



casa systems

**Verizon 4G LTE
Network Extender 3
for Enterprise**

User Guide
v8.1

© 2023 Casa Systems, Inc.

All rights reserved. Licensed software products are owned by Casa Systems or its suppliers and are protected by United States copyright laws and international treaty provisions.

The information regarding the product in this manual is subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of the product.

In no event shall Casa or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Casa or its suppliers have been advised of the possibility of such damages.

Contents

Preface

About this guide	vi
Document revision history.....	vii
Corporate facility	vii
Personal and Product Safety	viii
Site Safety.....	viii
Materials	viii
Electrical	ix
Shipping, Transport, and Manual Handling.....	ix
Installation.....	x
Maintenance	x
Environment.....	x
Grounding	xi
Technical documentation	xi
Support information.....	xi
Safety Warnings.....	xii

Chapter 1. Getting Started

Introduction	1-2
System Requirements	1-3
Network Extender Basics	1-4

Chapter 2. Installation

Unpacking the box	2-2
Required fasteners (not provided)	2-3
Coverage area	2-4
Building Layout	2-4

Installing the wall bracket	2-5
Securing the mounting bracket to the wall	2-6
Securing the mounting bracket to a dropped ceiling	2-9
Connecting the cables	2-13
Optional mounting configurations	2-15
Startup sequence	2-16
Indoor GPS antenna	2-20
INT/EXT antenna	2-22
PoE device	2-23
Making a call	2-25

Chapter 3. Web GUI

PC requirements	3-3
Accessing the Network Extender GUI	3-3
Connect to the GUI via the same network	3-4
Connect to the GUI via the LMT port	3-5
Network Extender GUI overview	3-7
Log in to the Network Extender GUI	3-7
Change admin password upon first login	3-8
Setting a password	3-8
Security questions	3-9
Setting a security answer	3-9
Web GUI header bar	3-10
4G service state management	3-11
Network Extender alarms	3-12
Dashboard	3-13
System Information Dashboard	3-13
System Information	3-14
Operational Status	3-14
Operational History	3-15
Location	3-16
Connected Devices	3-17

Performance	3-18
Alarms	3-19
Settings	3-21
Network Settings	3-21
Advanced Settings	3-26
Sync & Time Settings	3-29
Certificate Management	3-30
User Settings	3-31
Reset Device	3-33
About	3-34
Support	3-34

Chapter 4. Configuration

Firewall settings	4-2
Firewall rules for business	4-5
CSG User Configuration	4-6
CSG modes	4-6
Configuration steps	4-7

Chapter 5. Troubleshooting

Status LEDs	5-2
Alarm troubleshooting	5-4
List of Network Extender 3 Alarms	5-5

Chapter 6. Specifications

Key Specifications	6-1
Physical and Environmental Information	6-3
Supported Services	6-4

Appendix A. FAQs

About this appendix	A-1
Dashboard FAQs	A-3
How to verify the device operation mode	A-3
System Information FAQs	A-4
How to verify if the GPS location was acquired	A-4
How to check the number of connected users	A-5
How to check the active alarms and generate an alarm report	A-6
Settings FAQs	A-7
How to adjust MTU (maximum transfer unit) size	A-7
How to configure a static IP address	A-8
How to add a DNS	A-9
How to add a search domain	A-10
How to manually adjust the device transmission power	A-11
How to change the device operating channel	A-12
How to configure Network Extender Operation Mode	A-13
How to configure Synchronization Source	A-14
How to add a VLAN	A-15
How to set the power source	A-18
How to configure Network Extender Backhaul Limit	A-19
How to reboot or factory reset a device	A-20
CSG mode FAQs	A-21
Where can the user manage the CSG function?	A-21
Will the user be able to determine which CSG IDs are associated with the phone?	A-21
Can the user specify a particular CSG ID number?	A-21
How many CSG ID can be assigned to a Network Extender?	A-21
Will the CSG ID be changed if a Network Extender changed its CSG mode from Hybrid to Closed or vise versa?	A-21
Will different CSG mode impacts E911 calls?	A-21

Preface

About this guide

The *Network Extender 3 User Guide* is intended for system administrators, support engineers, and operators who are responsible for basic installation and configuration of Network Extender units. Users who perform these tasks should be familiar with the Apex hardware and software capabilities, as well as have experience with both 3G and 4G technologies.

The following chapters are provided in this guide:

For information about	See
Getting Started	Chapter 1.
Installation	Chapter 2.
Web GUI	Chapter 3.
Configuration	Chapter 4.
Troubleshooting	Chapter 5.
Specifications	Chapter 6.
FAQs	Appendix A

Document revision history

This document supports the following Network Extender 3 software. See the *Casa Systems – Apex eFemto Small Cell Release Notes* for additional information on new functionality not yet covered in this guide.

- Revision 1.0 — April 2021; initial version, R4.9.24.1
- Revision 2.0 — May 2021; revised version, R4.9.29
- Revision 3.0 — September 2021; initial version, R4.10.8
- Revision 3.1 — October 2021; revised version, R4.10.8.1
- Revision 3.2 — October 2021; revised version, R4.10.9
- Revision 3.3 — November 2021; revised version, R4.10.9
- Revision 4.0 — February 2022; revised Web GUI
- Revision 5.0 — March 2022; revised version
- Revision 6.0 — May 2022; revised Web GUI features
- Revision 7.0 — August 2022; revised version
- Revision 8.0 — December 2022; revised Casa contact information
- Revision 8.1 — January 2023; revised version
- Revision 8.1a — February 2023; revised per Accessibility Report results
- Revision 8.1b — March 2023; revised per Accessibility Report results

Corporate facility

Casa Systems, Inc.
100 Old River Road
Andover, MA 01810

Personal and Product Safety

This product safety information includes U.S. directives that you must follow. All applicable OSHA regulations and standards shall be followed.

The installation, maintenance, or removal of telecommunications equipment requires qualified, experienced personnel. Installation instructions are written for such installation personnel.

Site Safety

Site construction shall be design-approved and certified by engineers who have valid and up-to-date P.E. license approval with the National Society of Professional Engineers.

Workers shall evaluate site safety as per all applicable safety ordinances and requirements including, but not limited to OSHA, NFPA 70, and applicable building code requirements prior to, during, and after completion. Workers shall not conduct product work until and unless the site is in full safety compliance with associated regulatory requirements.

Materials

Workers shall use only approved materials that comply with applicable safety and environmental requirements. All materials shall be deployed in accordance with all applicable safety requirements, and according to manufacturer instruction. Workers shall not install any materials that are intrinsically unsafe, or have shipping, handling, or installation instructions that are intrinsically unsafe.

Electrical

This product contains hazardous energy levels as defined by UL 60950. Care must be taken as injury to personnel or damage to the equipment could result from mistakes. Maintenance should only be carried out by approved workers who have adequate training and understanding and are familiar with the required procedures and instructions.

In addition to all applicable safety requirements, workers shall abide by the latest edition of NFPA 70 national electrical code. Certified and licensed Electricians and Power Limited Technicians shall perform electrical work as required by applicable regulatory requirements.

All structural materials shall be grounded, and all input and outputs shall have built-in isolation from the network as per NFPA 70 standards and client-approved standards. All connectivity and input and output hardware ports that connect to external power sources shall be designed and installed to meet national safety and regulatory requirements.

Shipping, Transport, and Manual Handling

Worker shall assure they understand and abide by all associated regulatory and standards instruction applicable to shipping, transport and handling of product, including but not limited to OSHA and all associated documentation for product shipping, transport, and manual handling requirements.

Worker shall assure adequate and approved shipping, transport, and handling procedures are utilized to maintain safety.

Installation

Installation shall be carried out by trained and competent workers always observing all applicable safety rules and regulations.

Workers shall read, and understand the latest published installation documentation, and make sure all required workers, tools, and materials are approved and present prior to beginning any defined work task.

Workers shall also abide by the latest published installation documentation for general work procedures and guidance materials.

All relevant safety measures must be taken to ensure that equipment is not connected to live power and transmission sources during installation. Equipment must be correctly installed to meet the relevant safety standards and approval conditions.

Maintenance

Maintenance shall be carried out by trained and competent workers while always observing all applicable safety rules and regulations. Equipment covers shall not be removed while live power and/or transmission is connected unless specifically directed by a Casa published work instruction and as determined safe by all associated safety rules and regulations.

Environment

The product must be operated in an environment within the specified relative humidity and ambient temperature ranges.

Keep all liquids away from the equipment, as accidental spillage can cause severe damage.

Grounding

To comply with ANSI/NFPA70 and UL 60950, equipment must be connected to a safety grounding point via a permanent connection. Grounding points are located on the product for this purpose. Always connect the ground cable as per the latest published instructions before fitting other cables. The product must remain grounded continuously unless all system and power connections are removed.

If equipment is grounded through a cabinet or rack, make sure it is done so properly according to the latest published installation instructions.

Technical documentation

Casa Systems provides the following documentation set in PDF format, viewable using current versions of Adobe Reader®. The latest documentation and revisions are uploaded on a continued basis for Verizon customers.

Contact Verizon Support for assistance with downloading selected Casa documentation PDFs.

- *Casa Systems – Apex eFemto Small Cell User Guide* (this document)
- *Casa Systems – Apex eFemto Small Cell Quick Start Guide*

Support information

For detailed instructions and device information, visit:

www.verizon.com/support/4g-lte-network-extender-enterprise-basics/

Customer Support: 800-922-0204

Safety Warnings



AC System: Disconnect AC power, before servicing.



RF Cable Installation: Installation shall be in accordance with the applicable parts of Chapter 8 of ANSI/NFPA 70.



Circuit Breaker: Branch circuit protection.

The power system must be equipped with external branch circuit protection that complies with NEC requirement and have a rating maximum of 20A. (Use UL-listed circuit breaker.)

Chapter 1. Getting Started

About this chapter

This chapter provides Getting Started information for the Network Extender 3.

The following topics are covered in this chapter:

Topic	Page
Introduction	1-2
System Requirements	1-3
Network Extender Basics	1-4

Introduction

This user guide introduces the Verizon Wireless 4G LTE Network Extender 3 for Enterprise, designed to quickly enhance and extend the Verizon Wireless network experience for voice and data.

Figure 1-1. Network Extender 3



This Network Extender provides the following features:

- This Network Extender is a simple-to-install device that provides enhanced in-building wireless service without having to change your existing 4G LTE mobile phone.
- This Network Extender allows users to easily install and configure the system by connecting to an existing broadband network.
- This Network Extender supports an embedded web server, which allows you to customize your device settings providing troubleshooting and operational data.

System Requirements

- This device only supports Verizon Wireless 4G LTE mobile handsets with Advanced Calling turned on, as shown in Chapter 2, [Making a call](#).
- Internet Access: This Network Extender requires an Internet connection to operate and must be connected to an available port on a router or modem with always-on Internet connection with a recommended bandwidth greater than 50mbps.
 - Note:** A lower bandwidth configuration may impact the system performance and user experience.
- GPS signal: This Network Extender requires continuous GPS location to operate. Ensure the supplied GPS antenna is properly installed near or on a window with clear and open view of the sky. Sync LED should be green.
- Firewall modifications may be required to support the solution. Be sure to contact your IT administrator for the required changes. Please review the [Firewall rules for business](#) in Chapter 4. In the event that firewall changes are needed, please attempt to make these changes before calling into Customer Care.
 - Note:** For more clarity on firewall settings, please see [Firewall settings](#) in Chapter 4.
- The Network Extender supports IEEE 802.3ab Gigabit Ethernet Auto-Negotiation. Auto-Negotiation is a requirement of 802.3ab and may cause a speed and/or duplex mismatch if not fully enabled on the Network Extender switch/router port.

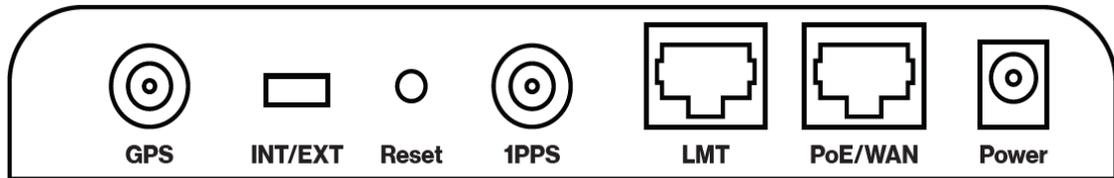
Casa recommends that Full auto-negotiation be enabled. If the Network Extender does not come into service as either 100/Full or 1000/Full, the recommendation is to configure statically as either 1000/Full (if capable) or 100/Full.

Note: If 100/Full is used, the Network Extender can go into service, but throughput will be limited.

Network Extender Basics

This section will guide you through the basic features and functions of your Network Extender. [Figure 1-2](#) details the ports on the back of the Network Extender.

Figure 1-2. Network Extender Ports



The RF Antenna of Network Extender is embedded in the Front cover and 6 different external antenna ports are located on the top of the Network Extender.

The included GPS antenna is required for the automated setup process and is necessary in the event the mobile phone is used to call for emergency services while in the coverage area of the Network Extender. [Table 1-1](#) provides port information for the Network Extender.

The Network Extender has multiple, single color LEDs used to indicate the device connectivity status. Please refer to [Chapter 5, Troubleshooting](#) when attempting to troubleshoot the solution.

Table 1-1. Network Extender port descriptions

Port Name	Function
GPS	To connect GPS antenna and receive GPS signal.
INT/EXT	To select antenna INT (Internal)/EXT (External). WARNING: Incorrect use of this switch may cause PA damage. Refer to INT/EXT antenna (page 2-22) for important information on the proper use of the INT/EXT switch.
Reset	Factory Reset.
1PPS	Reserved for future use.
LMT	Local Monitoring Terminal Port to manage setting and display device status.

Table 1-1. Network Extender port descriptions (continued)

Port Name	Function
PoE/WAN	To connect to a Power over Ethernet (PoE) and/or Wide Area Network (WAN) Port.
Power	To connect Power Supply (12V DC).

Chapter 2. Installation

About this chapter

This chapter includes installation information for the Network Extender 3. The following items are described in this chapter:

Topic	Page
Unpacking the box	2-2
Required fasteners (not provided)	2-3
Coverage area	2-4
Installing the wall bracket	2-5
Securing the mounting bracket to the wall	2-6
Securing the mounting bracket to a dropped ceiling	2-9
Connecting the cables	2-13
Optional mounting configurations	2-15
Startup sequence	2-16
Indoor GPS antenna	2-20
INT/EXT antenna	2-22
PoE device	2-23
Making a call	2-25

Unpacking the box

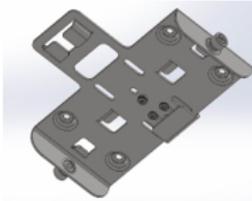
The following items are provided in the Network Extender box:

Figure 2-1. What's included in the box

4G LTE Network Extender 3

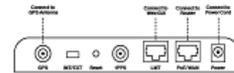


Mounting Bracket



QR Card

4GLTE Network Extender 3 for Enterprise



Instructions

- 1 Connect the GPS antenna cable to the GPS port.
- 2 Position the GPS antenna puck near a window so it provides a clear and open view of the sky.
- 3 Connect the Ethernet cable to the PoE/WAN port and connect the other end of the cable to the local router/switch.
- 4 If there is a Firewall in the network, please ensure the following server connections are available to the eFemto. The server's FQDN/IP addresses can be found in the Network Extender User Guide.
 - GPS Assistance Server: TCP port 80
 - DNS Server: UDP port 53
 - NTP Server: UDP port 123
 - Security Gateway: UDP port 500/4500
 - CMP: TCP port 80
- 5 Plug in the power supply to the Power port and twist to lock (for installations where PoE is not supported).
- 6 **OPTIONAL STEP:** For local configuration, connect a laptop to the LMT port to access the Web-UI. For detailed instructions refer to "Admin website access" in the Network Extender User Guide.
- 7 Mount the Network Extender to a wall or ceiling. Please wait up to 30 minutes for the unit to complete setup and the Status LEDs to turn GREEN indicating normal operation.

Visit www.hispertel.com (supported by the network extender enterprise features) or scan the QR code for detailed instructions and device information.



For more information about our privacy practices, visit www.hispertel.com/privacy
Customer Support: 800-909-0204
000-3907-01
Rev.10

Supplied Power Supply



GPS Antenna (length: 7m)



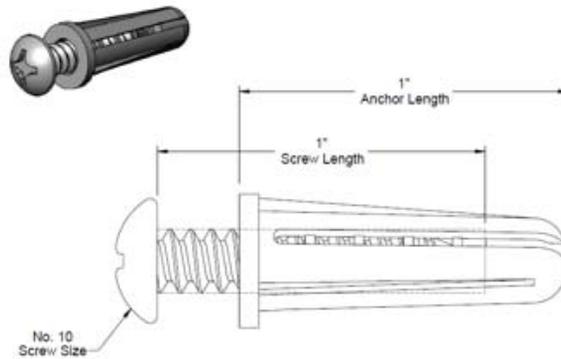
Ethernet Cable



Required fasteners (not provided)

The fasteners shown in [Figure 2-2](#) (Qty: 4) are required to mount the Network Extender to the wall.

Figure 2-2. Fasteners (not provided)



Coverage area

The coverage area of the Network Extender varies based on many factors including; the layout and building materials of the location in which it is deployed. An open floor plan will allow for greater coverage as compared to an office space with many metal and/or concrete walls, which impede the cellular signal.

Use [Table 2-1](#) to estimate coverage area and recommended distance between network extenders when deploying more than one in a location.

Table 2-1. Coverage area

Building Layout	Approximate Range of Network Extender (radius)	Recommended distance between network extenders
Open	200 feet	320 feet
Medium	100 feet	170 feet
Dense	70 feet	120 feet

Note: Coverage area can vary depending on number and size of obstructions and building material types.

Building Layout

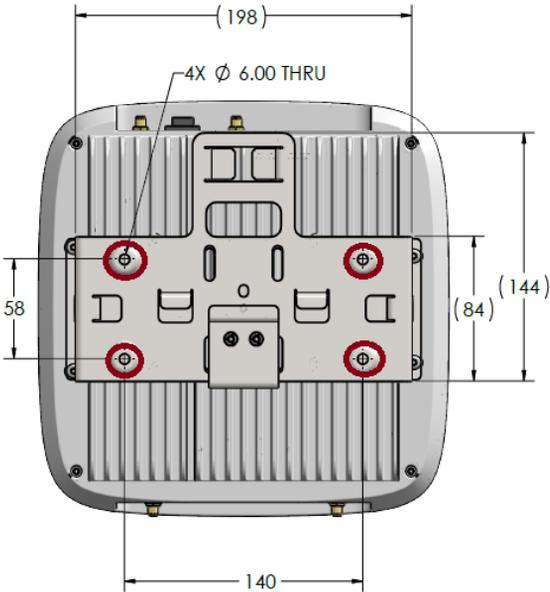
- Open: Open layout with no or few internal walls.
- Medium: mixed layout with open and scattered walled offices.
- Dense: walled office layout with narrow hallways

Installing the wall bracket

Marking the mounting position

Before placing the Network Extender, mark the position where it will be installed and also the positions where anchor bolts will be fixed using a pen or pencil. Mark the 4 holes using the bracket as a guide (see [Figure 2-3](#)).

