and operated as instructed, the RF emissions from the devices is equal to or less than the levels accepted as safe by the FCC and Industry Canada.

When used as intended, BLiNQ wireless networking devices do not pose health risks. Like other devices that emit RF energy (such as computers and microwave ovens), the level of RF emissions from BLiNQ devices is too low to cause harm. Further, BLiNQ wireless networking devices emit far lower levels of RF energy than cellular and cordless telephones, and are almost always used further away from the human body.

To prevent unnecessary exposure to RF energy:

- Always install the FW-300i system so as to provide and maintain a minimum separation distance of at least 1.1 metre from all persons.
- When the FW-300i system is operational, avoid standing directly in front of the FW-300i antennas. RF energy fields may be present when the transmitter is on.
- When the FW-300i system is operational, maintain a distance of at least 1.1 metre (43.3 inches) from the FW-300i antennas.
- Do not install the FW-300i system in a location where it is possible for people to stand or walk inadvertently in front of an antenna.

### Antenna Statement:

The antenna used for this transmitter must be installed to provide a separation distance of at least 1.1 metre (43.3 inches) from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

---

BLiNQ Networks évalue l'ensemble de ses produits afin de s'assurer qu'ils sont conformes à la limite d'émission énergétique sécuritaire de radiofréquence (RF) adoptée par la «Federal Communications

Commission» (FCC). BLiNQ Networks effectue ces évaluations en utilisant les règles et lignes directrices adoptées à la fois par le FCC et Industrie Canada. Elles sont basées sur les résultats de l'exposition maximale admissible, études menées par le FCC sur les appareils mobiles ou fixes, qui dictent les limites de l'exposition maximale admissible pour l'exposition humaine aux énergies RF.

Avant de vendre tout appareil de réseau sans fil au public, BLiNQ Networks présente ses appareils au FCC et à Industrie Canada pour l'évaluation de l'exposition maximale admissible. Ces études doivent démontrer que l'appareil est conforme aux limites réglementaires acceptées pour les émissions RF, sinon les appareils ne sont pas approuvés pour la vente par la FCC et ne peuvent donc pas être vendus au public. Cela signifie que lorsque des équipements sans fil, achetés auprès de BLiNQ Networks, sont installés et utilisés conformément aux instructions, les émissions RF provenant des dispositifs sont inférieures ou égales aux niveaux acceptés comme étant sécuritaire par la FCC et Industrie Canada.

Lorsqu'utilisés comme prévu, les périphériques sans fil BLiNQ ne posent pas de risques pour la santé. De la même façon que les autres appareils qui émettent de l'énergie RF (comme les ordinateurs et les fours à micro-ondes), le niveau des émissions RF des dispositifs BLiNQ est trop faible pour causer des dommages. En outre, les dispositifs de réseau sans fil BLiNQ émettent des niveaux beaucoup plus faibles d'énergie RF que les téléphones cellulaires et sans fil, et sont presque toujours utilisés loin du corps humain.

Pour éviter toute exposition inutile à l'énergie RF:

- Installer toujours le système FW-300i afin de fournir et de maintenir une distance de séparation minimale de 1.1 mètre au moins pour les personnes.
- Lorsque le système FW-300i est opérationnel, éviter de se tenir directement devant les antennes du FW-300i et leurs antennes internes. Les champs d'énergie RF peuvent être présents lorsque l'émetteur est en marche.
- Lorsque le système FW-300i est opérationnel, maintenir une distance d'au moins 1.1 mètre (43.3 pouces) à partir des antennes du FW-300i.
- Ne pas installer le système FW-300i dans un endroit où il est possible pour les gens de se tenir debout ou de marcher en face d'une antenne.

**Déclaration d'antenne:**

L'antenne utilisée pour cet émetteur doit être installée de façon à créer une distance de séparation d'au moins 1.1 mètre (43.3 pouces) de toute personne et ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou émetteur. Les utilisateurs et les installateurs doivent avoir reçus des instructions d'installation de l'antenne et des conditions de fonctionnement de l'émetteur pour satisfaire la conformité aux expositions RF.

## A.1 Equipment Compliance

---

### A.1.1 Federal Communications Commission (FCC) Notices

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.



**CAUTION:** Any changes or modifications not expressly approved by BLiNQ Networks could void the user's authority to operate this equipment.

