casa systems

Verizon 4G LTE Network Extender 3 for Enterprise

User Guide

DOC-3198-01
Document Revision 3.1.0
October 2021

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

Chapter 1. Getting Started

Chapter 2. Installation

Chapter 3. Web GUI

Chapter 4. Configuration

Chapter 5. Troubleshooting

Chapter 6. Specifications

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.

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 1.0.0 — April 2021; initial version, R4.9.24.1
- Revision 2.0.0 — May 2021; revised version, R4.9.29
- Revision 3.0.0 — September 2021; initial version, R4.10.8
- Revision 3.1.0 — October 2021; revised version, R4.10.8

Corporate facility

Casa Systems, Inc.
100 Old River Road
Andover, MA 01810
Tel.: 978-688-6706
World Wide Web: www.casa-systems.com

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 Casa customers.

Contact Casa Technical Support or a Casa Sales Representative for assistance with downloading selected Casa documentation PDFs.

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

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

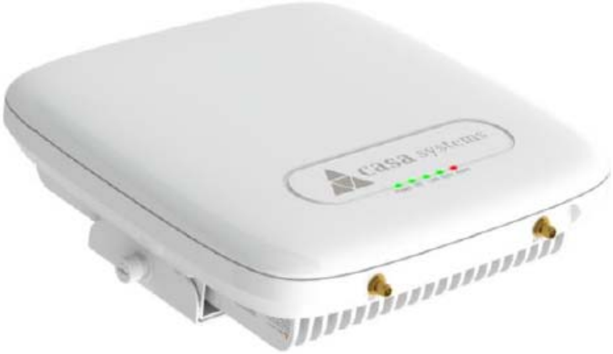
This chapter provides Getting Started information for the Network Extender 3.

The following topics are covered in this chapter:

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 Server Addresses and Firewall Rules in Chapter 4, Configuration.
- 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.

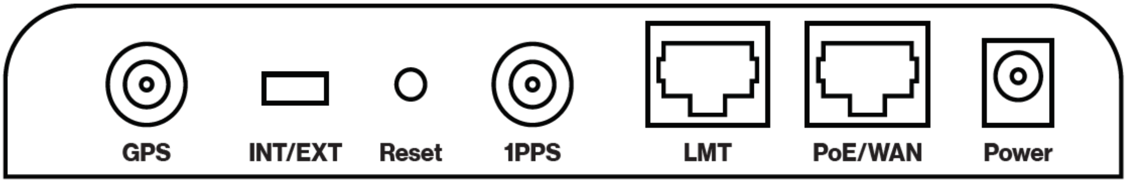
  Casa recommends that Full auto-negotiation be enabled. If the Network Extender does not come into service as either 100/Full or 1000/Full, the recommendation is to configure statically as either 1000/Full (if capable) or 100/Full.

  Note: If 100/Full is used, the Network Extender can go into service, but throughput will be limited.
- In the event that firewall changes are needed, please attempt to make these changes before calling into Customer Care. For more clarity on firewall settings, please see Chapter 4, Configuration.

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 2-20) for important information on the proper use of the INT/EXT switch.
Reset	Factory Reset.
1PPS	To connect 1PPS clock source (Iridium receiver or GPS receiver) and receive 1PPS signal.
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

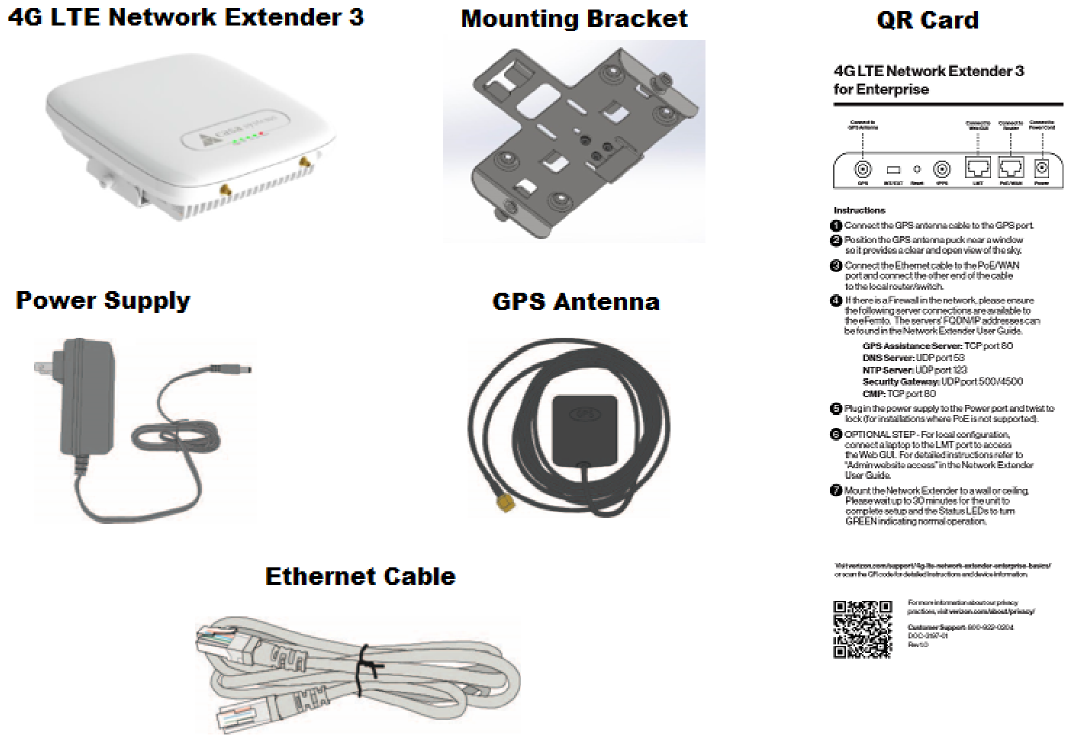
About this chapter

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

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

Power Supply

GPS Antenna

Ethernet Cable

4G LTE 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 servers' 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 GUI. 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 verizon.com/support/4g-lte-network-extender-enterprise-basics/ or scan the QR code for detailed instructions and device information.

