WiFiProtect® 3e-520 SERIES USER'S GUIDE

Document Number: 29010012-001, Revision J2

21 December 2020

Prepared by:

Ultra Intelligence & Communications

12410 Milestone Center Drive, Germantown, MD 20876
Tel 800-449-3384 Fax 301-515-1027
www.Ultra-3eTI.com

Government Rights Legend

Export Restrictions

This product contains components, software, and/or firmware which, if and when required to be exported from the United States will be done in accordance with U. S. export administration regulations. Diversion contrary to U.S. law is prohibited.

Revision History

Revision Letter	Date	Description
A	05-12-2014	Initial Release
B	03-19-2015	Revised for Common Criteria
C	03-26-2015	Updated with review comments
D	08-11-2015	Updated with reivew comments and fixed missing figures
E	09-10-2017	Updated for Common Criteria NDcPP20/WLANAScEP10
F	05-04-2018	Updated with review comments
G	05-08-2018	Updated with review comments
H	03-24-2020	Updated for DoDIN APL
I	10-22-2020	Include model 3e-523E-900
J2	12-21-2020	Updated 3e-523E-900 installation, channel and tx level specs,

Table of Contents

List of Figures

List of Tables

1. Introduction

This manual covers the installation and operation of 3e Technologies International's (3eTI) latest members of the WiFiProtect® product family. The WiFiProtect 3e-520 series product family consists of the 3e-523N and the 3e-525N Access Point (hereinafter referred to as WiFiProtect products, or 3e-520 series product unless otherwise specified). The WiFiProtect products are secure, ruggedized wireless devices that have been designed and tested for use in harsh demanding environments where durability is a key requirement. These WiFiProtect products support the latest 802.11a/g/n wireless standards and provide security consistent with Federal Information Processing Standards (FIPS) 140-2 requirements using Advanced Encryption Standard (AES) cryptographic modules for wireless encryption and Hyper Text Transfer Protocol Service (HTTPS) / Transport Layer Security (TLS) for secure web communication.

1.1 Typical Deployment

The 3e-520 series products can be deployed in any commercial and industrial solutions to protect the sensitive network and user data. The following diagram (Figure 1) represents a typical deployment using 3e-520 series products to transmit sensitive information between remote sites to the NOC (Network Operations Center) via secured wireless connections. In this deployment, the 3e-520 series products are configured in wireless Mesh, Access Point and Client modes.

The 3e-520 series products support remote management via Active directory LDAP server and OCSP responder (Refer to Section 2.8 and Section 2.9 for more detail). The management communications are protected between itself and the Authentication Server, NTP Server and Remote Audit Server using IPsec tunnels.

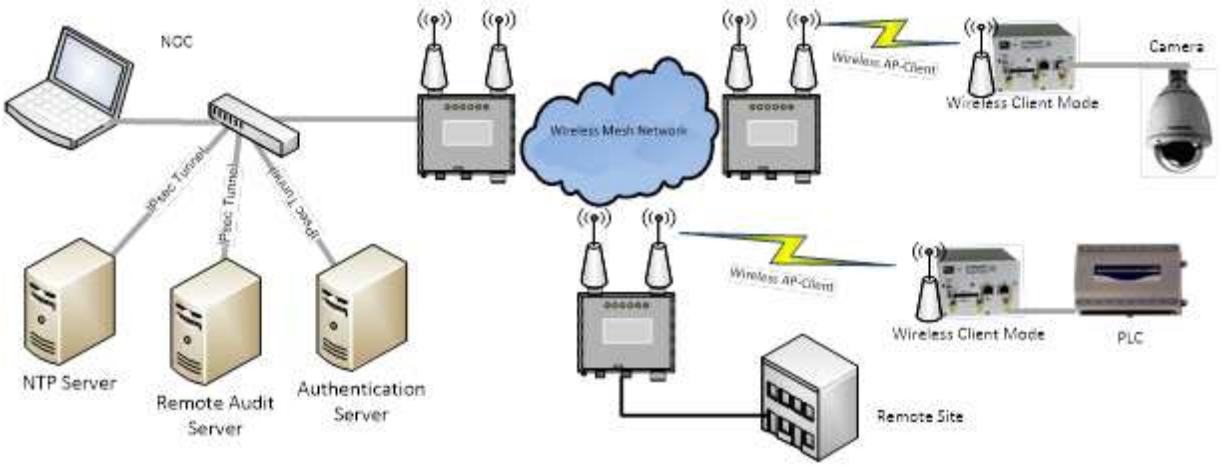


Figure 1: Typical Deployment Diagram

1.2 Products and Features

The 3e-520 series includes two different 802.11n products – 3e-523N and 3e-525N. Both products use a common hardware platform and run the same software. The major difference between these two models is single radio vs dual radio. The 3e-523N includes a single 802.11a/g/n radio card, indoor enclosure and is powered by a DC power adapter. The 3e-525N comes with dual 802.11a/g/n radio cards, an outdoor-rated enclosure and is powered by a PoE injector.