## Appendix B PCI Planning Guidelines

When setting up your system, you must abide by the rules outlined below in order to minimize Physical Cell ID (PCI) collision and enforce an effective PCI assignment strategy:

### Rule 1: Same PCI Utilization

- Multiple cells within a FW-300i on the same frequency should not have the same PCI
- Immediate neighbour cells on the same frequency should not have the same PCI

### Rule 2: PCI MOD3

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD3 (i.e.,  $PCI_{cellA} \neq PCI_{cellB}$ )
- Occurs due to the fact that when PCI X is changed by a factor of  $X+3n$  (where n is an integer) there is a collision on the reference signals between the two antenna ports, i.e., between the PCI[X]-antenna port0 and PCI[X+3n]-antenna port1
- Applicable for MIMO transmission only

### Rule 3: PCI MOD6

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD6
- Applicable for SISO transmission only

### Rule 4: PCI MOD30+

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD30
- Occurs due to the collision of the uplink (UL) reference signals (RS) which leads to a higher bit error rate (BER) in the UL

### Rule 5: PCI MOD50 (20MHz Bandwidth (BW)) or PCI MOD25 (10MHz BW)

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD50/MOD25
- Occurs due to the collision on the Physical Control Format Indicator Channel (PCFICH) which leads to failure in decoding on the Physical Downlink Control Channel (PDCCH)

### Rule 6: Cell Group ID Correlation

- Cell Group ID is derived from two length-31 binary m-sequences (m0, m1)
- Each time m0/m1 repeats, the overall correlation between the two Cell Group ID values is higher
- No impact to the performance of Key Performance Indicators (KPI) due to this type of interference
- Only causes network entry delay (by 5-10ms)

## Appendix C Alarms and Events (Fault Management)



This appendix lists the alarms and events for the BLiNQ FW-300i system.

**Note:** There is no need to open the FW-300i module casing. If there is an unsolvable problem or a module malfunction, please contact our Customer Service Department for help or a return merchandise authorization (RMA) number/procedure.

The FW-300i system issues an alarm notification when a fault condition occurs. You view alarms through the:

- FW-300i WebUI **Events** > **Alarms** page (See Section 6.1.3.1, “*Alarms Page*”)

These alarms require operation and maintenance actions to restore functionality and/or to prevent a more serious situation from developing.

**Error! Reference source not found., Error! Reference source not found.** shows each alarm (whose name also represents the particular problem), the alarm ID, type and explanation on the likely cause of the alarm and possible solution (as applicable).

The FW-300i system issues an event notification when something of importance happens that does not trigger an alarm, but is considered significant enough to take note. You view these events through the:

- FW-300i WebUI **Events** > **History** page (See Section 6.1.3.2, “*History Page*”)

[Table 7-1 List of Alarms](#)

[Table 7-2 Table 7-1 List of Alarms](#)

~~Table 7-2~~, List of Events shows each event (whose name also represents the particular problem), the event ID, type and explanation on the likely cause of the event.

Severity is also defined for each listed alarm and event, to indicate the relative level of urgency for operator action:

- **CRITICAL** — the alarm or event requires immediate corrective action, regardless of the time
- **Major** — the alarm or event requires immediate corrective action, within working hours
- **Minor** — the alarm or event requires corrective action at a suitable time or, at least, continuous close observation
- **Warning** — the alarm or event requires corrective action on a scheduled maintenance basis
- **Information** — the alarm or event requires no corrective action; it is for informational purposes only