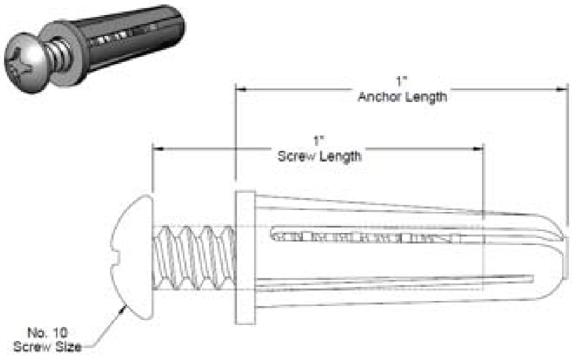
For more information about our privacy practices, visit verizon.com/about/privacy/

Customer Support: 800-922-0204
DOC-3197-01
Rev 5.0

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)

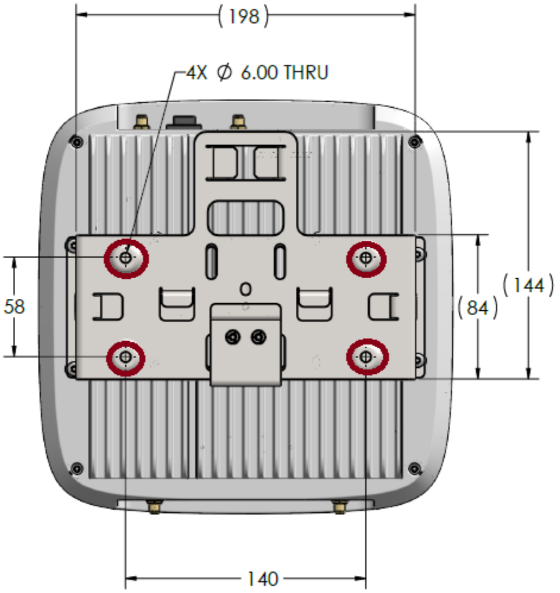


Installing the wall bracket

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

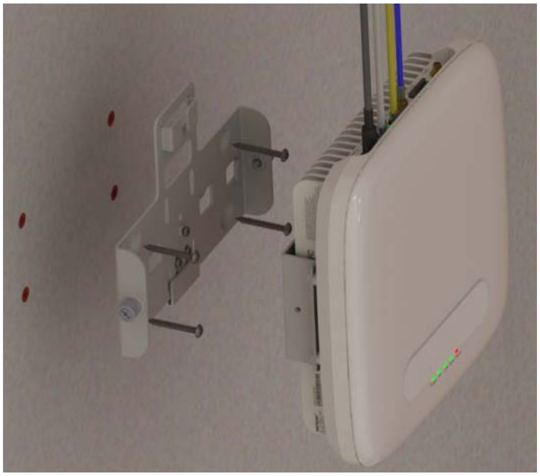


When anchoring on a wall, ensure the positions are marked as horizontal or vertical, as only a limited range of tuning is allowed for leveling after the system is mounted.

Securing the mounting bracket to the wall

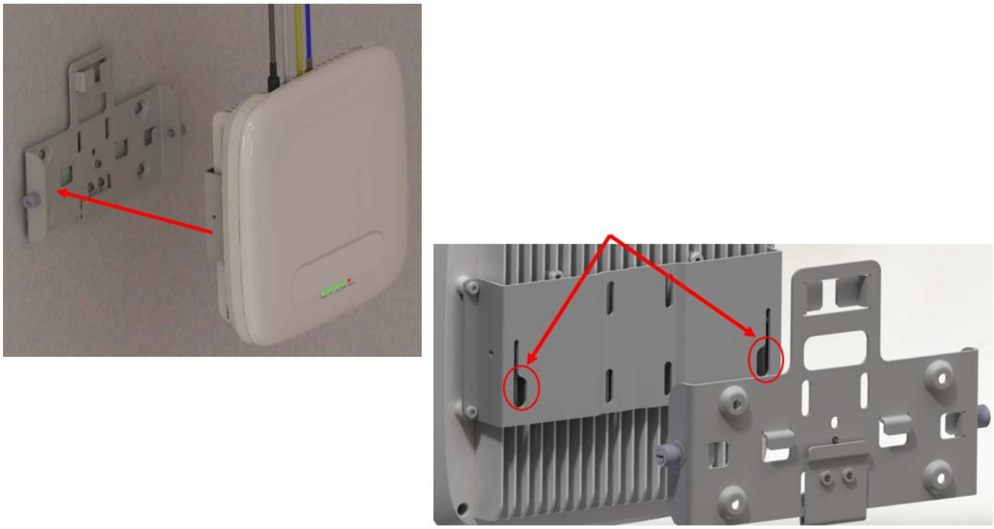
1. Attach the upper bracket to the wall/ceiling (see Figure 2-4).

Figure 2-4. Attach bracket



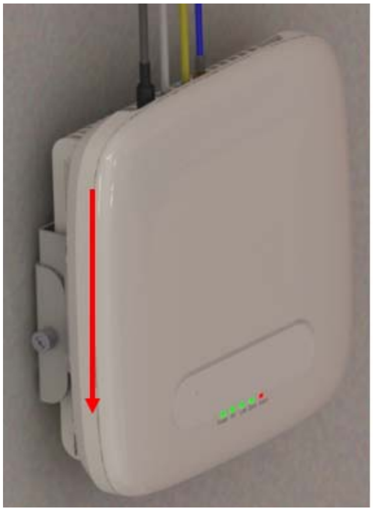
2. Align the tabs on the upper bracket with the opening on the lower bracket and push inward (see Figure 2-5).

Figure 2-5. Align tabs



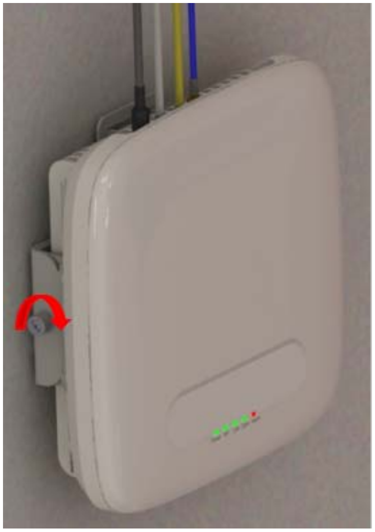
3. Push downward to seat the unit (see Figure 2-6).

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



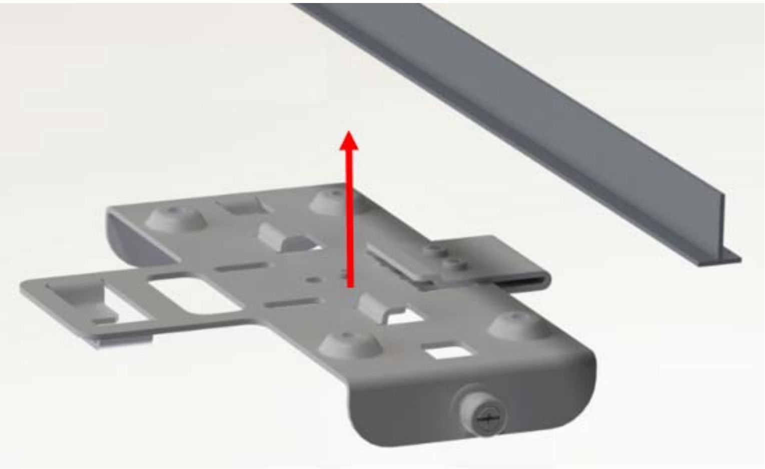
Securing the mounting bracket to a dropped ceiling

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.