Please refer to the product-specific hardware sections later in this document for additional technical details.

1.2.1 3e-523N Access Point

The 3e–523N Data Point has the following key features:

- FIPS 140-2, 802.11 Wi-Fi (Wireless Fidelity) and Common Criteria,
- Supports 802.11n wireless standard with Multiple-input and Multiple-output (MIMO), channel bonding and packet aggregation to achieve link rates of up to 300 Megabits per second (Mbps),
- Self-forming, self-healing mesh network for always-on availability,
- Standards-based interface connectivity for devices with Ethernet or serial data interfaces:
    - One 10/100/1000 Base-T WAN (UPLINK) Ethernet port,
    - One 10/100/1000 Base-T LAN (LOCAL) Ethernet port,
    - Three MIMO antenna ports,
    - Supports RS-232 / 422 / 485 serial interface.
- Power: +5 to +12 Volts Direct Current (VDC).

1.2.1.1 External Interfaces

The purpose of this section is to describe the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Figure 2 shows the location of the external connectors, indicator Light Emitting Diodes (LEDs) and Reset Button on the 3e–523N.

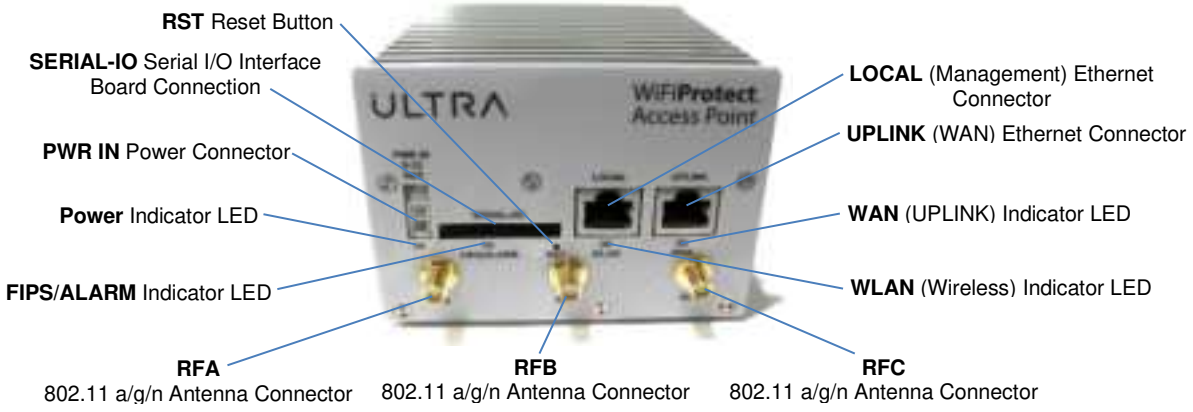


Figure 2: 3e-523 External Connectors and Indicators

Table 1: 3e-523N External Connectors and Indicators	
Interfaces	**Description**
RF A, RF B, RF C Antenna Ports	For 802.11 a/g operation, connect a single antenna to **RF A**; it can be mounted directly to the unit, or mounted remotely. For 802.11n MIMO operation, it requires the use of three antennas. Although they can be mounted directly to the unit, it is recommended that they be separated to improve MIMO performance.
UPLINK (WAN)	The Uplink port is used to connect the unit to the enterprise local network. It supports the 10/100/1000 BaseT Ethernet standard.
LOCAL (WLAN)	The Local port is used to access the device's web management Graphical User Interface (GUI). It can only access the management interface; it cannot access the wireless radio or the uplink data path. This port supports the 10/100/1000 BaseT Ethernet standard.
SERIAL – I/O	This connector is used to connect to the (optional) Serial I/O Interface Board as shown in Appendix C. Serial I/O Interface Board.
PWR IN	This connector supplies 5-12 VDC power to the unit; see Section 0 below for details.
RST	The operation of this Reset Button is described in Section 1.2.1.4 below. Note that the unit can also be reset via the Serial I/O Interface Board and the unit's Web GUI.

1.2.1.2 Power

Power is supplied to the unit via the PWR IN connector. Figure 3 shows the optional 9 VDC power supply (Desktop Power Kit), and the location of the ground connection provided on the side of the 3e-523N. A DIN-Rail Mounted Power Kit and a Power Pigtail Cable are also available with the custom power connector used on the 3e-523N – see Section 3.1, Table 17, for a listing of available accessories.