Figure 2-3. Anchor locations

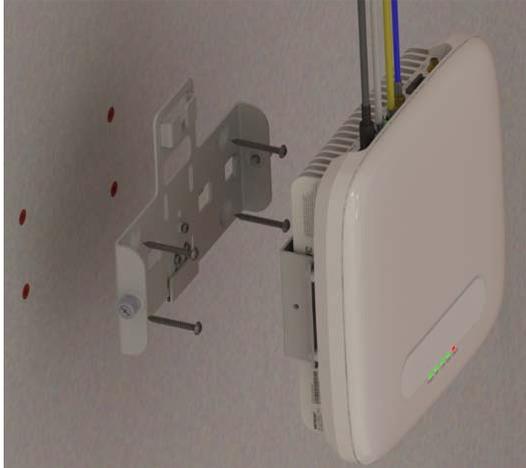


When anchoring on a wall, ensure the positions are marked as horizontal or vertical, as only a limited range of tuning is allowed for leveling after the system is mounted.

Securing the mounting bracket to the wall

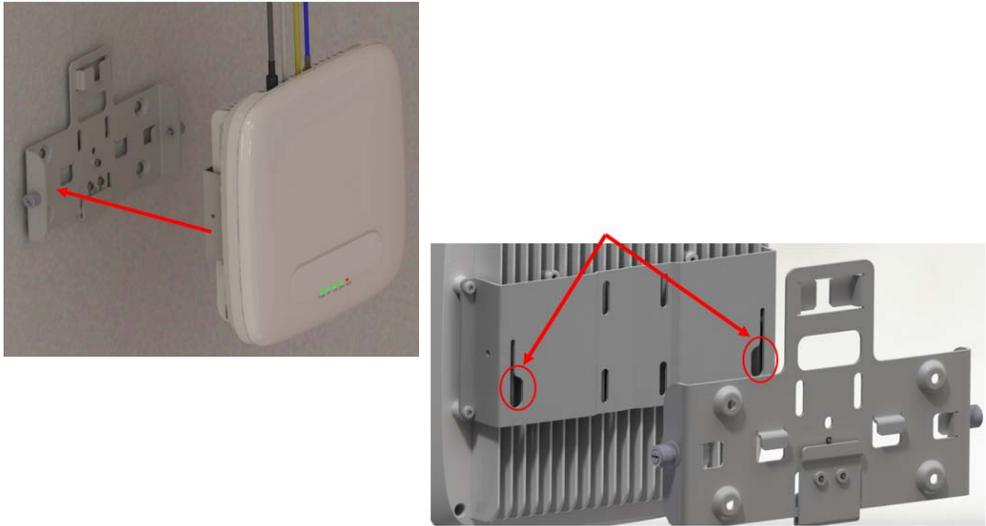
1. Attach the upper bracket to the wall/ceiling (see [Figure 2-4](#)).

Figure 2-4. Attach bracket



2. Align the tabs on the upper bracket with the opening on the lower bracket and push inward (see [Figure 2-5](#)).

Figure 2-5. Align tabs



3. Push downward to seat the unit (see [Figure 2-6](#)).

Figure 2-6. Seat the unit



4. Tighten the screw fasteners, one on each side (see [Figure 2-7](#)).

Figure 2-7. Tighten the fasteners

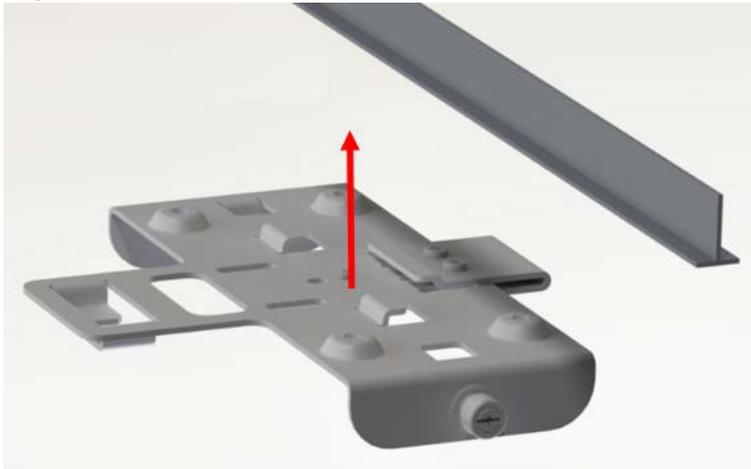
Securing the mounting bracket to a dropped ceiling

The following procedure details how to attach the Network Extender in a suspended ceiling application.

WARNING: Before installing the Network Extender to a dropped ceiling, the installer should ensure that the structure is secure and capable of supporting the weight of the Network Extender. Additional ceiling support hangers may be required to ensure a safe installation and all hangers used for installing the Network Extender should adhere to local building codes.

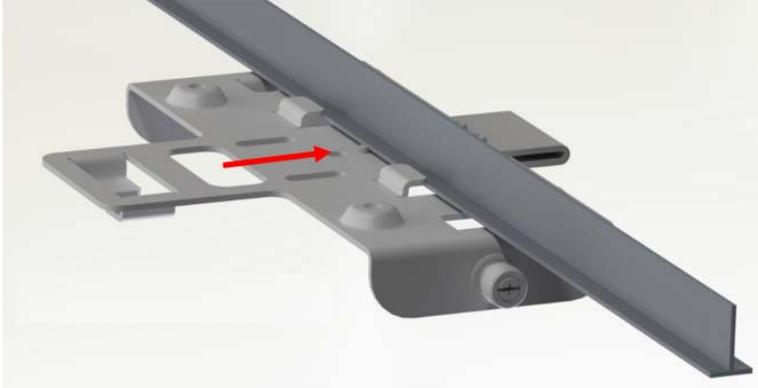
1. Push the upper bracket up against the bottom of the T-Rail (see [Figure 2-8](#)).

Figure 2-8. Push upper bracket



2. Push the upper bracket back against the T-Rail to engage the tabs (see [Figure 2-9](#)).

Figure 2-9. Engage tabs



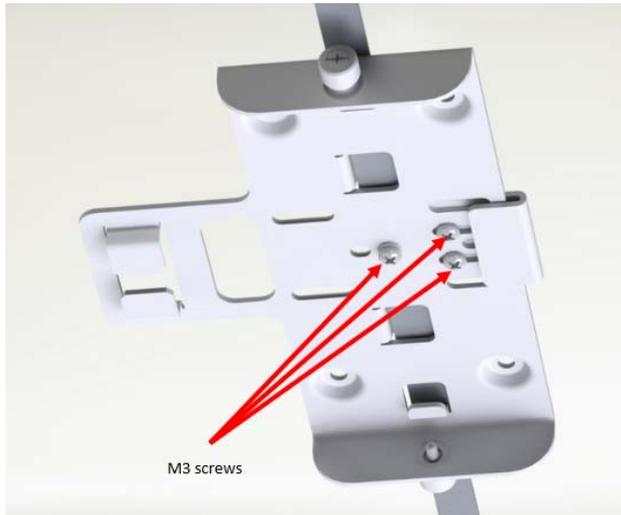
3. Push the clamp back against the T-Rail to engage tabs on both sides of the rail (see [Figure 2-10](#)).

Figure 2-10. Push clamp



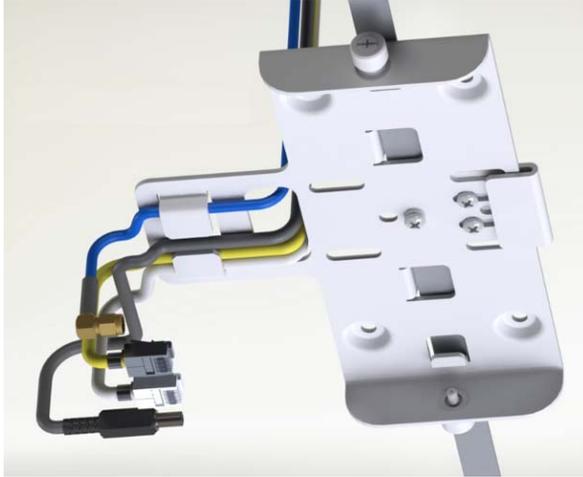
4. Tighten the three M3 screws to lock the clamp and the upper bracket onto the T-Rail (see [Figure 2-11](#)).

Figure 2-11. Tighten screws



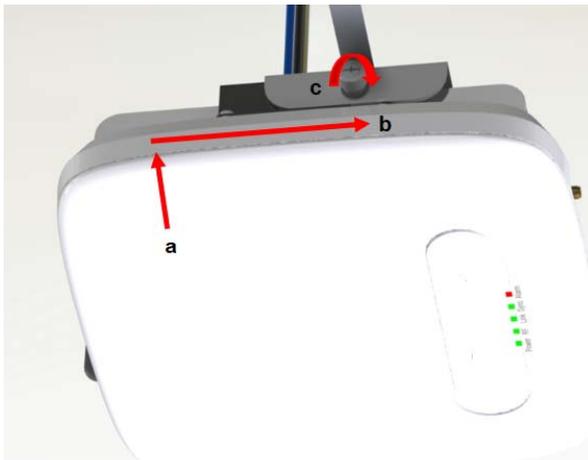
5. Route the cables in the cable management tabs (see [Figure 2-12](#)).

Figure 2-12. Route cables



6. Push the Network Extender up (a) and back (b) locking it into the upper bracket, then tighten the screw fasteners (c) on both sides (see [Figure 2-13](#)).

Figure 2-13. Push the unit



Connecting the cables

The Network Extender unit can be connected to the network via an Ethernet connection. The Ethernet connection is plug-and-play.

1. Connect the GPS antenna cable to the GPS port on the unit (see [Figure 2-14](#)).

Figure 2-14. GPS port



2. Position the GPS antenna puck near a window so it provides a clear and open view of the sky.

WARNING: The unit will not connect to the LTE network if the GPS antenna fails to lock on its location.

3. Connect the Ethernet cable to the PoE/WAN port on the unit (see [Figure 2-15](#)).

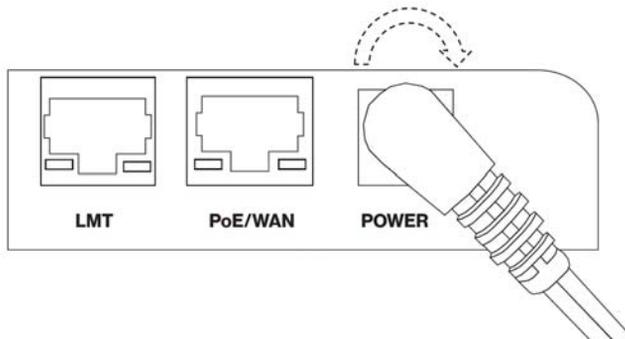
Figure 2-15. PoE/WAN port



4. Connect the other end of the Ethernet cable to a port on the home router/switch or connect it to the Ethernet outlet that has service.

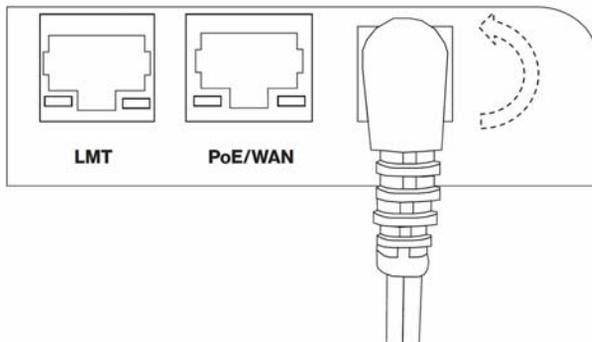
5. To install the power cable, it should be plugged in at 45 Degrees and twist clockwise to secure the power cord in the lock position (see [Figure 2-16](#)).

Figure 2-16. Lock the power cable



6. To unlock the power cable, twist it counterclockwise from the lock position (45 Degrees) as shown in [Figure 2-17](#).

Figure 2-17. Unlock the power cable



Optional mounting configurations

The Network Extender can be mounted on a plenum above the ceiling (see [Figure 2-18](#)) or on a pole (see [Figure 2-19](#)).

Note: The mounting bracket cross bar (shown in [Figure 2-18](#)) is an accessory that is not included with the Network Extender and is shown for reference only.

Figure 2-18. Plenum above ceiling

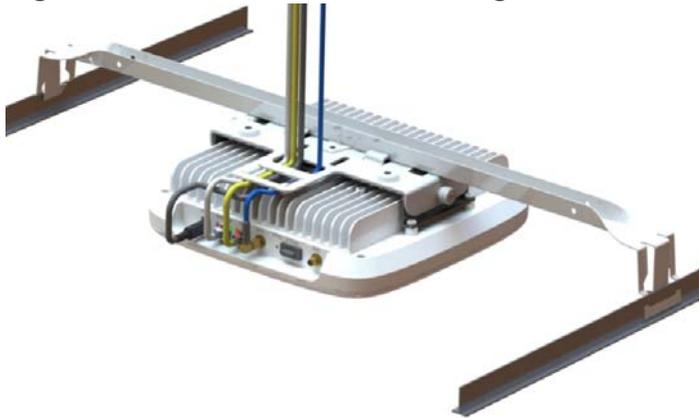


Figure 2-19. Pole mount installation



Startup sequence

The following steps provide detail Network Extender states during the startup sequence. [Table 2-1](#) provides functional details for each status LED during the startup sequence.

Table 2-1. Status LED functions

LED	Color	Function
Power		OFF: Power not detected.
		ON: All the power rails are present.
		Flashing: Unit booting or firmware upgrading.
RF		OFF: Radio activity disabled, not transmitting and receiving.
		ON: Radio activity enabled, unit transmitting and receiving.
Link		OFF: Ethernet link down.
		ON: Ethernet link up.
Sync		OFF: Synchronization not established with the GPS.
		ON: GPS synchronization complete.
		Flashing: Lost GPS synchronization.
Alarm		OFF: No alarms detected.
		Flashing: System critical alarm.

1. Powered-on and hardware initializing.

The Network Extender State: The device has been powered on and the system is performing hardware tests.

Note: The Network Extender is under an autonomous hardware test cycle. It is not possible to load or run any software, including the user Admin Website Page.

2. Hardware test completed and software loaded (“Boot Complete”).

The Network Extender State: The device has completed hardware initialization and loaded all software.

Admin Website State: The software is loaded. The Admin Website is accessible only from the LMT port.

Note: The device has completed its autonomous hardware tests and loaded all software. It will start the process of connecting to Verizon's network and coming into service. See [Accessing the Network Extender GUI](#) for information on how to log into the Network Extender Admin Web page.

3. Acquired IPv4 address (“Acquired an IP address”).

The Network Extender State: The device is running its software and has started to connect to the Verizon network.

The unit is configured by default to acquire a local IPv4 address from the local DHCP server.

Admin Website State: The Admin Website is accessible from the LMT and WAN ports.

4. Conducting DNS lookups (“Identifying the Initial Network”).

The Network Extender State: The device has acquired a local IPv4/IPv6 address from local DHCP. The next step is to conduct DNS lookups for the public FQDNs provisioned at the factory.

Admin Website State: The Admin Website is accessible.

Note: The Network Extender needs to resolve the FQDNs for A-GPS, and initial SeGW from the public DNS server.

5. GPS acquisition in progress (“Waiting for GPS position fix”).

The Network Extender State: The device is awaiting a GPS fix before progressing.

Admin Website State: The Admin Website is accessible.

Note: Until a GPS fix is provided, the device will not be able to continue and receive configuration information.

6. Attempting to reach the Initial SeGW (“Attempting to reach Initial network”).

The Network Extender State: The device has conducted DNS lookups for the public FQDNs provisioned at the factory and is trying to contact the initial SeGW.

Admin Website State: The Admin Website is accessible.

Note: This status details that the Network Extender has attempted to communicate with the SeGW.

7. Successfully reached the Initial SeGW (“Successfully reached the Initial network”).

The Network Extender State: The device has contacted the initial SeGW successfully.

Admin Website State: The Admin Website is accessible.

Note: Status details that the device can communicate with the SeGW, but the IPSec tunnel is still not established at this point.

8. VPN setup to Initial SeGW completed (“Authentication to Initial Network completed successfully”).

The Network Extender State: The device has brought up the IPSec tunnel with the initial SeGW.

Admin Website State: The Admin Website is accessible.

Note: This confirms that the device has set up a VPN connection with Verizon's network.

9. Authentication failure during IPSec tunnel setup to Initial SeGW (“Authentication failure to Initial Network. Unit is not provisioned. Please contact Verizon Wireless Customer Care for further assistance”).

The Network Extender State: The device has failed to set up a VPN tunnel with the initial SeGW with an explicit “Authentication Failure.”

Admin Website State: The Admin Website is accessible.

Note: This details that the device been notified it failed authentication with the Verizon Authentication server.

10. Connection with the management system (“Connecting to Initial Management Server”).

The Network Extender State: The device acquired location information and is connecting with the AeMS.

Admin Website State: The Admin Website is accessible.

Note: The device will be allocated a serving AeMS and possibly an alternate serving SeGW based on its location. It may re-establish IPsec to the new SeGW at this point if required. If not, it will contact the AeMS and request configuration information.

11. Software download in progress.

The Network Extender State: The device is assigned a AeMS and has been instructed to download new software.

Admin Website State: The Admin Website is accessible.

Note: The device will download the newest software and reboot. The process will start from the first steps again, but the GPS acquisition will occur much faster.

12. Configuration download in progress.

The Network Extender State: The device is communicating with the Verizon management system (AeMS) and may have received new software. It will need to complete the “Radio Environment Scan” before receiving additional configuration parameters.

Admin Website State: The Admin Website is accessible.

Note: During the REM scan process, if no adjacent neighbor Network Extenders or Macro cells are detected, the Verizon Management system (AeMS) will then provide the configuration solely based on the GPS location.

13. Operational status.

The Network Extender State: The device is in normal in-service operation and has completed all steps.

Admin Website State: The Admin Website is accessible.

Note: If the Alarm LED state is Red, this means an alarm condition has occurred. In this case, please refer to [Alarm troubleshooting](#) in Chapter 5, for more information on alarm codes.