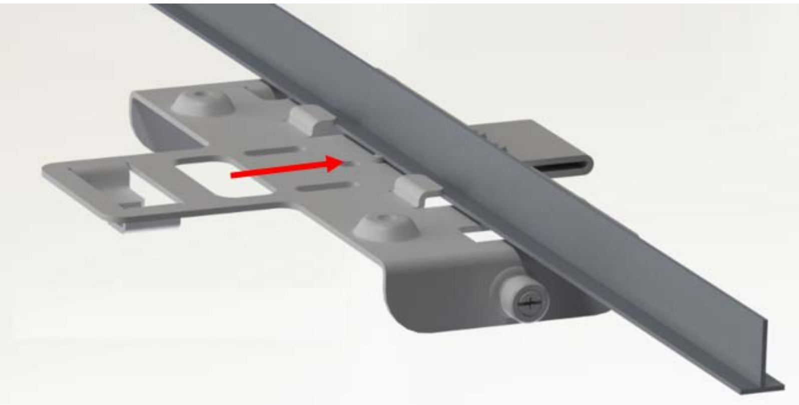
1. Push the upper bracket up against the bottom of the T-Rail (see Figure 2-8).

Figure 2-8. Push upper bracket



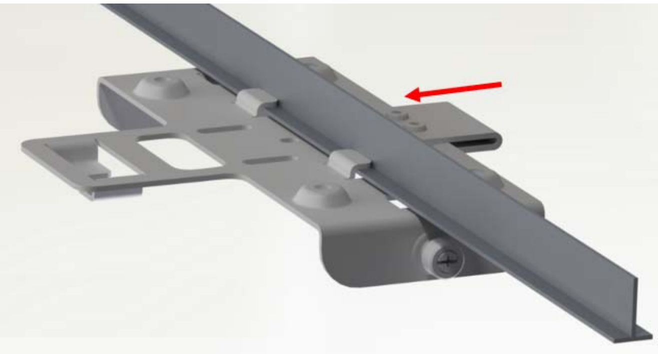
2. Push the upper bracket back against the T-Rail to engage the tabs (see Figure 2-9).

Figure 2-9. Engage tabs



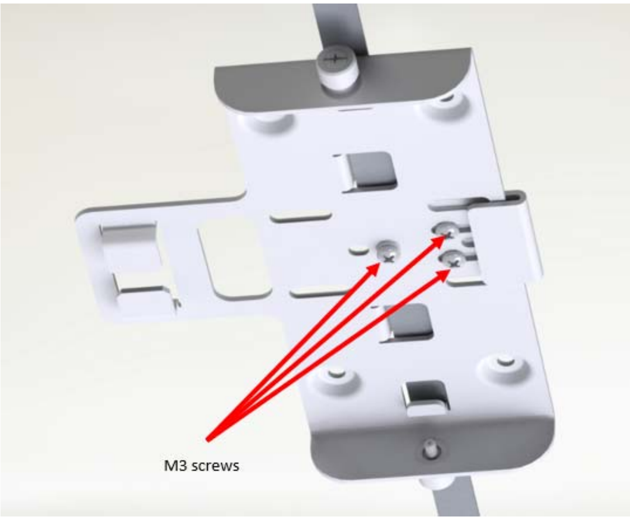
3. Push the clamp back against the T-Rail to engage tabs on both sides of the rail (see Figure 2-10).

Figure 2-10. Push clamp



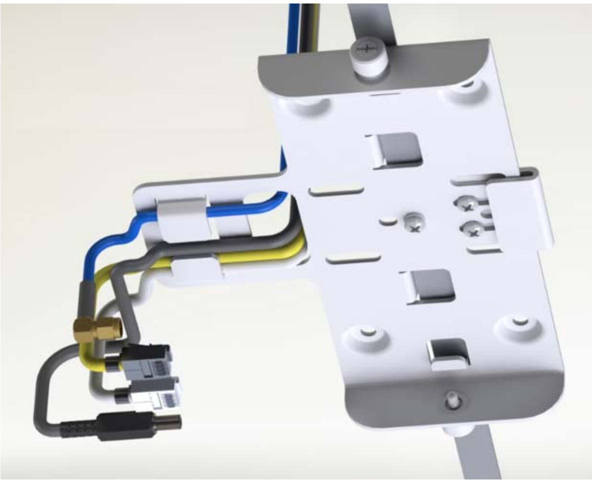
4. Tighten the three M3 screws to lock the clamp and the upper bracket onto the T-Rail (see Figure 2-11).

Figure 2-11. Tighten screws



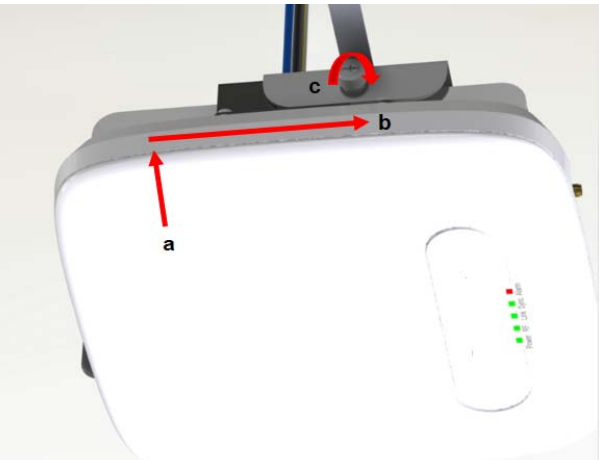
5. Route the cables in the cable management tabs (see Figure 2-12).

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

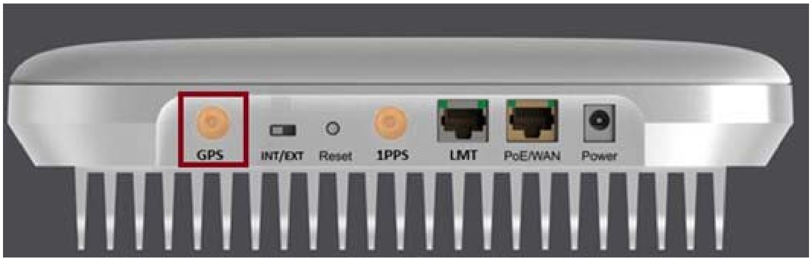


Connecting the cables

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

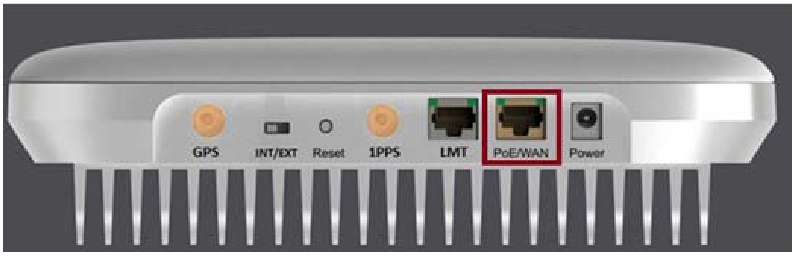


2. Position the GPS antenna puck near a window so it provides a clear and open view of the sky.

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).

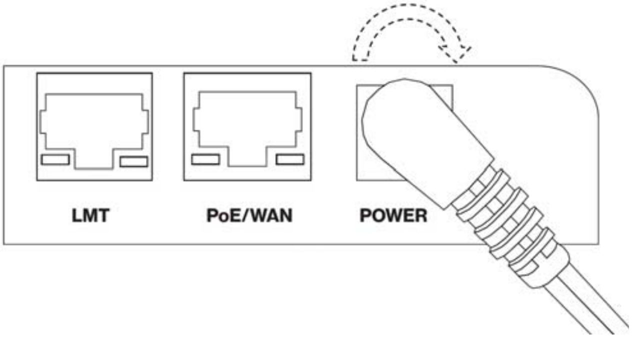
Figure 2-15. PoE/WAN port



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.