ID	NAME	DESCRIPTION/COMMENTS	TYPE	SEVERITY
4001	Ethernet Port Down	Ethernet link is down, can be caused by Eth cable unplugged or connected port defective, administratively disabled, equipment down, etc. System recovers when Ethernet link is re-established.	Comms <sup>1</sup> .	Major
5004	Radio Disabled	An operator has administratively disabled the radio in the unit. Identified per sector.	Equip. <sup>2</sup>	Major
5006	Radio Module Down	Configuration issue e.g. radio enabled but not used by any sector. Identified per RF instance.	Equip.	Major
5008	Radio Temperature Warning	The radio operating temperature has exceeded the normal operating range. Identified per sector.	Equip.	Major
5009	Radio RF Calibration	This alarm usually indicates a hardware failure. The unit should be replaced. Identified per RF instance.	Equip.	CRITICAL
5014	Radio DCA No Frequency Available	The system is using all the available frequency channels and pauses the jump sequence to prevent flip-flopping.	Comms.	Minor
6002	GPS Antenna Failure	This indicates a hardware fault with the GPS antenna of the FW-300i.	Equip.	CRITICAL
6003	Hardware Temperature	The alarm triggers with 2 severity levels: - Major - this warns that temperature is above normal range (85C) and - Critical - when the temperature exceeds safety limits and the radio is stopped (90C).	Equip.	Major/ CRITICAL
6004	Phy Start Issue	Failure to load or start the PHY code.	Comms.	CRITICAL
6005	RF Power Amp Issue	1611 could not start, power failure or other issue	Equip.	CRITICAL
6006	CA Chain Issue	RF card not Carrier Aggregation (CA) capable. Badly configured CA chain.	Comms.	CRITICAL
7001	System GPS Synchronization Lost	When operating in GPS mode, the GPS receiver has lost synchronization. When operating in 1588 mode, the 1588 client has lost communication with the 1588 master clock.  Upon FW-300i reset, this alarm is not raised until 60 s after reset and if synchronization still is not achieved. After holdover time expires (5 minutes), system transitions to unsynchronized state.	Comms.	Major

<sup>1</sup> Comms = Communications

<sup>2</sup> Equip. = Equipment

ID	NAME	DESCRIPTION/COMMENTS	TYPE	SEVERITY
<b>7002</b>	System Synchronization Failed	When operating in GPS mode, the GPS receiver has lost synchronization. When operating in 1588 mode, the 1588 client has lost communication with the 1588 master clock. This alarm is raised when the module fails to achieve system timing synchronization. Probably caused by a loss of signal.	Equip.	<b>CRITICAL</b>
<b>7006</b>	Sync E Unreliable	The provider of SyncE connected to the FW-300i is either malfunctioning or not configured to provide SyncE on the FW-300i connection port.	Comms.	<b>CRITICAL</b>
<b>7010</b>	DHCP Server Unavailable	The system has not been able to obtain a DHCP address.	Comms.	<b>Major</b>
<b>9003</b>	PM Automatic File Upload Failure	The unit could not perform the FTP transfer of the performance data. The FTP system is inaccessible. (Module cannot upload PM files to the specified server. Indicates a server connectivity or access error. System recovers when connectivity/access to the PM server is restored.)	Comms.	Minor
<b>11001</b>	SAS Server Registration Failure (CBSD)	Registration with SAS server failed.	Comms.	<b>CRITICAL</b>
<b>11002</b>	Grant Suspended or Terminated (CBSD)	Grant was suspended or terminated by SAS server.	Comms.	<b>CRITICAL</b>

**Table 7-1 List of Alarms**



**Table 7-2 List of Events**

ID	NAME	DESCRIPTION/COMMENTS	TYPE	SEVERITY
<b>2001</b>	Configuration Changed	A configuration change has been committed to the running configuration.	System	Information
<b>3001</b>	Software Download	Downloading software image.	System	Information
<b>3002</b>	Software Download Successful	Successful download of software image.	System	Information
<b>3003</b>	Software Download Error	Software error: A software download is already in progress.	System	Minor
<b>3004</b>	Software Boot Failure	This may indicate a physical or logical corruption of the system non-volatile storage.	Equip.	<b>CRITICAL</b>
<b>5004</b>	Radio Module Disabled	Radio Module is initialized and has received an administrative disable configuration.	Equip.	Information
<b>7003</b>	System Synchronized	GPS entered synchronized state.	Equip.	Information
<b>7004</b>	GPS State Change	The GPS state machine gained or lost GPS synchronization (specific state indicated by the comment text).	Equip.	Information
<b>8001</b>	Authentication Failed	Attempts to authenticate on one of the management interfaces of the equipment failed.	Security	Warning
<b>10001<sup>1</sup></b>	License successfully applied	A license was successfully applied to module.	System	<b>Major</b>
<b>10002<sup>3</sup></b>	Invalid license	Invalid license: Digital signature does not match license content.	System	<b>Major</b>
<b>10003<sup>3</sup></b>	License not applicable	License not applicable to module: MAC address does not match filter or license capabilities do not match the hardware.	System	<b>Major</b>
<b>12001</b>	S1 State Enabled Event (ENB)	S1 State Enabled	System	Information
<b>12002</b>	UE Attached Event (ENB)	User Equipment (UE) Attached	System	Information
<b>12003</b>	UE Detached Event (ENB)	UE Detached	System	Information