Indoor GPS antenna

The Network Extender receives timing information from the GPS. The Network Extender is required to be placed such that the GPS receiver has an unobstructed line of sight with at least 4 strong satellites in order for it to get a position fix during the booting process. Thereafter, the Network Extender is required to maintain sync with at least one satellite to be able to continue to monitor the position fix.

Without adequate GPS signal, the Network Extender cannot function properly. When positioning the Indoor GPS antenna, ensure that it is:

- Installed in a horizontal position.
- Adjacent to a window and in an open area. This ensures clear reception of the GPS signal.
- 7m GPS antenna (included)

Note: Extended length GPS antenna cables and PTP servers are available, see [Verizon Network Extender support page](#)

This section outlines the installation and relocation of the Indoor GPS Line (see [Figure 2-20](#)).

Figure 2-20. GPS port



1. Turn off the Network Extender.
2. Connect the provided Indoor GPS antenna cable to the GPS port on the Network Extender.
3. Place the antenna near a window where the GPS signal is stronger. To help evaluate GPS signal quality in each location, a free smart phone application called “GPS Test” can be used.
4. Turn on the Network Extender to allow the detection of an available GPS signal.

Notes:

If GPS signal cannot be detected, reposition the GPS antenna and place it in a new location to receive a stronger signal. This new location should be located close to a window. In some cases, if the GPS signal indoors is very weak, an external outdoor GPS (not included) may need to be installed.

A GPS signal is required for proper operation and E911 service. If a GPS signal is not acquired after 30 to 60 minutes, please see [Configuration steps](#) in Chapter 4.

To see the status of the GPS acquisition, use the Admin website (Local) as shown in [System Information Dashboard](#) in Chapter 3.

INT/EXT antenna

The Network Extender provides a switch (INT/EXT) (see [Figure 2-21](#)) used to select an Internal or External Antenna for the Network Extender.

Figure 2-21. INT/EXT switch



Setting the Network Extender to EXT without an external antenna connected will end with PA damage. Changing the switch during unit operation produces the same effect.

- INT means internal antennas are used.
- EXT is to use the connectors available in the back to connect external antennas/DAS.

Warning: The mechanical switch should be changed only when the unit is powered off or when the radio is disabled.

PoE device

The Network Extender provides the ability to be powered with an ultra-high Power over Ethernet (Class 5 PoE++) source (see [Figure 2-22](#)).

Figure 2-22. PoE/WAN port



[Table 2-1](#) provides the recommended PoE specifications for the Network Extender.

Table 2-1. Recommended PoE specifications

Characteristic	Recommendation
Maximum Output Power	60W
Output Current	960mA ~ 1.1A
Minimum Voltage	50V
Ethernet Output Interface Specification	CAT5e or better 4-pair powering: (Pin 3,4,5,6(+)) Pins 1,2,7,8(-))

The Network Extender's PoE details are as follows:

Power class negotiation

- Fully supported standard power negotiation protocol including PoE++ hardware negotiation and LLDP negotiation.
- Have a fixed class 5 setting in the Network Extender. When it is powered by 802.3bt, it will ask for 40W and when it is powered by 802.3at, it will get maximum 25.5W.
- The Web GUI indicates that only the licensed band will be used when 802.3at is available.

Available power awareness

- A UART interface has been provided between the CPU and the POE controller to read the assigned power class, disabling the RF when a lower power class is provided by the Power Device.

The LED indicator on the Network Extender indicates errors associated with the PoE port. See [Status LEDs](#) in Chapter 5 for more details.

Making a call

Once the Network Extender is in service, your phone must be within 50 feet of the Network Extender to connect to the Network Extender and make calls.

To verify your Verizon phones are connected to the Network Extender:

- Make sure your Verizon Wireless 4G LTE mobile phone has the Advanced Calling feature turned on.
- Dial #48 from your mobile phone and listen for the following confirmation: “You are under 4G LTE Network Extender coverage ...”
- Some phones may show a home icon when connected to the Network Extender.

Note: The Network Extender's coverage depends on environmental factors, such as physical structures and the strength of external cell towers.

To turn on Advanced Calling on your 4G LTE Verizon Wireless phone, follow the steps below for your device's operating system:

- Android™: Go to Settings > Advanced Calling and turn ON service.

Note: On some devices, it may be found in Wireless Calling, HD Voice or VoLTE call.

- Apple® iOS: Go to Settings > Cellular > Cellular Data Options > Enable LTE > Voice & Data. Additionally, on the “My Verizon” Mobile App, enable Advance Calling feature for your phones.
- Windows®: Go to Settings > Cellular+SIM > SIM settings and turn ON Advanced Calling.

Chapter 3. Web GUI

About this chapter

This chapter contains detailed information regarding the Casa Systems Network Extender 3 Admin Website (Local) where you can monitor the device status and make changes to settings. The following topics are covered in this chapter:

Topic	Page
PC requirements	3-3
Accessing the Network Extender GUI	3-3
Connect to the GUI via the same network	3-4
Connect to the GUI via the LMT port	3-5
Network Extender GUI overview	3-7
Log in to the Network Extender GUI	3-7
Change admin password upon first login	3-8
Setting a password	3-8
Security questions	3-9
Setting a security answer	3-9
Web GUI header bar	3-10
4G service state management	3-11
Network Extender alarms	3-12
Dashboard	3-13
System Information	3-14
Operational Status	3-14
Operational History	3-15

Topic	Page
Location	3-16
Connected Devices	3-17
Performance	3-18
Alarms	3-19
Settings	3-21
Network Settings	3-21
Advanced Settings	3-26
Sync & Time Settings	3-29
Certificate Management	3-30
User Settings	3-31
Reset Device	3-33
About	3-34
Support	3-34

PC requirements

To access the Admin Website, a PC should satisfy the following conditions:

- Internet Explorer: 11 (Edge is recommended)
- Chrome: 35.0.1916.153 or higher version
- Firefox: 30.0 or higher version
- Safari: 7.0.2 or higher version
- Internet connection

Accessing the Network Extender GUI

There are two ways to access the Network Extender website GUI.

1. Directly connect to Network Extender by using the Network Extender IP address, in case your computer is connected to the [Network Extender GUI overview](#) as the Network Extender.
2. Use the [Connect to the GUI via the LMT port](#) on the back side of the Network Extender.

Connect to the GUI via the same network

To connect to the Network Extender GUI, you need to know the Network Extender IP address and your computer needs to be connected to the same network of the Network Extender.

1. Use a computer connected to the same network as the Network Extender.
2. Open a browser.
3. Enter the IP address of the Network Extender into the address bar:

`https://< IP address of Network Extender >`

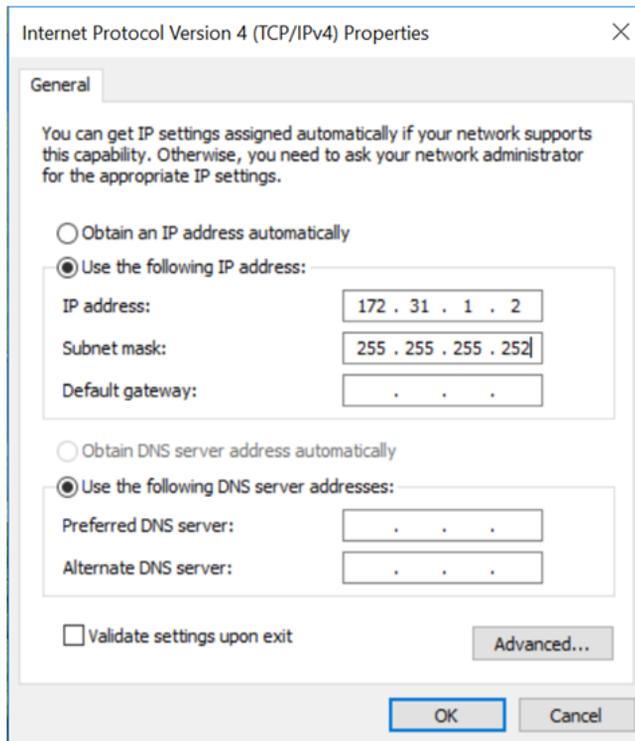
Connect to the GUI via the LMT port

To connect to the Network Extender GUI, you will need to change your TCP/IPv4 settings to connect directly to the LMT port from your laptop, using an Ethernet cable.

To access settings and manage the Network Extender, login to the web interface by following these steps:

1. In Windows, click **Control Panel** on the Start menu.
2. Click **Network and Sharing Center**.
3. Click the **Local Area connection** icon that represents your Ethernet connection.
4. Change the Internet Protocol Version 4 (TCP/IPv4) Properties for the local computer Ethernet connection as shown in [Figure 3-1](#), then click **OK**.

Figure 3-1. IPv4 (TCP/IPv4) Properties



5. Open Internet Explorer and enter <https://172.31.1.1/> into the address bar.
6. Click **Continue** and accept the self-signed Internet site certificate warning to launch the 4G LTE Network Extender 3 for Enterprise Admin Website.

Note: The device CA certificate can be downloaded from the Certificate Management page and added to trusted certificates in the Web browser to avoid future warnings (see [Figure 3-2](#)).

Figure 3-2. Certificate Management

The screenshot displays the Verizon Network Extender 3 web interface. The top navigation bar includes the Verizon logo, device status (CASA-ENB, Boot, 0 Users, Location Acquired), and system indicators (Power, Link, Sync, RF, Alarm). The user is logged in as 'admin'.

The left sidebar contains a navigation menu with sections: DASHBOARD (eFemto Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), SETTINGS (Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device), and ABOUT (Support). The 'Certificate Management' option is highlighted.

The main content area is titled 'SETTINGS / CERTIFICATE MANAGEMENT' and 'Certificate Management'. It features three tabs: 'Server Certificate' (selected), 'Operator Certificate', and 'Login Certificate'. Below the tabs, the 'Server Certificate Information' section provides details for the 4G LTE Network Extender Web Server certificate.

Server Certificate Information
This section allows downloading the Certification Authority certificate of the 4G LTE Network Extender Web Server.

Subject		Issuer	
Common Name	*.network-extender3.com	Common Name	Casa Systems Small Cells SubCA
Organization	Casa Systems	Organization	Casa Systems
Country	US	Country	US
State/Province	Massachusetts	State/Province	Massachusetts
Locality	Andover	Locality	Andover

Validity		Miscellaneous	
Not Before	9/6/2021, 8:00:00 PM	Serial Number	040DBF9A59D5342AEDDE44C31EF1A
Not After	1/26/2051, 7:00:00 AM	E4D	
		Version	3

A prominent black button labeled 'Download Server CA Certificate' is centered below the certificate details.

At the bottom of the page, a footer indicates 'Powered by Casa Systems Inc. - 4GLTE Network Extender 3' and a warning: 'Some external web pages may be not accessible when connecting to this device via the LMT port'.

Network Extender GUI overview

The Network Extender website GUI gives you detailed information on your Network Extender unit's status. You can also use the website to change settings. The Welcome page shows basic device information such as the Network Extender unit's MAC address, GPS fix location, device name, and IP address.

Log in to the Network Extender GUI

1. Once you are at the Welcome Page, enter the User and Password (see [Figure 3-3](#)).

The default administrator password is **VzWNetExtender3@ + last six digits of the MAC**. The MAC ID can be found on the label on the side of the Network Extender.

Example: VzWNetExtender3@213DA5

Note: The password is case-sensitive. Letters in the last six digits of the MAC ID should be UPPER case. The default password and all Network Extender settings can be set back to default by pressing the reset button located on the back of the Network extender for more than 10 seconds.

2. Click **Log in**.

Figure 3-3. The login page

4G LTE Network Extender
verizon✓

User
admin

Password
.....

Log in

[Forgot your password?](#)

[Login with certificate](#)

Change admin password upon first login

If the user is logging in using the default password, a warning pop-up window will be displayed, asking the user to set a new password. Clicking the OK button on the pop-up will navigate the user to the Settings > Change Admin Password page.

The Network Extender Change Password tab allows you to change the local Admin Password for the Network Extender. In the event of a lost password, insert a mini precision screwdriver or insulated tool into the RESET hole on the back of the Network Extender and hold for 10 seconds to reset the Network Extender to factory default settings.

Setting a password

Set a password following the rules described below:

- The password should be between 8 and 64 characters long.
- The password shall include uppercase characters, lowercase characters, numbers and special characters (!, ", #, \$, %, &, *, ?, @).
- The password should include one special character.
- The password should not include more than three identical characters in a row ("111", "aaa", "CCC").
- The password should include at least one lowercase letter, one uppercase letter and one number.
- The new password should not be identical to the current password.

Security questions

Select a Security Question among the five given questions listed below:

- What is your date of birth (mmddyy)?
- What is your birthplace?
- What was your first car?
- What is your mother's maiden name?
- What is your pet's name?

Setting a security answer

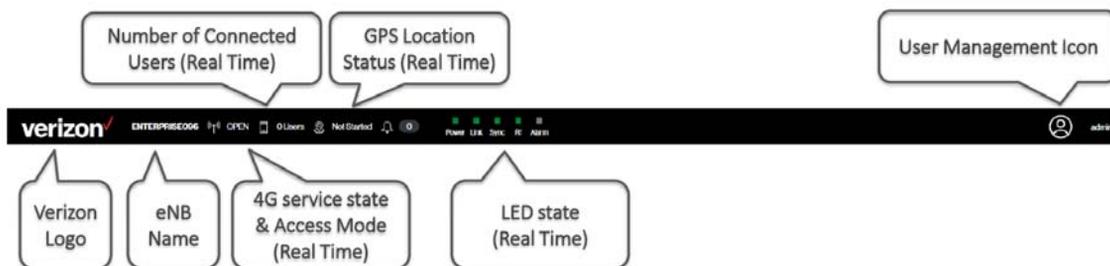
Set a Security Answer that should be between 1 and 64 characters long.

Web GUI header bar

The top of the Web GUI includes a Header Bar (see [Figure 3-4](#)) that provides contextual information which is dynamically updated by the Web GUI application in real time without the user's intervention.

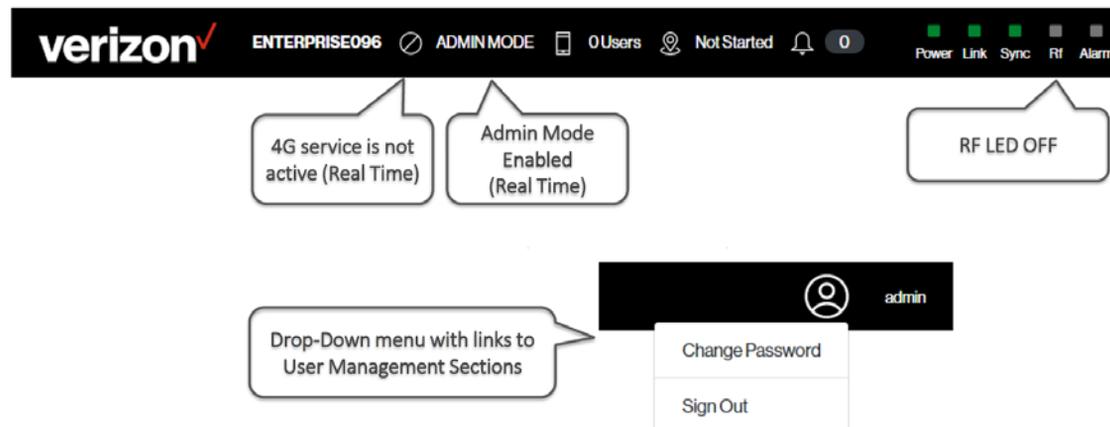
Header Bar information is common to all pages. The LEDs in the Header Bar show the same status as the physical LEDs on the Network Extender.

Figure 3-4. Header Bar



The Header Bar includes a shortcut to a drop-down menu providing access to the User Management sections and the ability to change the password and Sign Out (see [Figure 3-5](#)).

Figure 3-5. Header Bar drop-down menu



4G service state management

The Network Extender state management and operation mode is provided on the Header Bar and is maintained dynamically (see [Figure 3-6](#)). [Table 3-1](#) provides a short description for each Network Extender state.

Figure 3-6. Operational mode indicator



Table 3-1. Service states

Network Extender State	Descriptions
NO SERVICE	LTE Service not active or stopped - No communication with the device or Critical Failure.
BOOT	LTE Service not active or stopped because the Network Extender device is booting.
ADMIN MODE	LTE Service not active or stopped because of ADMIN MODE activation.
OPEN	LTE Service active and OPEN Access Mode.
HYBRID	LTE Service active and HYBRID Access Mode.
CLOSED	LTE Service active and CLOSED Access Mode.

Network Extender alarms

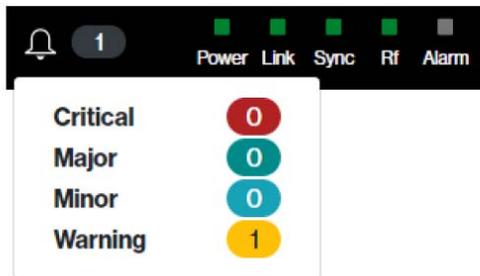
The alarms drop-down menu shows the active alarms in the system in all pages (see [Figure 3-7](#)).

Figure 3-7. Active alarms



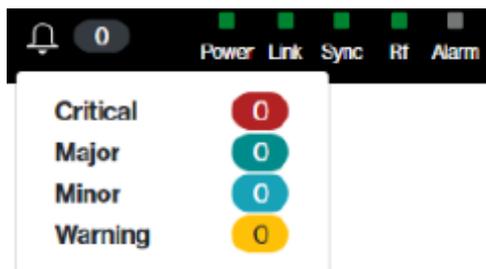
The alarms drop-down menu showing a Warning alarm (see [Figure 3-8](#)).

Figure 3-8. Alarm drop-down menu



The alarms drop-down menu showing no alarms (see [Figure 3-9](#)).