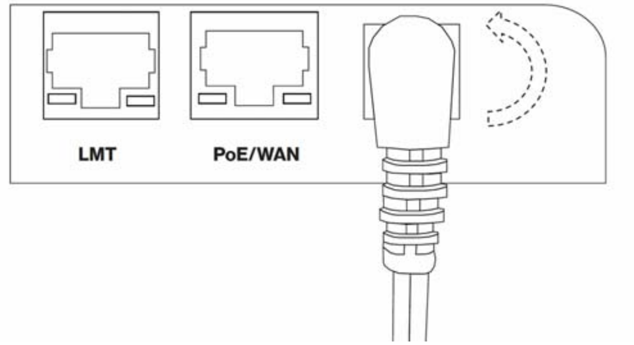
5. To install the power cable, it should be plugged in at 45 Degrees and twist clockwise to secure the power cord in the lock position (see Figure 2-16).

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

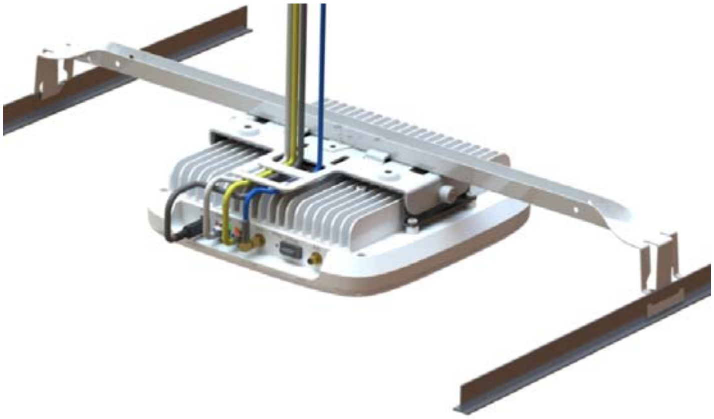
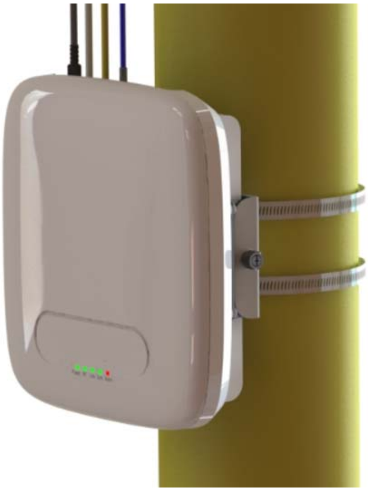


Figure 2-19. Pole mount installation



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	Green	ON: All the power rails are present.
		Flashing: Unit booting or firmware upgrading.
RF	Green	OFF: No activity.
		ON: Transmit or receive activity.
Link	Green	OFF: No link. ON: Link OK, Speed = 1000Mbps.
Sync	Green	OFF: No Sync.
		ON: Sync OK.
Alarm	Red	ON: System 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 Chapter 3, Web 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 Chapter 5, Troubleshooting for more information on alarm codes.

Indoor GPS antenna

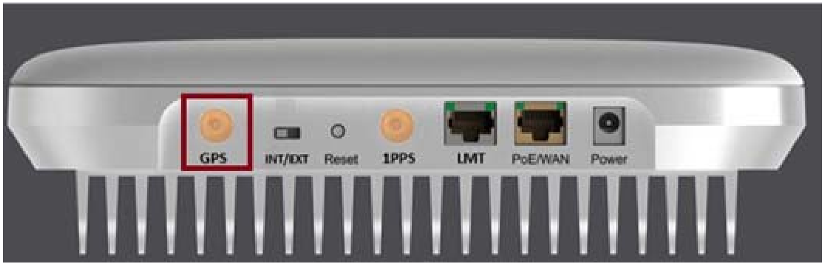
The Network Extender receives timing information from the GPS. The Network Extender is required to be placed such that the GPS receiver has an unobstructed line of sight with at least 4 strong satellites in order for it to get a position fix during the booting process. Thereafter, the Network Extender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

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.

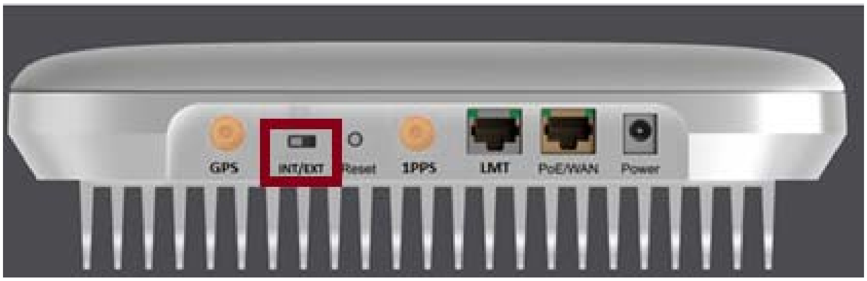
A GPS signal is required for proper operation and E911 service. If a GPS signal is not acquired after 30 to 60 minutes, please see Chapter 4, Configuration.

To see the status of the GPS acquisition, use the Admin website (Local) as shown in Chapter 3, Web GUI.

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

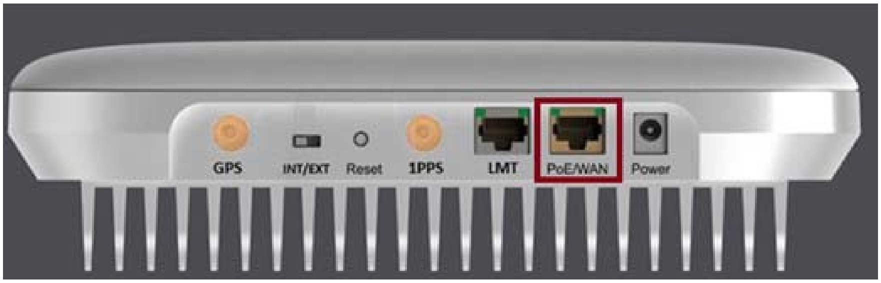


Table 2-1 provides the recommended PoE specifications for the Network Extender.

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. More detail is included in Chapter 5, Troubleshooting.

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:

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

Admin website access

There are two ways to access the Network Extender Admin Website.

1. Use the LMT port on the back side of the Network Extender.
2. Directly connect to Network Extender by using the Network Extender IP address, in case your computer is connected to the Same network as the Network Extender.