<sup>1</sup> Future Software Release

## Appendix D List of Acronyms

ACRONYM	MEANING
3CC	Three Component Carriers
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting (centralized networking protocol)
AAS	Active Antenna System
ACK	Acknowledgment
AES	Advanced Encryption Standard
AF	Assured Forwarding behavior, DSCP
APN	Access Point Name
ANR	Automatic Neighbour Relation
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
ATP	Automatic Transmit Power
BCCH	Broadcast Channel
BER	Bit Error Rate
BMC	Best Master Clock
BSI	Best Signal Indication
BSR	Buffer Status Report
BTS	Base Transceiver Station
BW	Bandwidth
CAC	Call Admission Control
CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband Radio Service Device
CC	Component Carrier
CDB	Common Database
CINR	Carrier to Interference plus Noise Ratio
CIO	Cell Individual Offset
CIR	Committed Information Rate
CLI	Command Line Interface
CPE	Customer Premise Equipment
CPI	Certified Professional Installer
CPIR-ID	Certified Professional Installer Registration Identification
CQI	Channel Quality Indicator
Craft IP	IP address typically used by technical personnel to test the equipment
CRC	Cyclic Redundancy Check
CS	Class Selector, DSCP
CTX	Channel Transmit

ACRONYM	MEANING
CW	Continuous Wave (carrier)
dBi	Decibel isotropic
DBS	Dynamic Bandwidth Sharing
DCA	Dynamic Channel Assignment
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DRX	Discontinuous Reception
DSCP	Differentiated Services Code Point
DSR	Diameter Signaling Router
DSN	Domain Name System
EARFCN	Evolved Absolute Radio Frequency Channel Number (LTE)
EF	Expedited Forwarding behavior, DSCP
eICIC	Enhanced Inter-Cell Interference Coordination
EIRP	Equivalent/Effective Isotropic Radiated Power
EMS	Element Management System
eNB	See eNodeB
eNodeB	E-UTRAN Node B, also identified as Evolved Node B (abbreviated as eNodeB or eNB) is an element of an LTE Radio Access Network (RAN)
EPC	Evolved Packet Core
EPRE	Energy Per Resource Element
ETWS	Earthquake and Tsunami Warning System
EUTRAN	Evolved Universal Terrestrial Radio Access Network
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FDE	Frequency Domain Equalized
FTP	File Transfer Protocol
FWA	Fixed Wireless Access
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPS	Global Positioning System
GTP	GPRS Tunneling Protocol
HARQ	Hybrid Automatic Repeat reQuest
HD	High Density
HLR	Home Location Register
HO	Handover
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICIC	Inter-Cell Interference Coordination
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

ACRONYM	MEANING
IP	Internet Protocol
ISDN	Integrated Services Digital Network
Kbps	Kilobits per second
KPI	Key Performance Indicators
L2	Layer 2
LL	Low Latency
LLDP	Link Layer Discovery Protocol
LOS	Line-of-Sight
LTE	Long Term Evolution refers to a mobile device, high-speed, wireless communications standard.
MAC	Media Access Control
Mbps	Megabits per second
MCC	Mobile Country Code
MCS	Modulation and Coding Scheme
MHz	Megahertz
MGP	Measurement Gap Configuration Pattern
MIMO	Multiple Input Multiple Output
MIMO-SM	Multiple Output-Spatial Multiplexing
MME	Mobility Management Entity; the key control-node for the LTE access-network
MNC	Mobile Network Code
MPE	Maximum Permissible Exposure
MPLS	Multiprotocol Label Switching
ms or msec	Millisecond
MSB	Most Significant Bit
MSISDN	Mobile Subscriber ISDN Number
MSR	Multi-Standard Radio
MU-MIMO	Multiple-user Multiple Input Multiple Output
NACK	negative acknowledgment
NETCONF	Network Configuration Protocol
nLOS	near Line-of-Sight
NLOS	Non Line-of-Sight
NMS	Network Management System
NOM	Network Operations Mode
OAM	Operations, Administration and Maintenance
OLLA	Outer Loop Link Adaptation
OSS	Operations Support System
PBCH	Physical Broadcast Channel
PCCH	Paging Control Channel (PCCH)
PCFICH	Physical Control Format Indicator Channel
PDCCH	Physical Downlink Control Channel
PDPC	Packet Data Convergence Protocol