Figure 3-9. No alarms

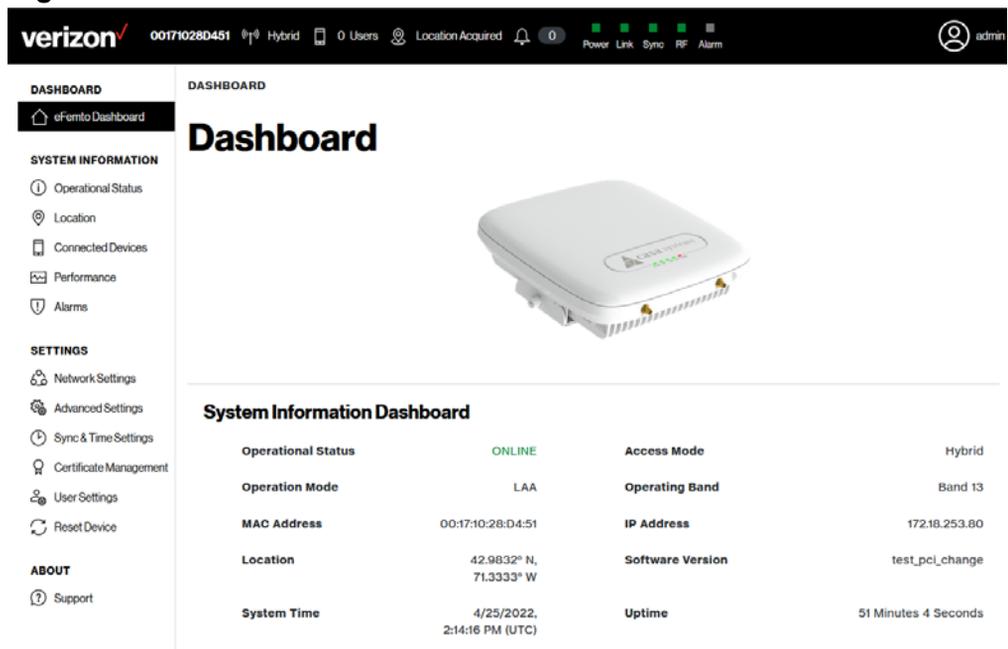


Dashboard

The Network Extender Dashboard (see [Figure 3-10](#)) provides both system information and Network Extender settings.

Refer to the following FAQ (in Appendix A) for detailed instructions:
[How to verify the device operation mode](#)

Figure 3-10. Network Extender dashboard



Dashboard

System Information Dashboard

Operational Status	ONLINE	Access Mode	Hybrid
Operation Mode	LAA	Operating Band	Band 13
MAC Address	00:17:10:28:D4:51	IP Address	172.18.253.80
Location	42.9832° N, 71.3333° W	Software Version	test_pci_change
System Time	4/25/2022, 2:14:16 PM (UTC)	Uptime	51 Minutes 4 Seconds

System Information Dashboard

Operational Status: Operational status of the Network Extender.

Operation Mode: Operational mode status of the Network Extender.

MAC Address: MAC Address of the Network Extender.

Location: GPS location of the Network Extender.

System Time: Date and time of the System which the Network Extender is connected.

Access Mode: Access mode of the Network Extender.

Operating Band: Operational band supported by the Network Extender.

IP Address: IP Address of the Network Extender.

Software Version: Latest version software loaded onto the Network Extender.

Uptime: Total time the Network Extender has been online.

System Information

Operational Status

The Operational Status page (see [Figure 3-11](#)) is a read only page and provides operational status for both the device and the 4G service.

Refer to the following FAQ (in Appendix A) for detailed instructions:

[How to verify if the GPS location was acquired](#)

Figure 3-11. Operational Status page

The screenshot displays the Verizon Network Extender's Operational Status page. The interface includes a top navigation bar with the Verizon logo, device model (VERIZON-D458), and various status indicators like 'Open', '0 Users', 'Not Started', and 'Power Link Sync RF Alarm'. A sidebar on the left contains navigation options for Dashboard, System Information (Operational Status, Location, Connected Devices, Performance, Alarms), Settings (Network, Advanced, Sync & Time, Certificate, User, Reset), and About (Support). The main content area is titled 'SYSTEM INFORMATION / OPERATIONAL STATUS' and features a 'Operational Status' tab. It is divided into two sections: 'Device Operational Status' and '4G Service Operational Status'. The Device section lists: Power Source (PSU), Ethernet Link (UP), IP Address (DHCP 192.168.61.57), GPS Location (Not Started), DNS (Configured), and IPsec (Waiting For Location). The 4G Service section lists: S1 Link (SETUP), Current Status (ONLINE), HeMS (Connected), and Last refresh (3/4/2022, 12:12:50 PM).

Device Operational Status			
Power Source	PSU	GPS Location	Not Started
Ethernet Link	UP	DNS	Configured
IP Address	DHCP 192.168.61.57	IPsec	Waiting For Location

4G Service Operational Status			
S1 Link	SETUP	HeMS	Connected
Current Status	ONLINE	Last refresh	3/4/2022, 12:12:50 PM

Operational History

The Operational Status page is a read only page and provides operational history (see [Figure 3-12](#)).

Figure 3-12. Operational History page

The screenshot displays the Verizon eFemto Dashboard interface. At the top, the Verizon logo and device information (VERIZON-D458) are visible. The dashboard includes a navigation menu on the left with sections for Dashboard, System Information, Settings, and About. The main content area is titled 'Operational Status' and features a sub-section for 'Operational History'. A search bar and a 'Generate report' button are present above a table of events.

Event Time	Event Type	Additional Info
3/4/2022, 10:49:14 AM	eNB Online	
3/4/2022, 10:49:09 AM	DNS Resolution Success	
3/4/2022, 10:49:09 AM	Admin Mode Enabled	
3/4/2022, 10:48:42 AM	eNB Online	
3/4/2022, 10:48:36 AM	DNS Resolution Success	
3/4/2022, 10:48:36 AM	Admin Mode Enabled	
3/4/2022, 10:48:11 AM	eNB Online	

Location

The Location page is a read only page and provides specific location information for the device along with a position map (see [Figure 3-13](#)).

Figure 3-13. Location page

The screenshot displays the Verizon eFemto Location page. The top navigation bar includes the Verizon logo, system status (CASA-ENB, Boot, 0 Users, Location Acquired, 1 notification), and a user profile (admin). The left sidebar contains navigation options: DASHBOARD (eFemto Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), SETTINGS (Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device), and ABOUT (Support). The main content area is titled 'SYSTEM INFORMATION / LOCATION' and 'Location'. It features a 'Device Location' section with the following data:

- Latitude:** 42.6914° N
- Longitude:** 71.2031° W
- Altitude:** 32767 m
- Satellites:** 4

Below this is a 'Satellite Quality Legend' table:

SNR (dB)	Quality
31-99	strong
20-30	fair
0-19	weak

To the right is a 'Device Position Map' showing a street view with a blue location pin. The map includes labels for 'River Road', 'Old River Road', and 'Federal Street'. A 'Report a problem' link and '© OpenStreetMap contributors' are visible at the bottom of the map.

Connected Devices

The Connected Devices page is a read only page and provides specific information for all active UEs in the system (see [Figure 3-14](#)).

Refer to the following FAQ (in Appendix A) for detailed instructions:
[How to check the number of connected users](#)

Figure 3-14. Connected Devices page

The screenshot shows the Verizon eFemto dashboard with the following elements:

- Header:** Verizon logo, ID 00171028D451, Hybrid mode, 1 User, Location Acquired, and status indicators for Power, Link, Sync, RF, and Alarm.
- Navigation Menu:**
 - DASHBOARD:** eFemto Dashboard
 - SYSTEM INFORMATION:** Operational Status, Location, **Connected Devices** (selected), Performance, Alarms
 - SETTINGS:** Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device
 - ABOUT:** Support
- Main Content:**

SYSTEM INFORMATION / CONNECTED DEVICES

Connected Devices

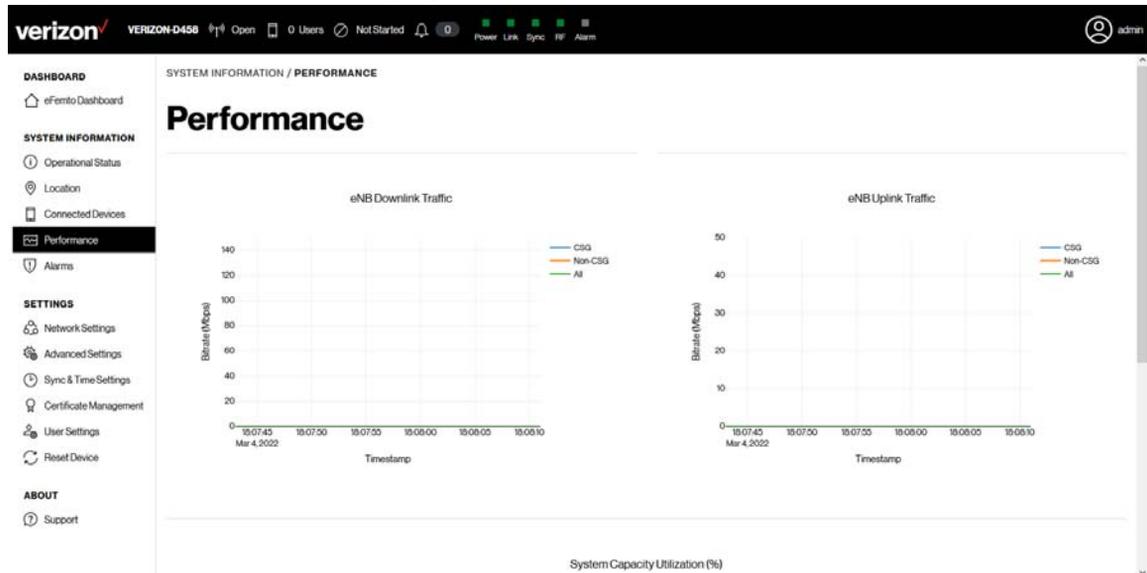
UE ▲	Type	CSG Membership	DL Traffic (kbps)	UL Traffic (kbps)
1	LTE	Yes	0	0
- Summary Statistics:**

Total DL traffic Mbps	0	Total UL traffic Mbps	0	Max number of CSG users During the last 8 hours	1	Max number of Non-CSG users During the last 8 hours	1
---------------------------------	----------	---------------------------------	----------	---	----------	---	----------

Performance

The Performance page is a read only page and displays traffic data for eNB Downlink and Uplink Traffic (see [Figure 3-15](#)).

Figure 3-15. Performance graphs



Alarms

The Alarms page is a read only page and displays Active Alarms data (see [Figure 3-16](#)) and Alarm History (see [Figure 3-17](#)).

Refer to the following FAQ (in Appendix A) for detailed instructions:
[How to check the active alarms and generate an alarm report](#)

Figure 3-16. Active Alarms page

verizon CASA-ENB No Service 0 Users Location Acquired Power Link Sync RF Alarm admin

SYSTEM INFORMATION / ALARMS

Alarms

[Active Alarms](#) [Alarm History](#)

Active Alarms

Search: [Generate report](#)

Raised Time	Event Type	Probable Cause	Specific Problem	Perceived Severity	More info
1/18/2022, 12:01:54 PM	Processing Error	Configuration or Customization Error	Critical configuration failure	Critical	+
1/18/2022, 11:59:48 AM	Communications	Connection Establishment Error	IPsec tunnel is down	Critical	+

10 Showing 1 to 2 of 2 entries [First](#) [Previous](#) [Next](#) [Last](#)

Powered by Casa Systems Inc. - 4G LTE Network Extender 3 Some external web pages may be not accessible when connecting to this device via the LMT port

Figure 3-17. Alarm History page

The screenshot shows the Verizon alarm history page. The top navigation bar includes the Verizon logo, device ID 'VERIZON-D458', and various status icons. The left sidebar contains navigation options for Dashboard, System Information, and Settings. The main content area is titled 'Alarms' and includes a search bar and a 'Generate report' button. Below these is a table of alarm history entries.

Raised Time	Cleared Time	Event Type	Probable Cause	Specific Problem	Perceived Severity
3/4/2022, 10:49:08 AM	3/4/2022, 10:49:09 AM	Communications	Connection Establishment Error	MME connection is down	Critical
3/4/2022, 10:49:08 AM	3/4/2022, 10:49:09 AM	Communications	Connection Establishment Error	Single MME connection is down	Warning
3/4/2022, 10:49:08 AM	3/4/2022, 10:49:09 AM	Communications	Communication Protocol Error	SCTP failure	Major
3/4/2022, 10:48:35 AM	3/4/2022, 10:48:37 AM	Communications	Connection Establishment Error	MME connection is down	Critical
3/4/2022, 10:48:35 AM	3/4/2022, 10:48:37 AM	Communications	Connection Establishment Error	Single MME connection is down	Warning
3/4/2022, 10:48:35 AM	3/4/2022, 10:48:36 AM	Communications	Communication Protocol Error	SCTP failure	Major

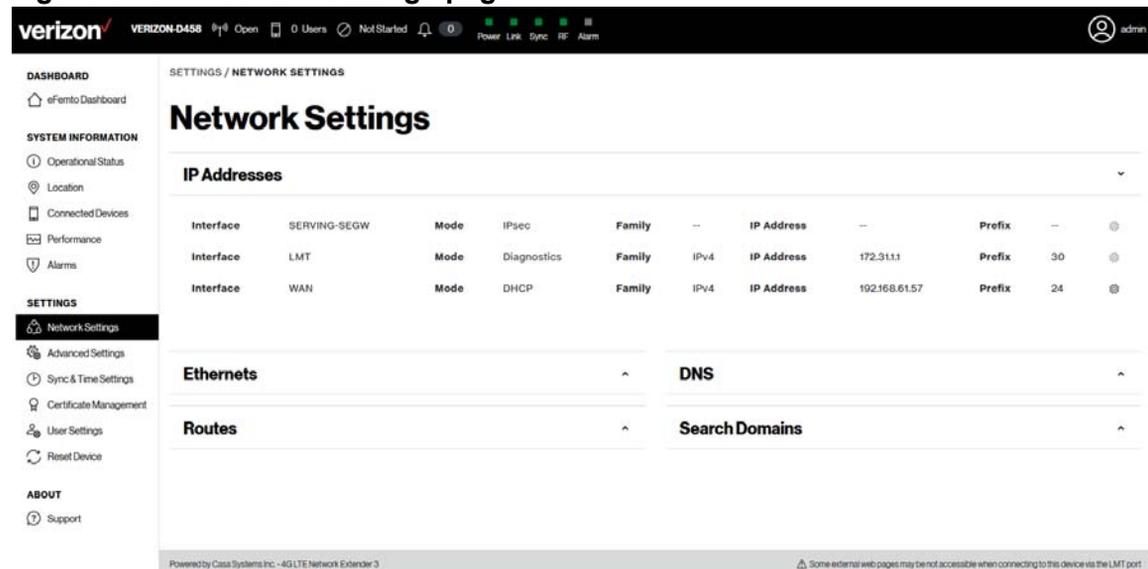
Settings

Network Settings

The Network Settings page (see [Figure 3-18](#)) displays the following:

- [IP Addresses](#),
- [Ethernets](#) information,
- [DNS](#) data,
- [Routes](#),
- [Search Domains](#) settings,
- [VLAN](#) information.

Figure 3-18. Network Settings page



verizon VERIZON-D458 0 Users Not Started Power Link Sync RF Alarm admin

DASHBOARD
eFemto Dashboard

SYSTEM INFORMATION
Operational Status
Location
Connected Devices
Performance
Alarms

SETTINGS
Network Settings
Advanced Settings
Sync & Time Settings
Certificate Management
User Settings
Reset Device

ABOUT
Support

SETTINGS / NETWORK SETTINGS

Network Settings

IP Addresses

Interface	Mode	Family	IP Address	Prefix
SERVING-SEGW	IPsec	--	--	--
LMT	Diagnostics	IPv4	172.31.1.1	30
WAN	DHCP	IPv4	192.168.61.57	24

Ethernets

DNS

Routes

Search Domains

Powered by Casa Systems Inc. - 4G LTE Network Extender 3

Some external web pages may be not accessible when connecting to this device via the LMT port.

IP Addresses

The IP Addresses section of the Network Settings page includes information on each Interface, Mode, Family, IP Address, and Prefix (see [Figure 3-19](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions:
[How to configure a static IP address](#)

Figure 3-19. IP Addresses

IP Addresses										
Interface	SERVING-SEGW	Mode	IPsec	Family	--	IP Address	--	Prefix	--	
Interface	LMT	Mode	Diagnostics	Family	IPv4	IP Address	172.31.1.1	Prefix	30	
Interface	WAN	Mode	DHCP	Family	IPv4	IP Address	172.18.253.80	Prefix	24	
Interface	INITIAL-SEGW	Mode	IPsec	Family	IPv6	IP Address	2607:f160:10:23f2::10	Prefix	128	

Ethernets

The Ethernets section of the Network Settings page displays Ethernet information including Interface, MAC Address, and MTU settings (see [Figure 3-20](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions: [How to adjust MTU \(maximum transfer unit\) size](#)

Figure 3-20. Ethernets

Ethernets						
Interface	WAN	MAC Address	00:17:10:28:D4:51	MTU	1448	
Interface	LMT	MAC Address	02:17:10:28:D4:51	MTU	1500	

DNS

The DNS section of the Network Settings page displays DNS information including IP and Label for each active DNS (see [Figure 3-21](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions: [How to add a DNS](#)

Figure 3-21. DNS

DNS				
IP	8.8.8.8	Label	dhcp	
IP	2607:f160:10:242c:ce:103:0:6	Label	ipsec	
IP	2607:f160:10:242c:ce:103:0:5	Label	ipsec	

Routes

The Routes section of the Network Settings page displays active route information (see [Figure 3-22](#)).

Figure 3-22. Routes

Routes								▼
From	default	To	default	Gateway	172.18.253.1	Label	dhcp	🗑️

Search Domains

The Search Domains section of the Network Settings page displays active domains (see [Figure 3-23](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions:
[How to add a search domain](#)

Figure 3-23. Search Domains

Search Domains	▼
Search Domains not configured	
Add Search Domain	

VLAN

The VLAN section of the Network Settings page allows you to configure a VLAN (see [Figure 3-24](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions:
[How to add a VLAN](#)

Figure 3-24. VLANs

VLAN

VLAN not configured

Configure VLAN

Advanced Settings

The Advanced Settings page provides access to the eNB configuration page (see [Figure 3-25](#)), PCell configuration page (see [Figure 3-26](#)), and the SCell configuration page (see [Figure 3-27](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions:

[How to add a DNS](#)

[How to change the device operating channel](#)

[How to configure Network Extender Operation Mode](#)

eNB Configuration page

Figure 3-25. Advanced Settings > eNB configuration page

The screenshot displays the Verizon eNB configuration page. The top navigation bar includes the Verizon logo, device ID (00171028D451), and various status indicators like Hybrid mode, 0 Users, Location Acquired, and system health (Power, Link, Sync, RF, Alarm). The user is logged in as 'admin'.

The left sidebar contains a navigation menu with sections: DASHBOARD (eFemto Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), SETTINGS (Network Settings, **Advanced Settings**, Sync & Time Settings, Certificate Management, User Settings, Reset Device), and ABOUT (Support).