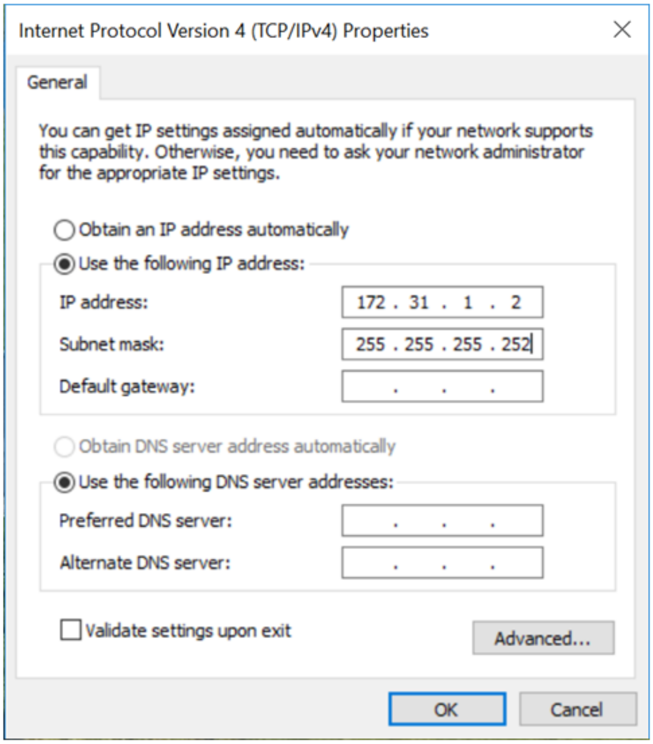
LMT port

To connect to the Network Extender, 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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 31 . 1 . 2
Subnet mask: 255 . 255 . 255 . 252
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

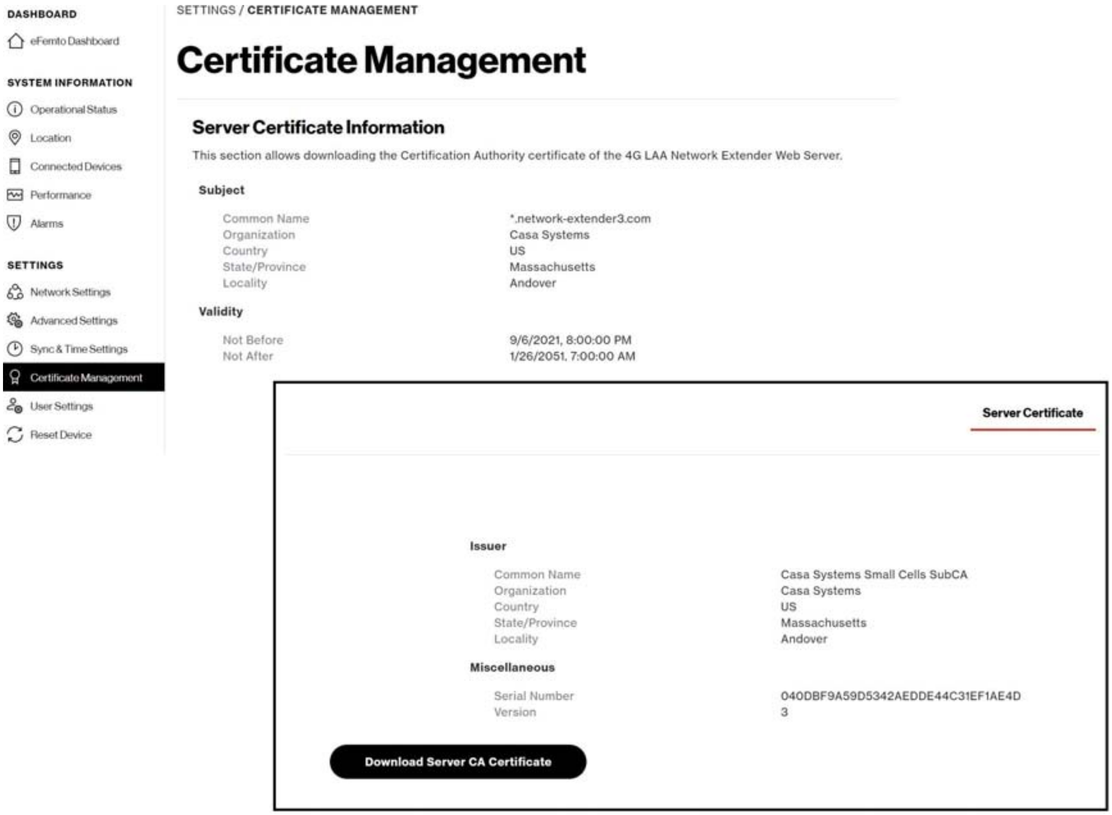
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

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



Certificate Management

Server Certificate Information

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

Subject

Common Name	*.network-extender3.com
Organization	Casa Systems
Country	US
State/Province	Massachusetts
Locality	Andover

Validity

Not Before	9/6/2021, 8:00:00 PM
Not After	1/26/2051, 7:00:00 AM

Issuer

Common Name	Casa Systems Small Cells SubCA
Organization	Casa Systems
Country	US
State/Province	Massachusetts
Locality	Andover