ACRONYM	MEANING
PDN	Packet Data Network
PDSCH	Physical Downlink Shared Channel
PHICH	Physical Hybrid-Automatic Repeat Request (ARQ) (HARQ) Indicator Channel
PHR	Power Headroom Report
PHY	Physical Layer
PLMN-ID	Public Land Mobile Network Identifier (PLMN-ID = MCC + MNC)
PM	Performance Measurement
PMI	Precoding Matrix Indicator
PMP	Point-to-Multipoint
PPS	Pulse Per Second
PRACH	Physical Random Access Channel
PSS	Primary Synchronization Signal
PTP	Point-to-Point
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
RAN	Radio Access Network
RARP	Reverse Address Resolution Protocol
RAT	Radio Access Technology
RF	Radio Frequency
RI	Rank Indication
RLC	Radio Link Control
RNTI	Radio Network Temporary Identifier
ROHC	Robust Header Compression
RRC	Radio Resource Control
RS	Reference Signal
RSSI	Received Signal Strength Indicator
RSCP	Received Signal Code Power
RSRQ	Reference Signal Received Quality
RSRP	Reference Signal Received Power
RTP	Received Target Power
RX	Received
s	second
S1	Interface between an eNB and the Core Network (CN)
SAS	Spectrum Access System
SCH	Shared Channel
SCTP	Stream Control Transmission Protocol
SeGW	Security Gateway

ACRONYM	MEANING
SFP	Small form-factor pluggable
SFTP	Secure File Transfer Protocol
SGW	Serving Gateway; routes and forwards user data packets, also acts as mobility anchor
SI	System Information
SIB3	System Information Block type 3
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
SISO	Single Input Single Output
SLA	Service Level Agreement
SMC	Security Mode Command
SNMP	Simple Network Management Protocol
SON	Self-Organizing Network
SPS	Semi-Persistent Scheduling
SR	Scheduling Request
SRB	Signaling Radio Bearer
SRS	Sounding Reference Signal
SSH	Secure Shell protocol
SSS	Secondary Synchronization Signal
S-VLAN	Stacked VLAN
SW	Software
TAC	Tracking Area Code
TAI	Tracking Area Identifier
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexed
TM	Transmission Mode
ToS	Type of Service
TPC	Transmit Power Control
TTI	Transmission Time Interval
TTW	Time To Wait
TX	Transmit
UDP/IP	User Datagram/Internet Protocol
UE	User Equipment
uint16	Unsigned 16-bit integer with specified range, if any
UInt32	Unsigned 32-bit integer with specified range, if any
uint8	Unsigned 8-bit integer with specified range, if any
UL	Uplink
UMTS	Universal Mobile Telecommunications System
U-NII	Unlicensed National Information Infrastructure
URL	Universal Resource Locator

ACRONYM	MEANING
UTC	Coordinated Universal Time
UTRAN	UMTS Terrestrial Radio Access Network
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio
WFP	Weighted Fair Priority
X2	Interface that interconnects eNBs
XPIC	Cross Polarization Interference Cancellation





**© Copyright 2012-2020 BLiNQ Networks Inc. All rights reserved.**

CONFIDENTIAL INFORMATION  
RESTRICTED USE AND DUPLICATION

The information contained herein is the property of BLiNQ Networks Inc. and is strictly confidential. Except as expressly authorized in writing by BLiNQ Networks Inc., the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care.

Except as expressly authorized in writing by BLiNQ Networks Inc., the holder is granted no rights to use the information contained herein.

BLiNQ and BLiNQ Networks Inc. corporate logo are trademarks of BLiNQ Networks Inc. All other trademarks used in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between BLiNQ and any other company.

**Disclaimer**

The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Additionally, BLiNQ Networks makes no representations or warranties, either expressed or implied, regarding the contents of this product. BLiNQ Networks shall not be liable for any misuse regarding this product. The information in this document is subject to change without notice.