The main content area is titled 'SETTINGS / ADVANCED SETTINGS' and 'Advanced Settings'. It has three tabs: 'eNB configuration' (selected), 'PCell configuration', and 'SCell configuration'.

ENB Configuration

eNB Name	00171028D451	eNB ID	264318572
CSG ID	16777219	Access Mode	Hybrid
Operation Mode	LAA	VoLTE Emergency Calls	True

Neighbour Cells

Cell ID	PCI	EARFCN	eNB ID
264318615	479	5230	264318615

Showing 1 to 1 of 1 entries

Navigation buttons: First, Previous, Next, Last

PCell configuration page

Figure 3-26. Advanced Settings > PCell configuration page

The screenshot displays the Verizon eFemto Advanced Settings page. The top navigation bar includes the Verizon logo, device ID (00171028D451), network type (Hybrid), user count (1 User), and location status (Location Acquired). The main content area is titled 'Advanced Settings' and is divided into three tabs: 'eNB configuration', 'PCell configuration' (which is selected), and 'SCell configuration'. The 'PCell configuration' tab contains two sections: 'Primary Cell Radio Configuration' and 'Transmission Power Configuration'. The 'Primary Cell Radio Configuration' section lists various parameters such as Primary PLMNID, PCI, Operating Band, DL Bandwidth, Reference Signal Power, Cell Barred, Cell ID, TAC, EARFCN, UL Bandwidth, RF Tx Status, and Administrative State. The 'Transmission Power Configuration' section lists Tx Power and Enable Manual Power Selection.

Primary Cell Radio Configuration			
Primary PLMNID	311480	Cell ID	264318572
PCI	481	TAC	15861
Operating Band	Band 13	EARFCN	5230
DL Bandwidth	10 MHz	UL Bandwidth	10 MHz
Reference Signal Power	-10	RF Tx Status	On
Cell Barred	False	Administrative State	True

Transmission Power Configuration			
Tx Power	21 dBm	Enable Manual Power Selection	<input type="checkbox"/>

SCell configuration page

Note: When the Network Extender Operation Mode is set to LAA, the SCell configuration page displays as shown in [Figure 3-27](#).

Figure 3-27. Advanced Settings > SCell configuration page

The screenshot shows the Verizon eFemto Advanced Settings page. The top navigation bar includes the Verizon logo, device ID (00171028D451), Hybrid mode, 0 Users, Location Acquired, and status indicators for Power, LAA, Sync, RF, and Alarm. The user is logged in as 'admin'.

The left sidebar contains the following menu items:

- DASHBOARD
 - eFemto Dashboard
- SYSTEM INFORMATION
 - Operational Status
 - Location
 - Connected Devices
 - Performance
 - Alarms
- SETTINGS
 - Network Settings
 - Advanced Settings**
 - Sync & Time Settings
 - Certificate Management
 - User Settings
 - Reset Device
- ABOUT
 - Support

The main content area is titled 'SETTINGS / ADVANCED SETTINGS' and 'Advanced Settings'. It has three tabs: eNB configuration, PCell configuration, and **SCell configuration**.

The 'Secondary Cell Radio Configuration' section displays the following parameters:

PCI	402	Cell ID	264318572
Operating Band	Band 4	EARFCN	46890
DL Bandwidth	20 MHz	TAC	15861
Reference Signal Power	-7	RF Tx Status	On
Administrative State	True		

The 'Transmission Power Configuration' section shows a slider for Tx Power set to 27 dBm. A 'Set Tx Power' button is located below the slider. A callout box displays the current settings: Tx Power 27 dBm, 501 mW.

Sync & Time Settings

The Sync & Time Settings page displays Common Synchronization Configuration settings (see [Figure 3-28](#)).

Refer to the following FAQ (in Appendix A) for detailed instructions:
[How to configure Synchronization Source](#)

Figure 3-28. Sync & Time Settings page

verizon CASA-ENB Boot 0 Users Location Acquired 1 Power Link Sync RF Alarm admin

DASHBOARD

- eFemto Dashboard

SYSTEM INFORMATION

- Operational Status
- Location
- Connected Devices
- Performance
- Alarms

SETTINGS

- Network Settings
- Advanced Settings
- Sync & Time Settings**
- Certificate Management
- User Settings
- Reset Device

ABOUT

- Support

SETTINGS / SYNC & TIME SETTINGS

Sync & Time Settings

Common Synchronization Configuration

Synchronization Source	PTP - IEEE 1588V2	Status	Synchronized
Mode	Frequency	Failure Action	System Reboot
Holdover Period	86400 seconds	Holdover Action	System Reboot

[Configure Sync Source](#)

1588v2 PTP Configuration

NTP Servers Configuration

Time Zone Configuration

Powered by Casa Systems Inc. - 4G LTE Network Extender 3 Some external web pages may be not accessible when connecting to this device via the LMT port

Certificate Management

The Certificate Management page displays Server Certificate Information for the select device (see [Figure 3-29](#)).

Figure 3-29. Certificate Information page

The screenshot shows the Verizon web interface for Certificate Management. The top navigation bar includes the Verizon logo, device status (CASA-ENB, Boot, 0 Users, Location Acquired), and system controls (Power, Link, Sync, RF, Alarm). The user is logged in as 'admin'.

The left sidebar contains a navigation menu with sections: DASHBOARD (eFemto Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), SETTINGS (Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device), and ABOUT (Support). The 'Certificate Management' option is highlighted.

The main content area is titled 'SETTINGS / CERTIFICATE MANAGEMENT' and 'Certificate Management'. It features tabs for 'Server Certificate' (selected), 'Operator Certificate', and 'Login Certificate'. Below the tabs is the 'Server Certificate Information' section, which includes a description: 'This section allows downloading the Certification Authority certificate of the 4G LTE Network Extender Web Server.' The information is presented in a table format:

Subject		Issuer	
Common Name	*.network-extender3.com	Common Name	Casa Systems Small Cells SubCA
Organization	Casa Systems	Organization	Casa Systems
Country	US	Country	US
State/Province	Massachusetts	State/Province	Massachusetts
Locality	Andover	Locality	Andover
Validity		Miscellaneous	
Not Before	9/6/2021, 8:00:00 PM	Serial Number	040DBF9A59D5342AEDDE44C31EF1A
Not After	1/26/2051, 7:00:00 AM	E4D	
		Version	3

Below the table is a prominent black button labeled 'Download Server CA Certificate'.

The footer of the page contains the text: 'Powered by Casa Systems Inc. - 4G LTE Network Extender 3' and a warning: 'Some external web pages may be not accessible when connecting to this device via the LMT port'.

User Settings

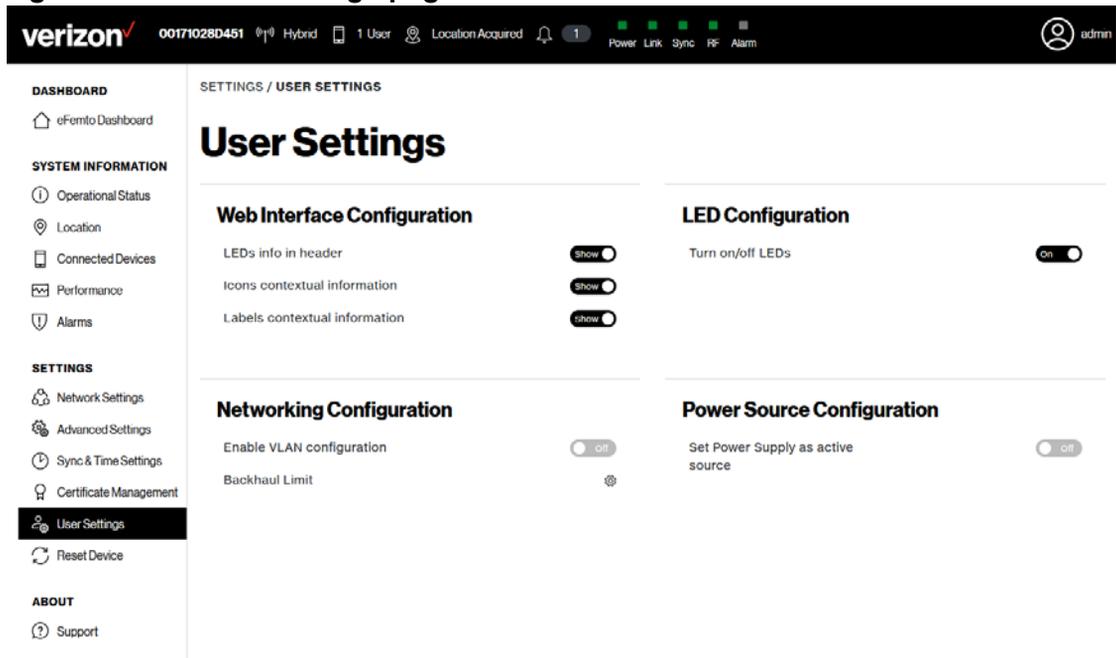
The User Settings page displays Web Interface Configuration, LED Configuration, and Network Configuration (see [Figure 3-30](#)).

Refer to the following FAQs (in Appendix A) for detailed instructions:

[How to add a VLAN](#)

[How to configure Network Extender Backhaul Limit](#)

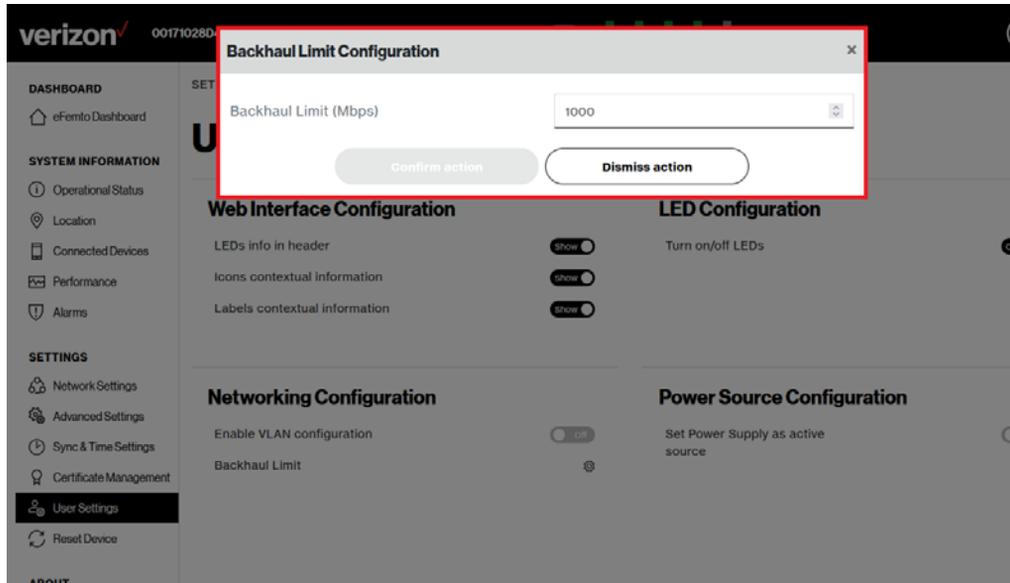
Figure 3-30. User Settings page



Setting the Backhaul Limit

The User Settings page provides configuration options for the Network Extender Backhaul Limit (see [Figure 3-31](#)).

Figure 3-31. Backhaul Limit Configuration dialog



Reset Device

The Reset Device page provides the ability to reset the Network Extender device and perform a Factory Reset (see [Figure 3-32](#)).

Refer to the following FAQ (in Appendix A) for detailed instructions:
[How to reboot or factory reset a device](#)

Figure 3-32. Reset Device page

The screenshot displays the Verizon eFemto Admin Web GUI. At the top, a black navigation bar features the Verizon logo, 'CASA-ENB', and various status icons: a refresh icon for 'Boot', a mobile phone icon for '0 Users', a location pin for 'Location Acquired', a bell for '1' notifications, and a row of colored squares for 'Power', 'Link', 'Sync', 'RF', and 'Alarm'. A user profile icon labeled 'admin' is in the top right.

The left sidebar is divided into sections:

- DASHBOARD**: eFemto Dashboard
- SYSTEM INFORMATION**: Operational Status, Location, Connected Devices, Performance, Alarms
- SETTINGS**: Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, **Reset Device** (highlighted)
- ABOUT**: Support

The main content area is titled 'SETTINGS / RESET DEVICE' and 'Reset Device'. It contains two primary actions:

- Reset Device**: A section with a paragraph explaining that this functionality remotely powers resets the 4G LTE Network Extender. It notes that if there are active E911 calls, the reset will be delayed until they are resolved. Once completed, connectivity is lost, and the user must reload the page and log back into the Admin Web GUI app. Below this text is a black button labeled 'Reboot eFemto'.
- Factory Reset**: A section with a paragraph explaining that this functionality remotely factory resets the 4G LTE Network Extender. It states that if there are active E911 calls, the reset will be delayed until they are resolved. This operation reverts all custom settings, including the WebAdmin GUI password and Static IP configuration. After the reset, connectivity is lost, and the user must reload the page and log back into the Admin Web GUI app. Below this text is a white button with a black border labeled 'Factory Reset eFemto'.

At the bottom of the page, a grey footer contains the text: 'Powered by Casa Systems Inc. - 4G LTE Network Extender 3' on the left and 'Some external web pages may be not accessible when connecting to this device via the LMT port' on the right.

About

Support

The Support page provides contact information to obtain customer support (see [Figure 3-33](#)).

Figure 3-33. Support page

verizon CASA-ENB Boot 0 Users Location Acquired 1 Power Link Sync RF Alarm admin

DASHBOARD

- eFemto Dashboard

SYSTEM INFORMATION

- Operational Status
- Location
- Connected Devices
- Performance
- Alarms

SETTINGS

- Network Settings
- Advanced Settings
- Sync & Time Settings
- Certificate Management
- User Settings
- Reset Device

ABOUT

- Support

ABOUT / SUPPORT

Support

Visit [verizon.com/support/4g-lte-network-extender-enterprise-basics](https://www.verizon.com/support/4g-lte-network-extender-enterprise-basics) for detailed instructions and device information.

For more information about our privacy practices, visit [verizon.com/about/privacy](https://www.verizon.com/about/privacy).

Customer Support: 800-922-0204

Powered by Casa Systems Inc. - 4G LTE Network Extender 3 ⚠️ Some external web pages may be not accessible when connecting to this device via the LMT port

Chapter 4. Configuration

About this chapter

This chapter describes firewall settings for configuring the Network Extender 3. The following topics are covered in this chapter:

Topic	Page
Firewall settings	4-2
Firewall rules for business	4-5
CSG User Configuration	4-6

Firewall settings

The Network Extender is designed to connect and automatically configure with minimal user involvement, though in some cases, depending on the firewall settings, some settings may need to be adjusted on the local LMT (see [Figure 4-1](#)).

Figure 4-1. LMT port



[Table 4-1](#) provides details on the destination ports regarding the firewall settings that are applicable for network administrators.

Table 4-1. Destination ports

Source	Destination	Protocol	Destination Port	Notes
Network Extender	GPS Assistance Server	TCP	80	
Network Extender	DNS Server	UDP	53	
Network Extender	NTP Server	UDP	123	
Network Extender	Verizon Security Gateway	UDP	500/4500	More than one port may be used for multiple device installation.
Network Extender	CMP	TCP	80	
Network Extender	Verizon Security Gateway	ESP/50	N/A	When NAT/PAT is not present.
Verizon SeGW	Network Extender	ESP/50	N/A	When NAT/PAT is not present.

Table 4-2 lists the IP addresses of each of the network elements that need to be included.

Table 4-2. Firewall settings

Network Element	Comment	Fully Qualified Domain Name (FQDN)
GPS Server	-	http://xtrapath1.izatcloud.net http://xtrapath2.izatcloud.net http://xtrapath3.izatcloud.net
Security Gateway (SeGW)	The serving server will be automatically assigned.	sgw.vzwfemto.com The FQDN of the initial-SeGW is resolved by the public DNS server sgw-rcmdva83.vzwfemto.com sgw-chntvaav.vzwfemto.com sgw-wsbomagj.vzwfemto.com sgw-ynkrnyzl.vzwfemto.com sgw-wmtppaaa.vzwfemto.com sgw-esyrnyen.vzwfemto.com sgw-aurscoty.vzwfemto.com sgw-temqazkw.vzwfemto.com sgw-snvacanx.vzwfemto.com sgw-rdmewa22.vzwfemto.com sgw-azusca21.vzwfemto.com sgw-elsstx13.vzwfemto.com sgw-hsnotx08.vzwfemto.com sgw-tulyok13.vzwfemto.com sgw-chrxnclh.vzwfemto.com sgw-orlhfl01.vzwfemto.com sgw-alprgagq.vzwfemto.com sgw-omalnexu.vzwfemto.com sgw-hchlilmt.vzwfemto.com sgw-lenykscj.vzwfemto.com sgw-jhtwpadp.vzwfemto.com sgw-sfldmilr.vzwfemto.com

Table 4-2. Firewall settings (continued)

Network Element	Comment	Fully Qualified Domain Name (FQDN)
CMP	-	cmp.securitycredentialing.com
NTP Server	<p>The default NTP server is based on a pool.ntp.org.</p> <p>Different locations will get different IP addresses.</p> <p>The user needs to make sure the FQDN is allowed.</p>	<p>0.north-america.pool.ntp.org</p> <p>1.north-america.pool.ntp.org</p>

Firewall rules for business

Business networks protect their data and clients using a firewall. Depending on the firewall configuration, certain ports may need to be opened on the firewall to allow the Network Extender to come into service.

The Network Extender communicates to the Verizon Wireless Gateway over an Internet Protocol Security Protocol (IPSEC) encrypted tunnel. The use of Network Address Translation (NAT)/Port Address Translation (PAT) within the network will determine which firewall rules need to be opened.

The Network Extender will also access a DNS Server to obtain the IP Address of Verizon's Security Gateways and may access a DHCP Server for its IP addresses. Since this communication is generally done within the same subnet/network, these settings are not included in the firewall table. If they are required, they use the standard DNS and DHCP ports. DNS-UDP uses port 53. DHCP-BOOTP uses port 67.

The Network Extender enables the IT administrator to deploy the solution in almost any scenario. The embedded web server allows for flexible configurations.

CSG User Configuration

The following information is used to configure Closed Subscriber Group (CSG) mode for the Network Extender.

Note: CSG mode must be configured using the Verizon tools and configuration steps described below. CSG mode cannot be configured through the Network Extender Web GUI.

CSG modes

Open Mode

- Default, out of the box.
- Any VzW UE within vicinity can attach to the Open Network Extender.

Hybrid Mode

- CSG subscribed members have priority over non-members.
- Non CSG subscribed members are allowed service only if resources are not used up by CSG members. Non members can be pre-empted in favor of CSG members.