Miscellaneous

Serial Number	040DBF9A59D5342AEDDE44C31EF1AE4D
Version	3

Same network

To connect to the Network Extender, 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>.
```

Admin website overview

The Admin Website 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.

Sign in

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

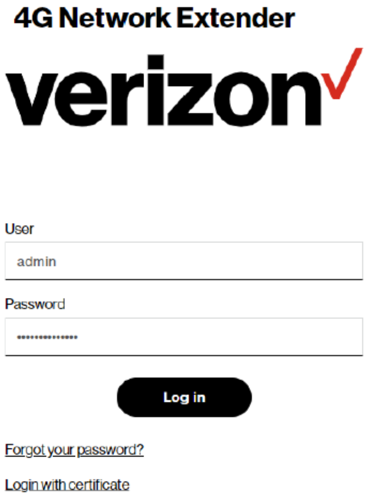
The default administrator password is **VzWNetExtender3@ + last six digits of the MAC**. The MAC ID can be found on the label on the side of the Network Extender.

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 Network Extender

User
admin

Password
••••••••••••••

Change admin password upon first sign in

If the user is signing 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

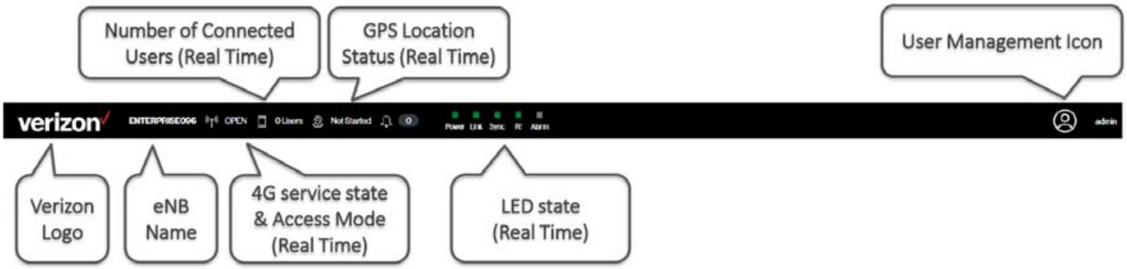
Set a Security Answer that should be between 1 and 64 characters long.

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.

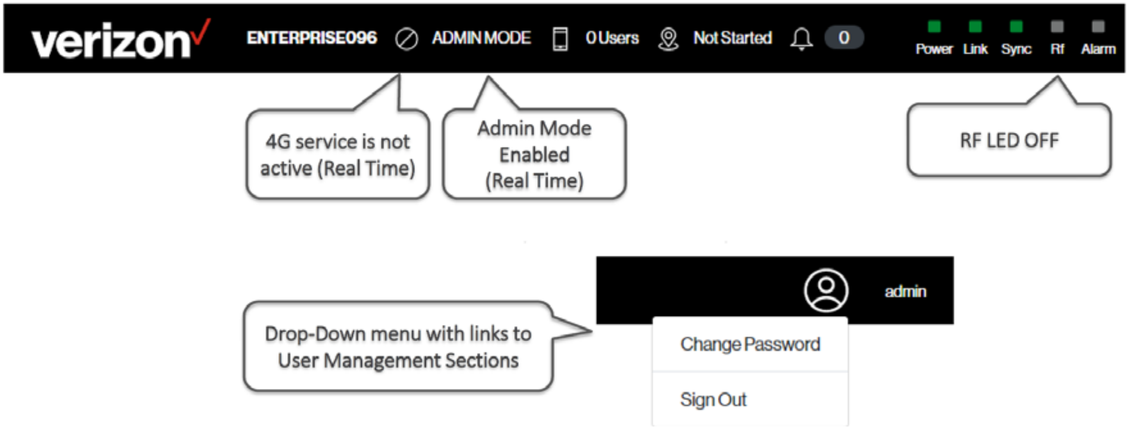
Header Bar information is common to all pages. The LEDs in the Header Bar show the same status as the physical LEDs on the Network Extender.

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


verizon
ENTERPRISE096
ADMIN MODE
0 Users
Not Started
0
Power
Link
Sync
Rf
Alarm
4G service is not active (Real Time)
Admin Mode Enabled (Real Time)
RF LED OFF
Drop-Down menu with links to User Management Sections
admin
Change Password
Sign Out

4G service state management

The eFemto 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 eFemto state.

Figure 3-6. Operational mode indicator

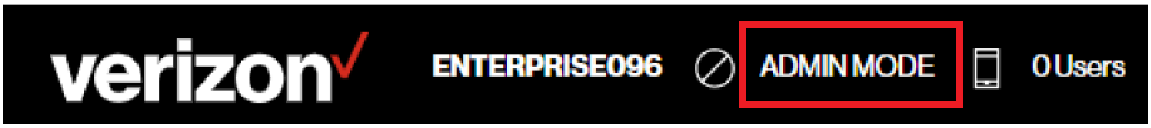


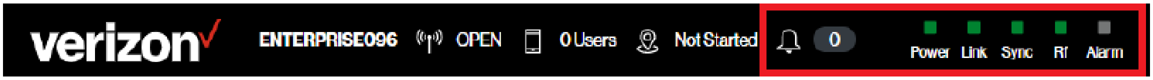
Table 3-1. Service states

eFemto 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 eFemto 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

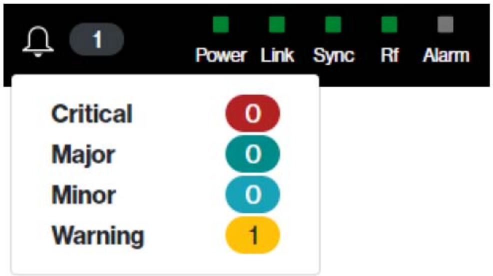
The alarms drop-down menu shows the active alarms in the system in all pages (see Figure 3-7).

Figure 3-7. Active alarms



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

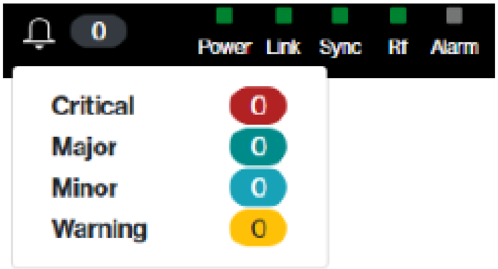
Figure 3-8. Alarm drop-down menu



Critical	0
Major	0
Minor	0
Warning	1

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

Figure 3-9. No alarms



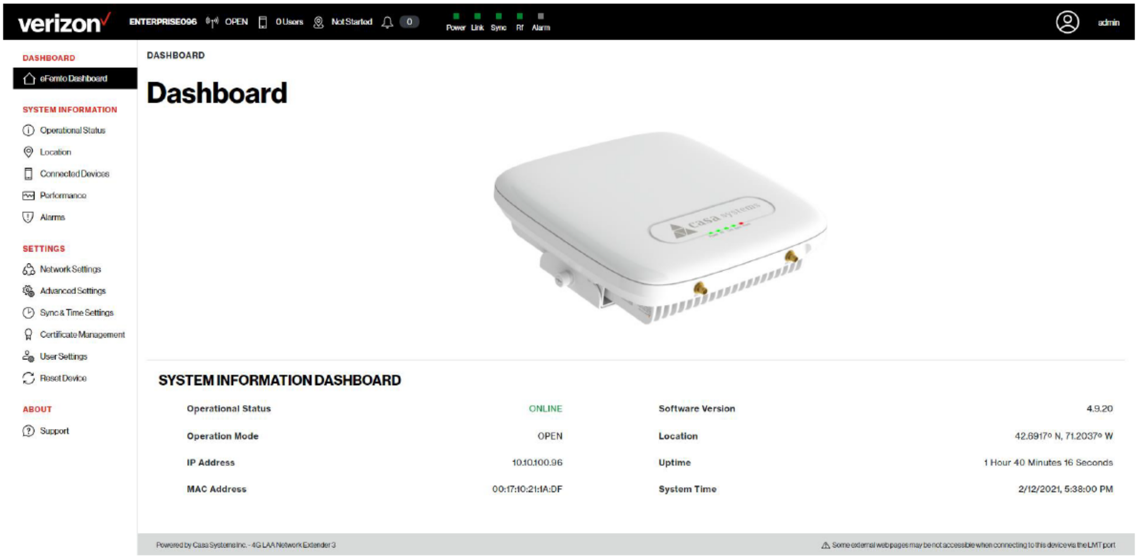
Critical	0
Major	0
Minor	0
Warning	0

Dashboard

The Web GUI dashboard (see Figure 3-10) provides both system information and Network Extender settings.

Refer to the *Verizon Enterprise Web GUI User Guide* for more information.

Figure 3-10. Network Extender dashboard



SYSTEM INFORMATION DASHBOARD

Operational Status	ONLINE	Software Version	4.9.20
Operation Mode	OPEN	Location	42.6917º N, 71.2037º W
IP Address	10.10.100.96	Uptime	1 Hour 40 Minutes 16 Seconds
MAC Address	00:17:10:21:1A:DF	System Time	2/12/2021, 5:38:00 PM

Powered by Casa Systems Inc. - 4G LAA 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:

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

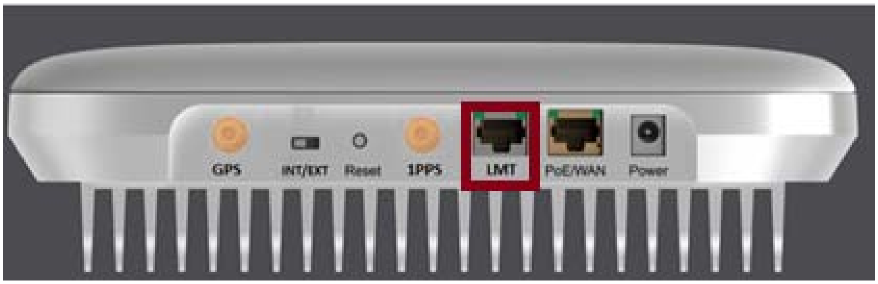


Table 4-1 provides details on the destination ports regarding the firewall settings that are applicable for network administrators.

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	IP Address	Fully Qualified Domain Name (FQDN)
GPS Server	-	http://xtrapath1.izatcloud.net http://xtrapath2.izatcloud.net http://xtrapath3.izatcloud.net
Security Gateway (SeGW)	141.207.245.235 141.207.137.235 141.207.129.235 141.207.243.235 141.207.249.235 141.207.225.235 141.207.213.235 141.207.233.235 141.207.197.235 141.207.193.235 141.207.145.235 141.207.151.235 141.207.177.235 141.207.173.235 141.207.181.235	sg.vzwfemto.com
NTP Server	The default NTP server is based on a pool.ntp.org. Different locations will get different IP addresses. The user needs to make sure the FQDN is allowed.	0.north-america.pool.ntp.org 1.north-america.pool.ntp.org

Note: The GPS Server URLs resolve to a varying list of IPs to ensure equal load distribution among the active servers. The three URLs are used in a round robin fashion in case of a DNS resolution failure or a server communication failure. The NTP service shall also be open. we are using as a default NTP server pool.ntp.org.

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.

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:

Status LEDs

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

Figure 5-1. Network Extender status LEDs

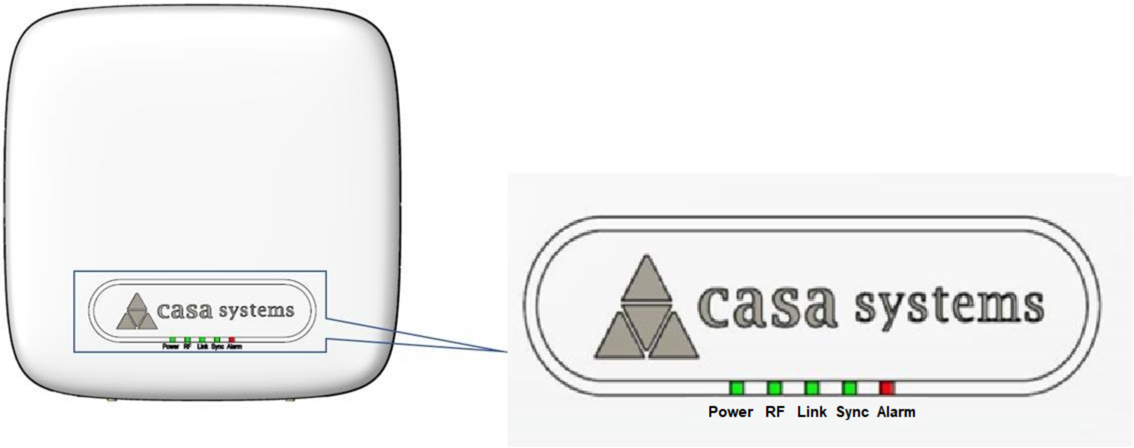


Table 5-1 provides functional details for each status LED applicable for network administrators.

Table 5-1. Status LED functions

LED	Color	Function
Power	Green	ON: All the power rails are present.
		Flashing: Unit booting or firmware upgrading.
RF	Green	OFF: No activity.
		ON: Transmit or receive activity.