Closed Mode

- Network Extender resources are exclusively reserved for CSG subscribed MDNs.

Dependencies

- CSG capable mobile phone (2018 or newer Verizon certified phones).
- Verizon post-pay subscriber account.
- Profile-07 or newer SIM card.

Configuration steps

1. To enable and/or manage CSG, the user must login to his/her Verizon account via MyVerizon or MyBiz portal.
2. Create a CSG Group ID.
3. Assign phone numbers to the CSG Group ID. Each phone can be assigned up to 10 CSG Group IDs.
4. Assign the CSG Group ID to the Network Extender. One CSG Group ID can be assigned to one or more Network Extenders.
5. Change CSG mode (Hybrid/Closed) for each Network Extender.

Chapter 5. Troubleshooting

About this chapter

This chapter provides troubleshooting information for the Network Extender 3 including status LEDs and list of alarms.

The following topics are covered in this chapter:

Topic	Page
Status LEDs	5-2
Alarm troubleshooting	5-4

Status LEDs

Figure 5-1 shows the location of the status LEDs for the Network Extender.

Figure 5-1. Network Extender status LEDs

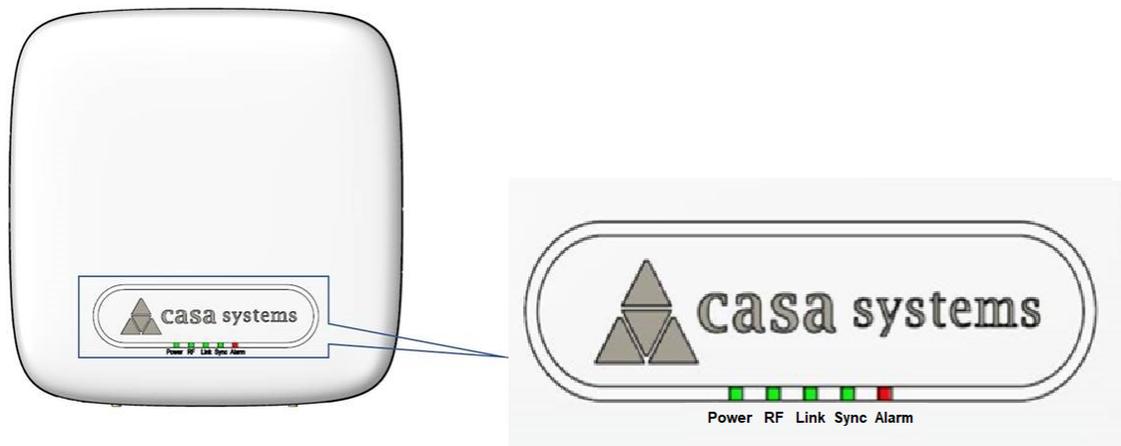


Table 5-1 provides functional details for each status LED applicable for network administrators.

Table 5-1. Status LED functions

LED	Color	Function
Power		OFF: Power not detected.
		ON: All the power rails are present.
		Flashing: Unit booting or firmware upgrading.
RF		OFF: Radio activity disabled, not transmitting and receiving.
		ON: Radio activity enabled, unit transmitting and receiving.

Table 5-1. Status LED functions (continued)

LED	Color	Function
Link		OFF: Ethernet link down.
		ON: Ethernet link up.
Sync		OFF: Synchronization not established with the GPS.
		ON: GPS synchronization complete.
		Flashing: Lost GPS synchronization.
Alarm		OFF: No alarms detected.
		Flashing: System critical alarm.

Alarm troubleshooting

The Web GUI provides a list of active alarms for the Network Extender. Access the list of active alarms from the Web GUI dashboard by clicking **Alarms** (see [Figure 5-2](#)). See [List of Network Extender 3 Alarms](#) for detailed information.

Figure 5-2. Web GUI alarms page

The screenshot displays the 'Alarms' page in the Web GUI. The page title is 'Alarms' and it includes tabs for 'Active Alarms' and 'Alarm History'. A search bar and a 'Generate report' button are located at the top right. The main content is a table of active alarms with the following columns: Raised Time, Event Type, Probable Cause, Specific Problem, Perceived Severity, and More info. Two entries are visible in the table.

Raised Time	Event Type	Probable Cause	Specific Problem	Perceived Severity	More info
3/18/2022, 2:28:49 PM	Equipment	Loss of Synchronization	Synchronization lost with all sources	Major	+
3/18/2022, 2:28:08 PM	Equipment	Antenna Failure	GPS Antenna not connected	Major	+

Showing 1 to 2 of 2 entries

Navigation: First Previous Next Last

List of Network Extender 3 Alarms

Table 5-2 provides recommended troubleshooting steps used to address issues raised by the alarm IDs shown on the active alarms page.

Table 5-2. Alarm troubleshooting

Alarm	Description	Recommendation	Unique Alarm ID (Code)
L3 not detected	LTE L3 software protocol stacks encountered an issue and LTE services are not available, the device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20001
L2 not detected	LTE L2 software protocol stacks encountered an issue and LTE services are not available, the device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20002
Flash memory usage	There is a temporary memory usage alert, but your device is still functioning correctly.	This alert should clear itself.	20004
MME connection is down	The device cannot communicate with Verizon's Network. Please check the LAN/Firewall settings, connectivity status and available bandwidth.	If the problem persists, please contact Verizon Wireless Customer Service.	20005
RRM overload	This alert should clear itself.	If the alert persists for a long time, please check the number of users in the "Connected Devices" tab and see the capacity section of the user guide.	20006
High CPU load	There is a temporary CPU load alert, but your device is still functioning correctly.	This alert should clear itself.	20008
High NACK level	This is related to RF quality issue, there is an excessive retransmission caused by an external source of interference.	Please check the radio environment and Network Extender Placement.	20009
Over-the-air synchronization lost	This is related to RF quality issue.	Please Check for availability of Verizon macro sites signal.	20010

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
GPS synchronization lost	There is an issue with the GPS.	Ensure open view of the sky. Reboot/power cycle the unit. If the issue persists, replace the unit.	20011
Cell synchronization failure	There is an issue with the GPS.	Ensure open view of the sky. LTE service may degrade if the unit operates for long period of time without synchronization.	20012
SCTP Failure	The device cannot communicate with Verizon's Network.	The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20013
Ethernet error	There is an issue with the Ethernet connection.	Power cycle the device to clear the issue. If symptom persists, the unit will need to be replaced.	20014
CPU Temperature Unacceptable	The device is over-heating.	Please locate the unit in an area with an ambient temperature between Operational Temperature range -10°C to 65°C (14°F to 149°F).	20015
PA Temperature Unacceptable	The device is over-heating.	Please locate the unit in an area with an ambient temperature between Operational Temperature range -10°C to 65°C (14°F to 149°F).	20016

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
HTTP failed access	The device cannot communicate with Verizon's Network.	Please check the LAN/ Firewall settings, connectivity status and available bandwidth. If the problem persists, please contact Verizon Wireless Customer Service.	20017
OAM errors	Parameters not set properly.	Verify that all parameters are set per guideline.	20018
RAM memory full	The RAM memory is full.	Power cycle the unit to clear the fault.	20019
Threshold Crossed: RLF	Radio Link Failure.	Caused by high interference of weak signal.	20020
Threshold Crossed: Low SINR	Low SINR.	Check the radio environment and Network Extender Placement.	20021
PA Biasing Failure	PA Biasing Failure.	Power cycle the device to clear the issue. If symptom persists, the unit will need to be replaced.	20022
PCI Collision	A neighboring Cell is operating on the same PCI/Frequency.	The unit will be assigned a different PCI by the Verizon's management system. No action needed.	20023
PCI Confusion	Two or more neighboring Cells are operating on the same PCI/Frequency.	The device is still functioning correctly, the Network Element management system shall resolve this alarm.	20024

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
L1 start timeout	Physical Layer (Layer 1) encountered an issue and LTE services are not available, the device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20026
DSP or PHY Crash	Physical Layer (Layer 1) encountered an issue and LTE services are not available, the device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20027
Cell not synchronized	There is an issue with the GPS. Ensure open view of the sky.	LTE service may degrade if the unit operates for long period of time without synchronization.	20028
Synchronization lost with all sources	There is an issue with the GPS.	Ensure open view of the sky. LTE service may degrade if the unit operates for long period of time without synchronization.	20029
Invalid PHY or RF configuration	Parameters not set properly.	Verify that all parameters are set per guideline.	20030
System information configuration failure	Parameters not set properly.	Verify that all parameters are set per guideline.	20031
Single MME connection is down	The device is still functioning correctly. The device will retry automatically establishing the connection again.	This alert indicates that the device cannot communicate with one of Verizon Network's redundancy systems. If the problem persists, please contact Verizon Wireless Customer Service.	20034
IPsec tunnel down	The device cannot communicate with Verizon's Network.	Please check the LAN/Firewall settings, connectivity status and available bandwidth. If the problem persists, please contact Verizon Wireless Customer Service.	20035

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
IPsec tunnel expiry	The device cannot communicate with Verizon's Network.	<p>Please check the LAN/ Firewall settings, connectivity status and available bandwidth. When the connection is re-established, the device will attempt to create a new tunnel automatically.</p> <p>If the problem persists, please contact Verizon Wireless Customer Service.</p>	20036
IPsec IKE SA expiry	The device cannot communicate with Verizon's Network.	<p>Please check the LAN/ Firewall settings, connectivity status and available bandwidth. When the connection is re-established, the device will attempt to create a new tunnel automatically.</p> <p>If the problem persists, please contact Verizon Wireless Customer Service.</p>	20037
Operator Certificate Expired	The device cannot communicate with Verizon's Network.	<p>Please check the LAN/ Firewall settings, connectivity status and available bandwidth. When the connection is re-established, the device will attempt to download certificate automatically from Verizon's Network.</p> <p>If the problem persists, please contact Verizon Wireless Customer Service.</p>	20038

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Holdover Period Expiration	LTE services are not available.	There is an issue with the GPS. Ensure open view of the sky. Reboot/power cycle the unit. If the issue persists, replace the unit.	20039
Administrative Reboot	This is a notification that the device was rebooted from Verizon's Management System.	No action needed.	20040
Forced Reboot	This is a notification that the device was rebooted from Verizon's Management System.	No action needed.	20041
Max MME connection attempts reached for all MME	The device cannot communicate with Verizon's Network.	The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20042
Reboot Loop	The device detected more than 5 continuous reboots in less than 30 minutes.	If the problem persists, please contact Verizon Wireless Customer Service.	20043
DNS Resolution Failure	The device cannot communicate with Verizon's Network.	Please check the LAN/Firewall settings and Review DNS server configuration, connectivity status and available bandwidth. If the problem persists, please contact Verizon Wireless Customer Service.	20044
TR069 Agent not detected	The device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20045
Watchdog not detected	The device shall resume normal operation after self-healing.	If the alert persists, please restart your device.	20046

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Critical configuration failure	Parameters not set properly.	Verify that all parameters are set per guideline.	20047
CMS server connection failure	The device cannot communicate with Verizon's Network.	Please check the LAN/ Firewall settings, connectivity status and available bandwidth. The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20049
AeMS connection no response	The device cannot communicate with Verizon's Network.	Please check the LAN/ Firewall settings, connectivity status and available bandwidth. The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20050
Low DC Power	PoE source is delivering up to class 4.	Verify PoE device supports class 5 and has sufficient power to feed the LTE Network extender device. Verify Ethernet cabling. If possible, change to a different switch port and wall patch panel socket.	20051

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Power Out of Range	PoE source is delivering up to class 3.	Verify PoE device supports class 5 and has sufficient power to feed the LTE Network extender device. Verify Ethernet cabling. If possible, change to a different switch port and wall patch panel socket.	20052
RX RACH Overload	A mobile phone is saturating the (RACH) channel.	Power cycle the device to clear the issue. If symptom persists, please contact Verizon Wireless Customer Service.	20053
RX PUCCH Overload	A mobile phone is saturating the (PUCCH) channel.	Power cycle the device to clear the issue. If symptom persists, please contact Verizon Wireless Customer Service.	20054
RX PUSCH Overload	A mobile phone is saturating the (PUSCH) channel.	Power cycle the device to clear the issue. If symptom persists, please contact Verizon Wireless Customer Service.	20055
GPS Antenna not connected	There is an issue with the GPS connector/ Antenna.	Ensure open view of the sky. Reboot/power cycle the unit. If the issue persists, replace the GPS Antenna.	20056

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Tampering detection	Unit cover has been removed.	This alarm is triggered when the cover of the unit is removed. Visually inspect the unit and contact Verizon Wireless Customer Service if the cover is not removed or damaged .	20057
Abnormal RSSI level	The received signal strength indicator (RSSI) level is below a threshold.	This is a warning that a poor radio signal strength is measured, but the device is still functioning correctly. No action is needed.	20058
IQ power out of range	Detected IQ power higher than a threshold in the transmission path.	The detected output power of the device is higher than the configured value. Reboot the device and if the problem persists contact Verizon Wireless Customer Service.	20059
RSI Collision	RSI conflict detected in the LTE network.	This alarm is triggered when an RSI conflict is detected by the device. No action is needed because SON automatically reconfigures the device with new, non-overlapping RSI.	20060
High Neighbor Interference	Radio interference detected from neighboring cells.	Use the manual band selection on the Web GUI to assign a different frequency to the Network Extender device. Navigate to advanced setting to change the Network Extender configuration.	20061

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Not Signed Upgrade Package	Software upgrade failed due to wrong non-signed upgrade file.	<p>An upgrade using wrong non-signed file has been attempted.</p> <p>No action is needed; the upgrade is rejected by the device.</p>	20062
Integrity Check Failure	Software upgrade failed due to corrupted file.	<p>An upgrade using corrupted file has been attempted. No action is needed; the upgrade is rejected by the device. Upgrade should be reattempted to discard file corruption during transfer.</p> <p>If upgrade fails again, please contact Verizon Wireless Customer Service.</p>	20063
Unable to get IP from DHCP	The unit failed to acquire a local IP address from the local DHCP server.	Verify the configuration of the LAN router and reboot if necessary to assign a valid IP to the device.	20064
Unable to get operator certificate from CMS server	The device cannot retrieve the operational Certificates from Verizon's Network.	<p>Please check the LAN/ Firewall settings, connectivity status and available bandwidth. The device will reboot automatically and try establishing the connection again.</p> <p>If the problem persists, please contact Verizon Wireless Customer Service.</p>	20065
Clock synchronization problem	There is an issue with the GPS.	Ensure open view of the sky. LTE service may degrade if the unit operates for long period of time without synchronization.	20066

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Operator certificate expired	The device cannot communicate with Verizon's Network.	Please contact Verizon Wireless Customer Service.	20067
Operator certificate within renewal expiration window	The device detected the operator certificate is about to expire (validity under one month)	No action is needed. Unit will download new certificate from Verizon's Network.	20068
CMS server connection failure on certificate renewal	The device cannot communicate with Verizon's Network.	Please check the LAN/Firewall settings, connectivity status and available bandwidth. The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20069
CMS server authentication failure on certificate renewal	The device cannot communicate with Verizon's Network.	Please check the LAN/Firewall settings, connectivity status and available bandwidth. The device will reboot automatically and try establishing the connection again. If the problem persists, please contact Verizon Wireless Customer Service.	20070
OAM Proxy not detected	The OAM component used to interface the different protocol stack applications has crashed.	The unit is not manageable, its operation will be degraded and shall be rebooted.	20071
Operator certificate Issuer is not accepted by SeGW	The device cannot communicate with Verizon's Network.	Please contact Verizon Wireless Customer Service.	20072

Table 5-2. Alarm troubleshooting (continued)

Alarm	Description	Recommendation	Unique Alarm ID (Code)
Connection failure for all NTP servers	The device cannot communicate with any of the configured NTP servers.	Please check the LAN/ Firewall settings, connectivity status and available bandwidth. The device will operate correctly if GPS signal is valid.	20073
GPS Antenna not connected on boot	There is an issue with the GPS connector/ Antenna.	Ensure open view of the sky. Reboot/power cycle the unit. If the issue persists, replace the GPS Antenna.	20074

Chapter 6. Specifications

Key Specifications

Table 6-1. Key specifications

Item	Details
Frequency Bands	Band 4, 13, and 66 Selectable (1 carrier), B46 (LAA)
Carriers	1 LTE Carrier + 1 LAA Carrier
BW Channelization - Licensed	5, 10, 15, 20 MHz
LAA Channel	20 MHz
Maximum Modulation	64 QAM
Max TX Power - Licensed	24 dBm (2 streams @ 21 dBm) per LTE carrier
Max 1X Power - 1 AA	27 dBm (2 streams @24 dBm) for each LAA port
Antenna Configuration	2 MIMO DL, UL Rx diversity (2 Tx/2 Rx) per LTE carrier
RF Ports - Internal	4 internal RF ports, 1 GPS port
RF Ports - External	2 licensed RF ports exposed to support DAS solutions
Backhaul Interface	10/100/1000 Gigabit Ethernet, RJ-45
LMT Interface	10/100/1000 Gigabit Ethernet, RJ-45
Logical Interfaces	LTE: S1-U, S1-MME, X2
Synchronization	GPS or IEEE 1588v2
GPS constellation	GPS (USA), SBAS (USA)
Maximum connected users	64

Table 6-1. Key specifications (continued)

Item	Details
Security protocol	IPSEC: AES, 3DES
Key Management	PKI: IKEv2 key management, certificate based authentication with secure boot.

Physical and Environmental Information

Table 6-2. Physical and Environmental Information

Item	Details
Dimensions	240 mm x 240 mm x 65 mm
Weight	<2200 Grams
Nominal Power Consumption	<25W at full capacity with licensed bands, < 29W with LAA
Power	12 VDC power supply @ 220 VAC
PoE	<ul style="list-style-type: none">• PoE+ 802.3at Class 4 with licensed bands only• PoE++ 802.3bt Class 5 when LAA is enabled
Operational Temperature	-10°C to 65°C (14°F to 149°F)
Humidity	5% to 95% Relative Humidity - non condensing
Protection	IP50

Supported Services

Table 6-3. Supported Services

Item	Details
Supported Services	<p>Supported services include:</p> <p>SON: Hybrid SON support with dSON and cSON; dSON agent can work with or without cSON and supports using a real-time interface through X2 or TR-069; SON macro integration supported through X2-GW, X2-Proxy or direct connection.</p> <hr/> <p>TR-069: TR-069 agent supports TR-196v2 and TR-181 data models.</p> <hr/> <p>CSG:</p> <p><u>Open Mode</u> (Default, out of the box): Any VzW UE within vicinity can attach to the Open Femto Cell.</p> <p><u>Hybrid Mode:</u> - CSG subscribed members have priority over non-members. - Non CSG subscribed members are allowed service only if resources are not used up by CSG members. Nonmembers can be pre-empted in favor of CSG members.</p> <p><u>Closed Mode:</u> Network Extender resources are exclusively reserved for CSG subscribed MDNs.</p>

Appendix A. FAQs

About this appendix

This Appendix provides the following Frequently Asked Questions (FAQs) for the Network Extender.