Link	Green	OFF: No link. ON: Link OK, Speed = 1000Mbps.

Table 5-1. Status LED functions (continued)

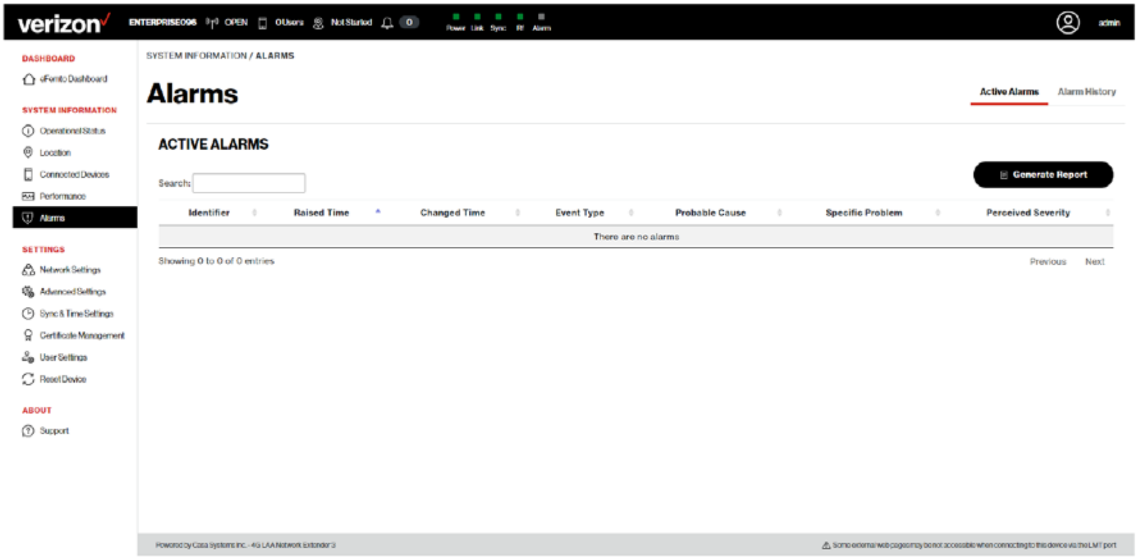
LED	Color	Function
Sync	Green	OFF: No Sync
		ON: Sync OK.
Alarm	Red	ON: System alarm.

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).

Note: Refer to the Verizon Enterprise Web GUI User Guide for more information.

Figure 5-2. Web GUI alarms page



SYSTEM INFORMATION / ALARMS

Alarms

ACTIVE ALARMS

Search:

Identifier	Raised Time	Changed Time	Event Type	Probable Cause	Specific Problem	Perceived Severity
There are no alarms						

Showing 0 to 0 of 0 entries

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

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

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

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20001	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.
20002	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.
20004	Flash memory usage	There is a temporary memory usage alert, but your device is still functioning correctly.	This alert should clear itself.
20005	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.
20006	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.
20008	High CPU load	There is a temporary CPU load alert, but your device is still functioning correctly.	This alert should clear itself.
20009	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 refer to the 4G LTE Network Extender Placement as described in Chapter 6.
20010	Over-the-air synchronization lost	This is related to RF quality issue.	Please Check for availability of Verizon macro sites signal.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20011	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.
20012	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.
20013	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.
20014	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.
20015	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).
20016	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).

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20017	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.
20018	OAM errors	Parameters not set properly.	Verify that all parameters are set per guideline.
20019	RAM memory full	The RAM memory is full.	Power cycle the unit to clear the fault.
20020	Threshold Crossed: RLF	Radio Link Failure.	Caused by high interference of weak signal.
20021	Threshold Crossed: Low SINR	Low SINR.	Check the radio environment. Please refer to the 4G LTE Network Extender Placement as described in Chapter 6.
20022	PA Biasing Failure	PA Biasing Failure.	Power cycle the device to clear the issue. If symptom persists, the unit will need to be replaced.
20023	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.
20024	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.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20026	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.
20027	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.
20028	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.
20029	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.
20030	Invalid PHY or RF configuration	Parameters not set properly.	Verify that all parameters are set per guideline.
20031	System information configuration failure	Parameters not set properly.	Verify that all parameters are set per guideline.
20034	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.
20035	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.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20036	IPsec tunnel expiry	The device cannot communicate with Verizon's Network.	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. If the problem persists, please contact Verizon Wireless Customer Service.
20037	IPsec IKE SA expiry	The device cannot communicate with Verizon's Network.	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. If the problem persists, please contact Verizon Wireless Customer Service.
20038	Operator Certificate Expired	The device cannot communicate with Verizon's Network.	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. If the problem persists, please contact Verizon Wireless Customer Service.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20039	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.
20040	Administrative Reboot	This is a notification that the device was rebooted from Verizon's Management System.	No action needed.
20041	Forced Reboot	This is a notification that the device was rebooted from Verizon's Management System.	No action needed.
20042	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.
20043	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.
20044	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.