Topic	Page
Dashboard FAQs	A-3
How to verify the device operation mode	A-3
System Information FAQs	A-4
How to verify if the GPS location was acquired	A-4
How to check the number of connected users	A-5
How to check the active alarms and generate an alarm report	A-6
Settings FAQs	A-7
How to adjust MTU (maximum transfer unit) size	A-7
How to configure a static IP address	A-8
How to add a DNS	A-9
How to add a search domain	A-10
How to manually adjust the device transmission power	A-11
How to change the device operating channel	A-12
How to configure Network Extender Operation Mode	A-13
How to configure Synchronization Source	A-14
How to add a VLAN	A-15
How to set the power source	A-18
How to configure Network Extender Backhaul Limit	A-19
How to reboot or factory reset a device	A-20
CSG mode FAQs	A-21
Where can the user manage the CSG function?	A-21

Topic	Page
Will the user be able to determine which CSG IDs are associated with the phone?	A-21
Can the user specify a particular CSG ID number?	A-21
How many CSG ID can be assigned to a Network Extender?	A-21
Will the CSG ID be changed if a Network Extender changed its CSG mode from Hybrid to Closed or vice versa?	A-21
Will different CSG mode impacts E911 calls?	A-21

Dashboard FAQs

How to verify the device operation mode

1. From the main Dashboard, click **Dashboard** (see [Figure A-1](#)).
2. Under System Information Dashboard, verify the **Operation Mode** of the Network Extender (selections include: Open, Hybrid, or Close).

Figure A-1. Operation Mode

The screenshot displays the dashboard interface. On the left, a sidebar menu lists various sections: DASHBOARD, SYSTEM INFORMATION, SETTINGS, and ABOUT. The 'Dashboard' option is highlighted with a red arrow and labeled 'Step 1'. The main content area shows the 'System Information Dashboard' with a table of system details. The 'Operational Status' is 'OUT OF SERVICE' and the 'Operation Mode' is 'OPEN', which is highlighted with a blue box and labeled 'Step 2'. An image of a white network extender device is shown to the right of the sidebar.

System Information Dashboard		Software Version	4.12.1
Operational Status	OUT OF SERVICE	Location	42.6919° N, 71.2032° W
Operation Mode	OPEN	Uptime	14 Days 2 Hours 30 Minutes 23 Seconds
IP Address	192.168.61.41	System Time	2/2/2022, 9:37:12 PM (UTC)
MAC Address	00:17:10:29:4E:B6		

System Information FAQs

How to verify if the GPS location was acquired

1. From the main Dashboard, click **System Information** > **Operational Status** (see [Figure A-2](#)).
2. On the upper right corner of the page, click **Operational Status**.
3. Under Device Operational Status, check the **GPS Location** (Location Acquired shown).

Figure A-2. GPS Location

The screenshot shows the 'Operational Status' page in the eFemto dashboard. The page is titled 'Operational Status' and has a breadcrumb trail 'SYSTEM INFORMATION / OPERATIONAL STATUS'. The page is divided into two main sections: 'Device Operational Status' and '4G Service Operational Status'. The 'Device Operational Status' section is further divided into 'Step 1' and 'Step 3'. 'Step 1' includes Power Source (PSU), Ethernet Link (UP), and IP Address (DHCP 192.168.61.41). 'Step 3' includes GPS Location (Location Acquired), DNS (Configured), and IPsec (Not Established). The '4G Service Operational Status' section includes S1 Link (NOT SETUP), Current Status (OUT OF SERVICE), HeMS (Connected), and Last refresh (2/2/2022, 4:43:39 PM). The 'Operational Status' link in the top right corner is highlighted with a blue box and labeled as 'Step 2'.

Section	Item	Status
Device Operational Status	Power Source	PSU
	Ethernet Link	UP
	IP Address	DHCP 192.168.61.41
Device Operational Status (Step 3)	GPS Location	Location Acquired
	DNS	Configured
	IPsec	Not Established
4G Service Operational Status	S1 Link	NOT SETUP
	Current Status	OUT OF SERVICE
	HeMS	Connected
	Last refresh	2/2/2022, 4:43:39 PM

How to check the number of connected users

1. The number of active users is displayed in the Web GUI header.
2. From the main Dashboard, click **System Information** > **Connected Devices** (see [Figure A-3](#)).
3. Under Connected Devices, the active UEs are displayed.

Figure A-3. Connected Devices

The screenshot shows the Verizon Web GUI interface. At the top, the header displays '0 Users' in a blue box, with a red arrow labeled 'Step 1' pointing to it. The left sidebar contains a menu with 'Connected Devices' highlighted, and a red arrow labeled 'Step 2' points to it. The main content area is titled 'Connected Devices' and features a table with the following columns: 'UE', 'CSG Membership', 'DL Traffic (kbps)', and 'UL Traffic (kbps)'. A red arrow labeled 'Step 3' points to the table, which contains the text 'There are no active UEs in the system'. Below the table, there are four summary statistics: 'Total DL traffic Mbps' (0), 'Total UL traffic Mbps' (0), 'Max number of CSG users During the last 8 hours' (0), and 'Max number of Non-CSG users' (0).

How to check the active alarms and generate an alarm report

1. From the main Dashboard, click **System Information > Alarms** (see [Figure A-4](#)).
2. On the upper right portion of the page, click **Active Alarms** to display a list of active alarms.
3. Click **Generate report** to generate an alarm report.

Figure A-4. Network Extender Alarms

The screenshot shows the 'Alarms' page in the Network Extender interface. The left sidebar contains navigation options: DASHBOARD (eFento Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), and SETTINGS (Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device). The main content area is titled 'SYSTEM INFORMATION / ALARMS' and 'Alarms'. It features a search bar (Step 1) and two tabs: 'Active Alarms' (Step 2) and 'Alarm History'. Below the tabs is a table of active alarms with columns: Raised Time, Event Type, Probable Cause, Specific Problem, Perceived Severity, and More info. A single entry is shown for 'Processing Error' on 1/19/2022 at 2:13:19 PM, with a 'Critical' severity. A 'Generate report' button (Step 3) is located at the bottom right of the table.

Raised Time	Event Type	Probable Cause	Specific Problem	Perceived Severity	More info
1/19/2022, 2:13:19 PM	Processing Error	Configuration or Customization Error	Critical configuration failure	Critical	+

Showing 1 to 1 of 1 entries

First Previous Next Last

Settings FAQs

How to adjust MTU (maximum transfer unit) size

1. From the main Dashboard, click **Settings > Network Settings** (see [Figure A-5](#)).
2. Under Ethernets, select the interface.
3. Click MTU and change the setting as needed.

Figure A-5. Network Settings

SETTINGS / NETWORK SETTINGS

Network Settings

IP Addresses

Interface	Mode	Family	IP Address	Prefix
SERVING-SEGW	IPsec	--	--	--
WAN	DHCP	IPv4	192.168.61.41	24
LMT	Diagnostics	IPv4	172.31.11	30

Ethernets

Interface	MAC Address	MTU
WAN	00:17:10:29:4E:B6	1500
LMT	00:27:10:29:4E:B9	1500

DNS

Search Domains

How to configure a static IP address

1. From the main Dashboard, click **Settings > Network Settings** (see [Figure A-6](#)).
2. Under IP Addresses, select the IP Address that requires the change.
3. On the **Configure WAN IP Address** page, under Mode, select either **DHCP** or **Static**.
4. Click **Confirm action**.

Figure A-6. Static IP address

The screenshot shows the Verizon eFemto Dashboard with the following components:

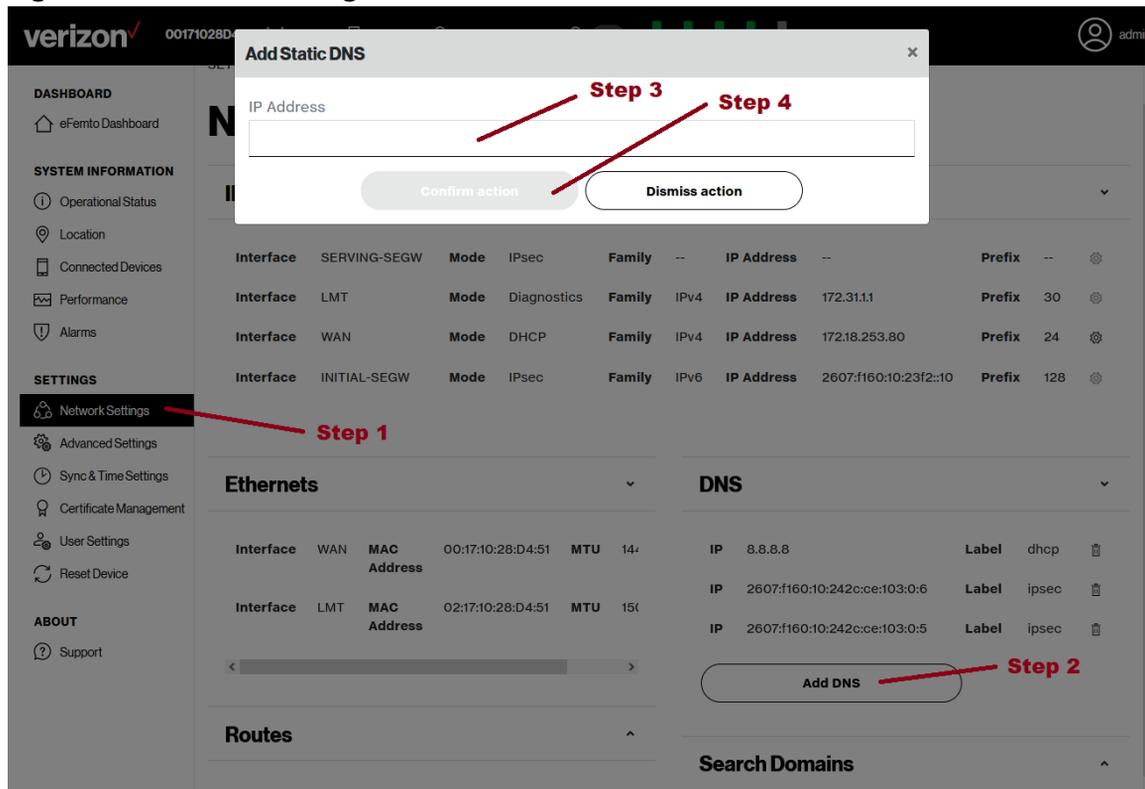
- Dashboard Header:** Verizon logo, VERIZON-4EB0, No Service.
- Left Sidebar (SETTINGS):** Network Settings (Step 1), Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device.
- Main Content Area:** Network Settings / NETWORK SETTINGS, Network Settings, IP Addresses table, Ethernets, Routes, DNS, Search Domains.
- IP Addresses Table:**

Interface	SERVING-SEGW	Mode	IPsec	Family	--	IP Address	Prefix	
Interface	WAN	Mode	DHCP	Family	IPv4	IP Address	192.168.61.41	Prefix
Interface	LMT	Mode	Diagnostics	Family	IPv4	IP Address	172.31.1.1	Prefix
- Configure WAN IP Address Dialog Box:**
 - Mode dropdown menu (Step 3) with options: DHCP, Static.
 - Family dropdown menu (Step 4) with option: IPv4.
 - Buttons: Confirm action, Dismiss action.

How to add a DNS

1. From the main Dashboard, click **Settings** > **Network Settings** (see [Figure A-7](#)).
2. Under DNS, click **Add DNS**.
3. On the **Add Static DNS** page, enter the DNS IP Address.
4. Click **Confirm action**.

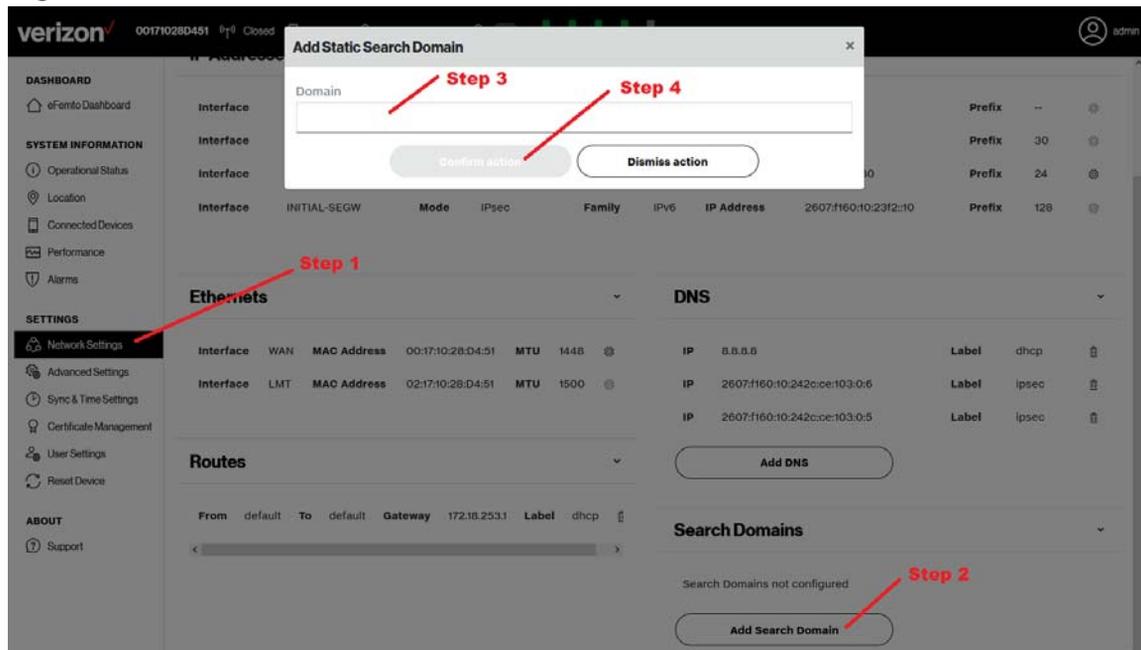
Figure A-7. DNS settings



How to add a search domain

1. From the main Dashboard, click **Settings > Network Settings** (see [Figure A-8](#)).
2. Under Search Domains, click **Add Search Domain**.
3. On the **Add Static Search Domain** page, enter the Domain Address.
4. Click **Confirm action**.

Figure A-8. Search domains



How to manually adjust the device transmission power

1. From the main Dashboard, click **Settings** > **Advanced Settings** (see [Figure A-9](#)).
2. On the upper right corner of the Advanced Settings page, select **PCell Configuration**.
3. Under Transmission Power Configuration, select **Enable Manual Power Selection**.
4. Click **Tx Power**.

Figure A-9. Advanced Settings

The screenshot shows the 'Advanced Settings' page with a left sidebar and a main content area. The sidebar includes sections for Dashboard, System Information, Settings, and About. The 'Settings' section is expanded, and 'Advanced Settings' is selected, marked with a red arrow and 'Step 1'. The main content area is titled 'Advanced Settings' and has two tabs: 'eNB configuration' (Step 2) and 'PCell configuration' (highlighted with a red box). Under 'PCell configuration', there is a table for 'Primary Cell Radio Configuration' and a 'Transmission Power Configuration' section. The 'Transmission Power Configuration' section shows 'Tx Power' at 24 dBm and a toggle for 'Enable Manual Power Selection' (Step 3) which is turned on. Below this is a slider for 'Tx Power' ranging from 0 dBm to 24 dBm (Recommended Tx Power), with a 'Set Tx Power' button (Step 4) highlighted in a red box. A summary box on the right shows 'Tx Power 24 dBm 251 mW'.

Parameter	Value	Parameter	Value
Primary PLMNID	311480	Cell ID	264193025
PCI	498	TAC	244
Operating Band	Band 13	EARFCN	5230
DL Bandwidth	10 MHz	UL Bandwidth	10 MHz
Reference Signal Power	-7	RF Tx Status	Off
Cell Barred	False	Administrative State	True

How to change the device operating channel

1. From the main Dashboard, click **Settings > Advanced Settings** (see [Figure A-10](#)).
2. On the upper right side of the page, click **eNB configuration**, and select **PCell configuration**.
3. On the Primary Cell Radio Configuration page, select the **operating channel** from the drop down menu.

Figure A-10. PCell configuration

The screenshot shows the Verizon eFemto Advanced Settings interface. The left sidebar contains a menu with 'Advanced Settings' highlighted and a red arrow pointing to it, labeled 'Step 1'. The main content area is titled 'Primary Cell Radio Configuration' and contains a warning message: 'The configuration of a new operating channel will force the reboot of your 4G LTE Network Extender. After the system reboot, the eFemto will operate in the selected channel.' Below the warning is a dropdown menu labeled 'Select operating channel...' with 'Step 3' next to it. The dropdown menu is open, showing two options: 'Band 13 - EARFCN 5230 - 10 MHz Bandwidth' and 'Band 4 - EARFCN 2050 - 20 MHz Bandwidth'. The background interface shows the 'PCell configuration' tab selected, with a red 'Step 2' label above it. The background also shows a table of configuration parameters:

Parameter	Value	Parameter	Value
Primary PLMNID		TAC	244
PCI	498	EARFCN	5230
Operating Band	Band 13	UL Bandwidth	10 MHz
DL Bandwidth	10 MHz	RF Tx Status	Off
Reference Signal Power	-7	Administrative State	True
Cell Barred	False		

Below the table is the 'Transmission Power Configuration' section, which includes 'Tx Power' set to 24 dBm and an 'Enable Manual Power Selection' toggle switch.

How to configure Network Extender Operation Mode

1. From the main Dashboard, click **Settings > Advanced Settings** (see [Figure A-11](#)).
2. On the Advanced Settings page, under ENB Configuration, click the settings icon (see [Figure A-11](#)).
3. On the Operation Mode Configuration dialog, select an operation mode (Single Carrier, CAT-M1, or LAA) (see [Figure A-12](#)).
4. Click **Confirm action** (see [Figure A-12](#)).

Figure A-11. Advanced settings

Advanced Settings

ENB Configuration

eNB Name	00171028D451	eNB ID	264318572
CSG ID	16777219	Access Mode	Hybrid
Operation Mode	LAA	VoLTE Emergency Calls	True

Neighbour Cells

Cell ID	PCI	EARFCN	eNB ID
264318554	487	5230	264318554
264318570	477	5230	264318570
264318615	485	5230	264318615

Figure A-12. Operation Mode dialog

Operation Mode Configuration

Configure the operation mode of your 4G LTE Network Extender.

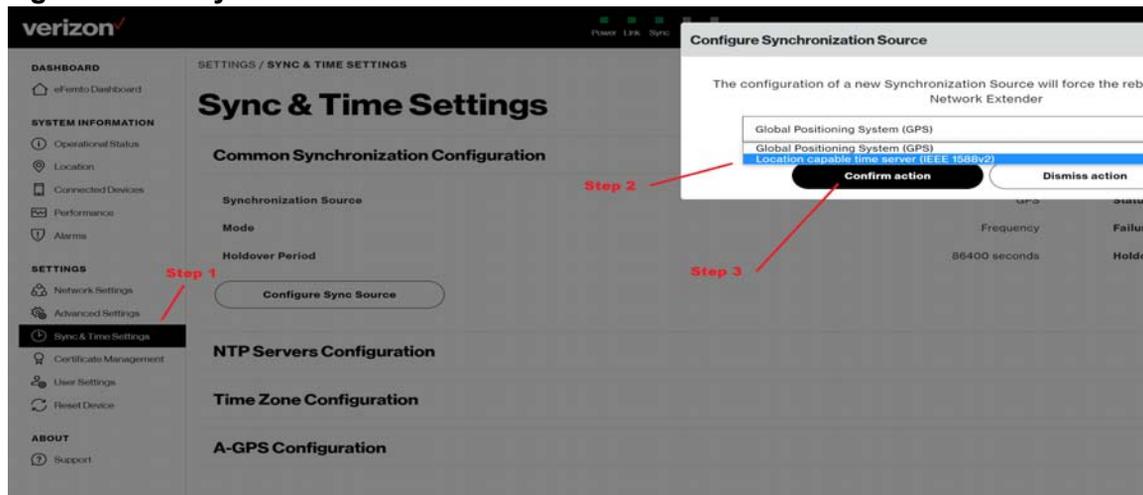
LAA

Confirm action **Dismiss action**

How to configure Synchronization Source

1. From the main Dashboard, click **Settings** > **Sync & Time Settings** (see [Figure A-13](#)).
2. On the Configure Synchronization Source dialog, select the synchronization source.
3. Click **Confirm action**.

Figure A-13. Synchronization Source

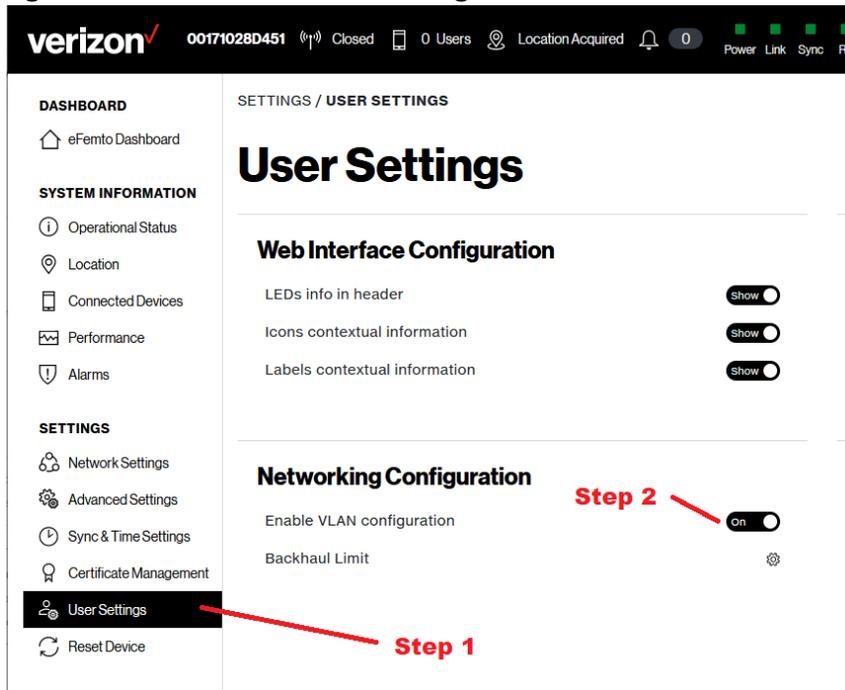


How to add a VLAN

The Web GUI provides the ability to configure a VLAN for the Network Extender.

1. From the main Dashboard, click **Settings > User Settings** (see [Figure A-14](#)).
2. Click **Enable VLAN configuration** (see [Figure A-14](#)).

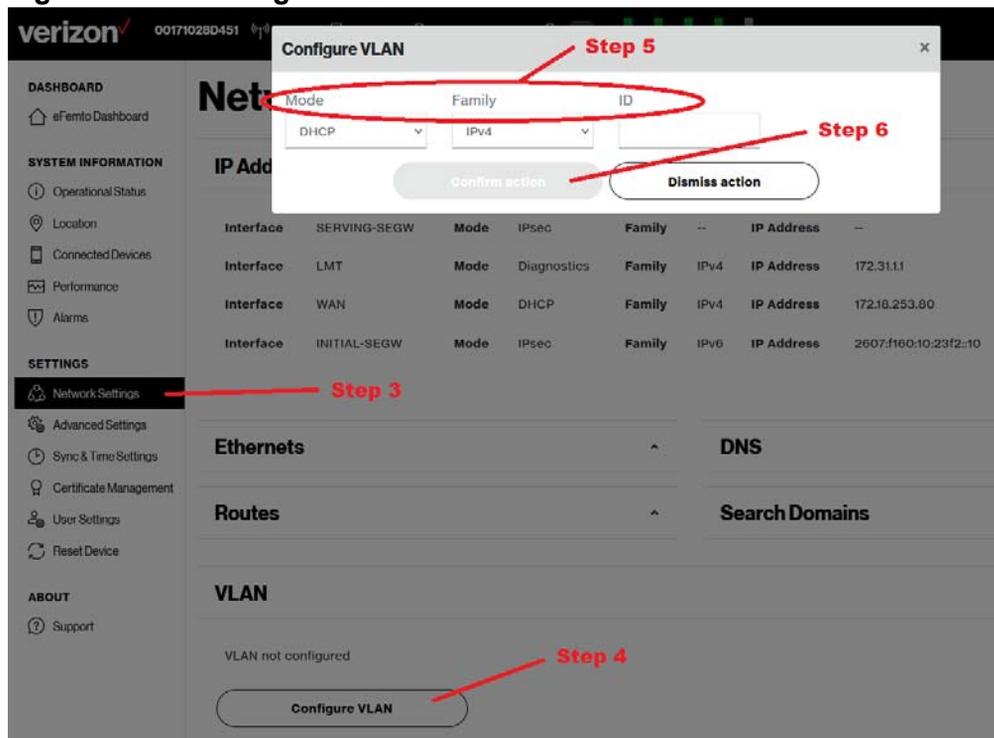
Figure A-14. Enable VLAN Configuration



3. Click **Network Settings** (see [Figure A-15](#)).
 4. Click **VLAN > Configure VLAN** (see [Figure A-15](#)).
 5. On the Configure VLAN dialog, set **Mode** (DHCP or Static), **Family**, and **ID**. This action will reboot the unit (see [Figure A-15](#)).
- If using DHCP, check that the unit can get IP address after reboot.
 - If not using DHCP, try to ping the unit static WAN IP from another device in the same VLAN.

- Click **Confirm action** (see [Figure A-15](#)).

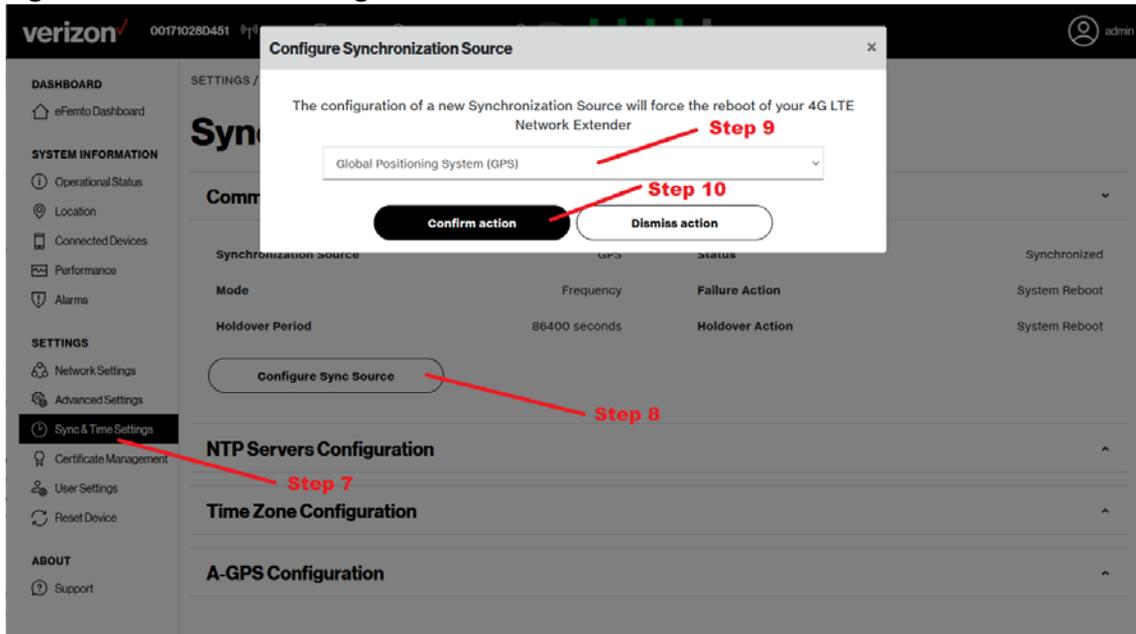
Figure A-15. Configure VLAN



- Under Settings, click **Sync & Time Settings** (see [Figure A-16](#)).
- Click **Configure Sync Source** (see [Figure A-16](#)).
- On the Configure Synchronization Source dialog, set the ePTP server IP address (see [Figure A-16](#)). This action will reboot the unit again.

10. Click **Confirm** action (see [Figure A-16](#)).

Figure A-16. VLAN Configuration



If the Network Extender cannot get a location, it is probably because the ePTP server is unreachable. Ping the Network Extender from a device in the same subnetwork used by the ePTP server.

How to set the power source

The Network Extender provides the ability to select the Network Extender power source to either PoE (Power Over Ethernet) or the AC power adapter.

1. From the main Dashboard, click **Settings** > **User Settings** (see [Figure A-17](#)).
2. Under Power Source Configuration, select **Off** to select PoE (power is provided via the Ethernet port), or **On** to select the AC power source.

Figure A-17. Power Source Configuration

The screenshot displays the 'User Settings' page. The left sidebar contains a navigation menu with sections: DASHBOARD (eFemto Dashboard), SYSTEM INFORMATION (Operational Status, Location, Connected Devices, Performance, Alarms), and SETTINGS (Network Settings, Advanced Settings, Sync & Time Settings, Certificate Management, User Settings, Reset Device). The 'User Settings' option is highlighted with a red arrow and labeled 'Step 1'. The main content area is titled 'User Settings' and includes three configuration sections: 'Web Interface Configuration' (with 'show' toggles for LEDs info, icons, and labels), 'Networking Configuration' (with an 'OFF' toggle for 'Enable VLAN configuration'), and 'Power Source Configuration' (with an 'OFF' toggle for 'Set Power Supply as active source'). The 'Power Source Configuration' section is enclosed in a blue box with a red arrow pointing to the 'OFF' toggle, labeled 'Step 2'.

How to configure Network Extender Backhaul Limit

1. From the main Dashboard, click **Settings > User Settings** (see [Figure A-18](#)).
2. On the User Settings page, click the settings icon for **Backhaul Limit** (see [Figure A-18](#)).
3. On the Backhaul Limit dialog, enter the desired limit (in Mbps) (see [Figure A-19](#)).
4. Click **Confirm action** (see [Figure A-19](#)).

Figure A-18. Setting the Backhaul Limit

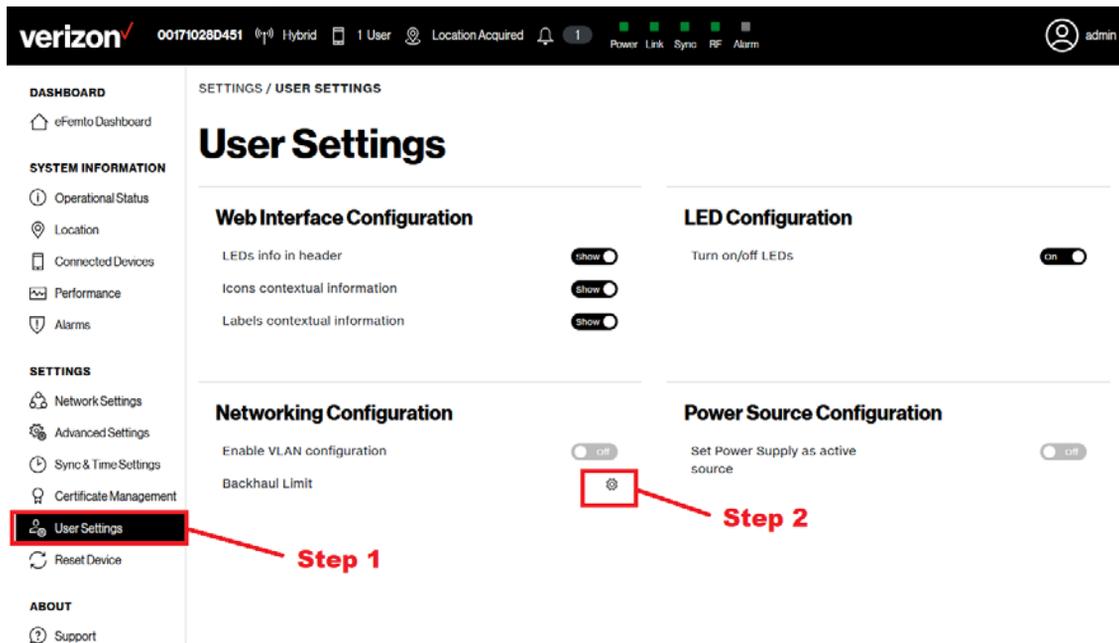
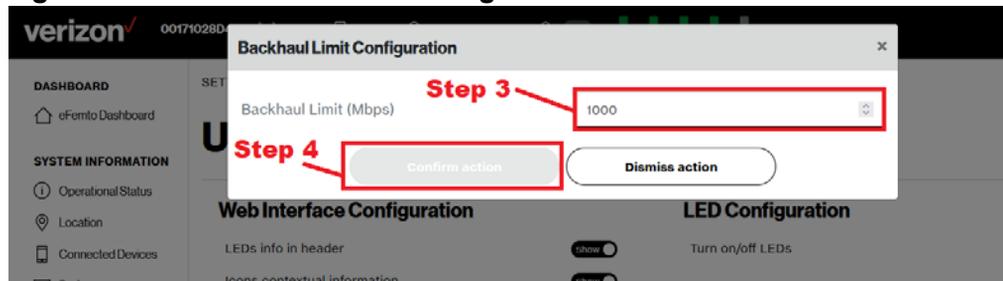


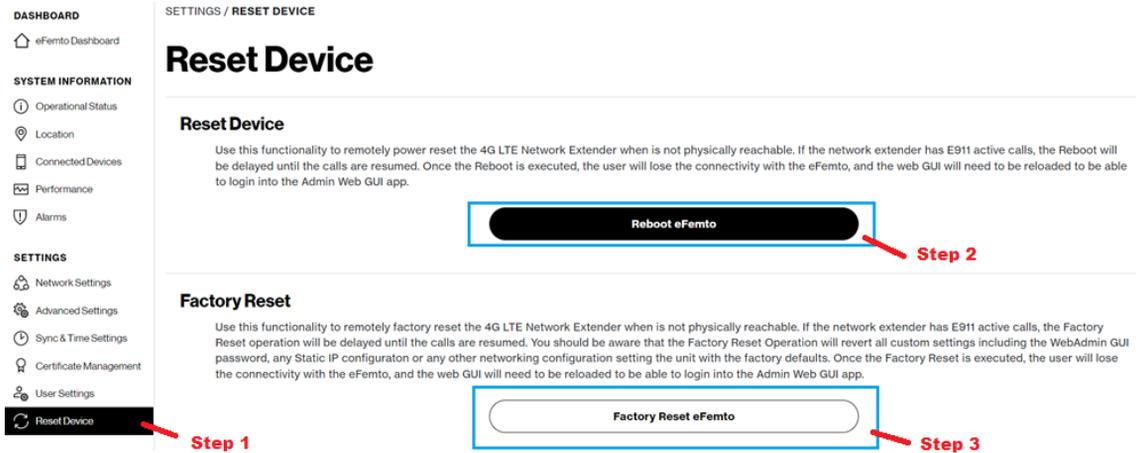
Figure A-19. Backhaul Limit dialog



How to reboot or factory reset a device

1. From the main Dashboard, click **Settings** > **Reset Device** (see [Figure A-20](#)).
2. To reset the Network Extender, on the Reset Device page, click **Reboot eFemto**.
3. To reset the Network Extender to Factory Settings, on the Reset Device page, click **Factory Reset eFemto**.

Figure A-20. Reset device



CSG mode FAQs

Where can the user manage the CSG function?

User will be able to manage the CSG function of the Network Extender via MyVerizon or MyBiz portal.

Will the user be able to determine which CSG IDs are associated with the phone?

User will have to login to the MyVerizon or MyBiz portal to view/manage the phone numbers associate with CSG IDs. There is no way to determine the assigned CSG IDs from the phone.

Can the user specify a particular CSG ID number?

No. The system assigns a CSG ID. However, the user can specify the name of the CSG group.

How many CSG ID can be assigned to a Network Extender?

Only one CSG ID per Network Extender. However, the Network Extender can be re-assigned a different CSG ID if necessary.

Will the CSG ID be changed if a Network Extender changed its CSG mode from Hybrid to Closed or vise versa?

No. The Network Extender keeps the same CSG group and ID but only change the mode.

Will different CSG mode impacts E911 calls?

No. Emergency E911 calls are supported regardless of CSG membership. Emergency active calls on the Network Extender CANNOT be pre-empted nor redirected.



casa systems

100 Old River Road
Andover, MA 01810
USA

Verizon 4G LTE Network Extender 3 for Enterprise User Guide

© 2023 Casa Systems, Inc.

All rights reserved.

DOC-3698-01

Document Revision 8.1b
March 2023

Printed in United States of America