20045	TR069 Agent not detected	The device shall resume normal operation after self-healing.	If the alert persists, please restart your device.
20046	Watchdog not detected	The device shall resume normal operation after self-healing.	If the alert persists, please restart your device.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20047	Critical configuration failure	Parameters not set properly.	Verify that all parameters are set per guideline.
20049	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.
20050	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.
20051	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.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20052	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.
20053	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.
20054	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.
20055	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.
20056	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.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20057	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 .
20058	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.
20059	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.
20060	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.
20061	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 eFemto device. Navigate to advanced setting to change the eFemto configuration.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20062	Not Signed Upgrade Package	Software upgrade failed due to wrong non-signed upgrade file.	An upgrade using wrong non-signed file has been attempted. No action is needed; the upgrade is rejected by the device.
20063	Integrity Check Failure	Software upgrade failed due to corrupted file.	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. If upgrade fails again, please contact Verizon Wireless Customer Service.
20064	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.
20065	Unable to get operator certificate from CMS server	The device cannot retrieve the operational Certificates from 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.
20066	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.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20067	Operator certificate expired	The device cannot communicate with Verizon's Network.	Please contact Verizon Wireless Customer Service.
20068	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.
20069	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.
20070	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.
20071	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.
20072	Operator certificate Issuer is not accepted by SeGW	The device cannot communicate with Verizon's Network.	Please contact Verizon Wireless Customer Service.

Table 5-2. Alarm troubleshooting (continued)

Unique Alarm ID (Code)	Alarm	Description	Recommendation
20073	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.
20074	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.

Chapter 6. Specifications

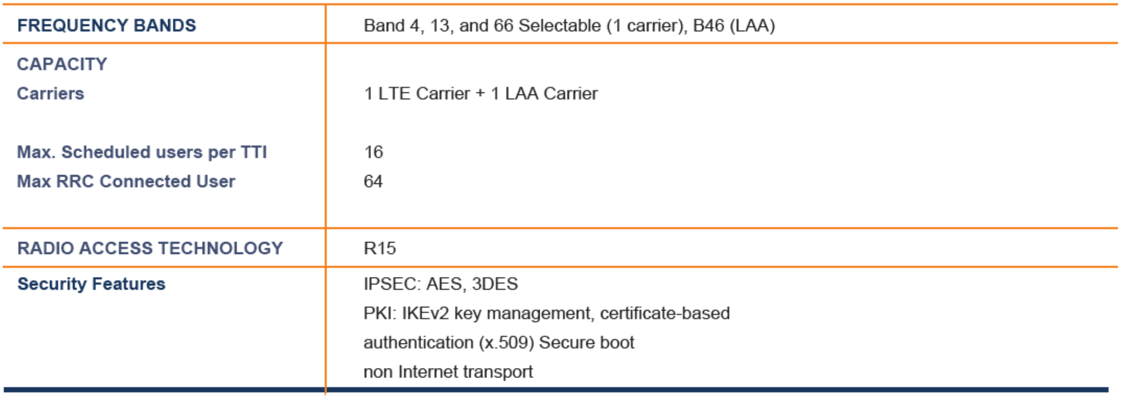
General information

Max TX Power - Licensed	24 dBm (2 streams @21 dBm) for the LTE carrier
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
BW Channelization - Licensed	5, 10, 15, 20 MHz
Max TX Power - LAA	27 dBm (2 streams @24 dBm) for each LAA port
LAA Channel	20 MHz
Logical Interfaces	LTE: S1-U, S1-MME, X2
Backhaul Options	10/100/1000 Gigabit Ethernet, RJ-45
Maximum Modulation	64 QAM
Synchronization	GPS or IEEE1588v2

Physical and Environmental

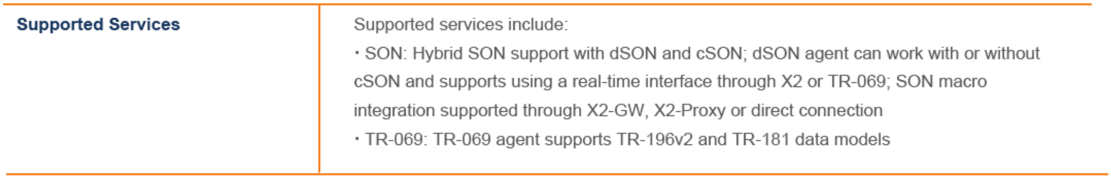
Dimensions	240 mm x 240 mm x 65 mm
Weight	<2200 Grams
Nominal Power Consumption Power	< 25W at full capacity with licensed bands, < 29W with LAA
	12 VDC power supply @ 220 VAC
	PoE+ 802.3at Class 4 with licensed bands only
	PoE++ 802.3bt Class 5 when LAA is enabled
Operational Temperature	-10ºC to 65ºC (14ºF to 149ºF)
Humidity	5% to 95% Relative Humidity - non condensing
Protection	IP50

Frequency bands



FREQUENCY BANDS	Band 4, 13, and 66 Selectable (1 carrier), B46 (LAA)
CAPACITY	
Carriers	1 LTE Carrier + 1 LAA Carrier
Max. Scheduled users per TTI	16
Max RRC Connected User	64
RADIO ACCESS TECHNOLOGY	R15
Security Features	IPSEC: AES, 3DES PKI: IKEv2 key management, certificate-based authentication (x.509) Secure boot non Internet transport

Supported services



Supported Services	Supported services include: • 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 • TR-069: TR-069 agent supports TR-196v2 and TR-181 data models

casa systems

100 Old River Road
Andover, MA 01810
USA
478-688-6706

Verizon 4G LTE Network Extender 3 for Enterprise User Guide

DOC-3198-01

Document Revision 3.1.0
October 2021

Printed in United States of America