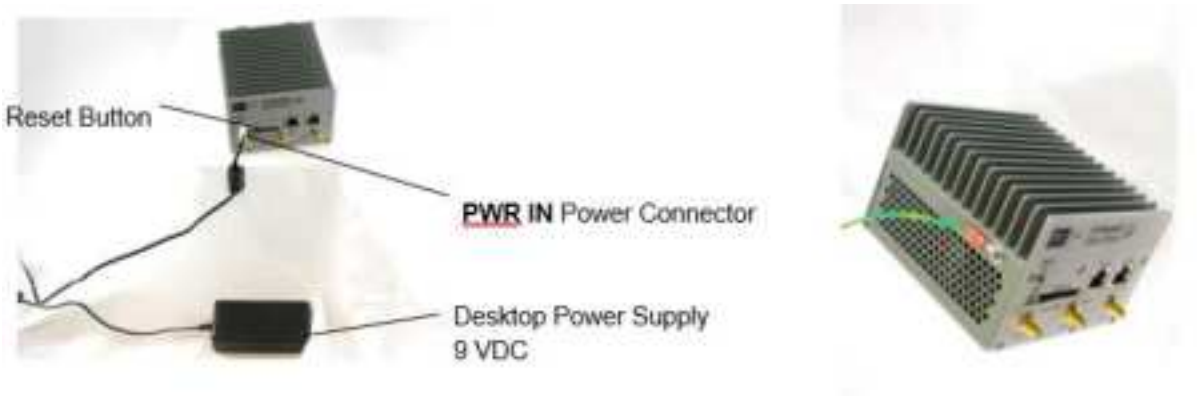


Figure 3: 3e-523N Power Supply and Ground Connections

1.2.1.3 Indicator LEDs

Figure 2 shows the location of the external connectors, indicator LEDs, and Reset Button on the 3e–523N. The LEDs and their function are described below in Table 2.

Table 2: 3e-523N Indicator LEDs	
LED	**Description**
Power	The Power Indicator LED will light to indicate that power is being supplied to the unit.
WAN	The WAN LED indicates activity and uplink signal strength on the WAN. • LED Off: no connection on the uplink, or the signal is very weak • LED blinks slowly (every 1 second): there is a connection, and the signal quality is poor • LED blinks fast: there is a connection, and the signal quality is good • LED remains on: there is a connection, and the signal quality is excellent This LED is not used when the operating mode of the device is set for access point mode.
WLAN	The WLAN LED will flash to indicate activity on the WLAN. It is also used to provide status information when the 3e-523N is reset; see Section 1.2.1.4 for details.
FIPS/ALARM	The FIPS/ALARM LED indicates whether the 3e–523N is in FIPS mode. When this LED is lit, the system is in FIPS mode; when it is not lit, the system is in non-FIPS mode.

1.2.1.4 Reset (RST) Button

Figure 4: 3e-523N External Connectors and Indicators

Figure 4 shows the location of the Reset Button on the 3e–523N and Figure 107 in Appendix C. shows the location of the Reset Button on the Serial I/O Interface Board. Both buttons operate identically.

The reset button has several purposes:

- Commanding a simple reboot,
- Commanding a restore to factory default configuration.

When the reset button is first pressed, the WLAN LED will light up, providing feedback that the button has indeed been pressed. If one continues to press the button, the LED will go dark after 5 seconds, light again after 10 seconds, and will return to showing WLAN radio activity after 15 seconds. If the button is pressed for more than 15 seconds, the button press is ignored, until released and subsequently pressed again.

For a simple reboot, hold the button for slightly more than 5 seconds, specifically until the WLAN LED goes dark. Then release the button. The device will reboot, and the LEDs will indicate the normal pattern one sees just after power up.

NOTE: If you hold the button too long, you could accidentally restore to factory defaults and wipe out your device configuration. To avoid this possibility, consider resetting the unit by removing power, or through the unit's web interface.

In order to restore to the factory default, press the button, then hold for at least 10 seconds, specifically until one sees the WLAN LED come on for a second time. Then release the button. The device will return to the user selected factory default state.

1.2.2 3e-525N Access Point

The 3e–525N Access Point has the following key features:

- Highly secure - AES 256, FIPS 140-2 validation AES and 802.11i,
- Dual radios with MIMO antennas with maximum data rate of 300 Mbps,
- 802.1Q Virtual Local Area Network (VLAN) allows use of multiple Service Set Identifiers (SSIDs),
- Power-over-Ethernet (PoE) standard 802.3 at compliant and 802.3af backward compatible,
- Standards-based interfaces:
    - One 10/100/1000 Base-T WAN (UPLINK) Ethernet port,
    - One 10/100/1000 Base-T LAN (LOCAL) Ethernet port,
    - Two 802.11n compatible wireless interfaces,
    - Six MIMO antenna ports.
- Power
    - 3e-525N supports 48 VDC PoE on UPLINK Ethernet Port

1.2.2.1 External Interfaces

The purpose of this section is to describe the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Figure 5 shows the location of the external connectors, indicator Light Emitting Diodes (LEDs) and Reset Button on the 3e–525N.

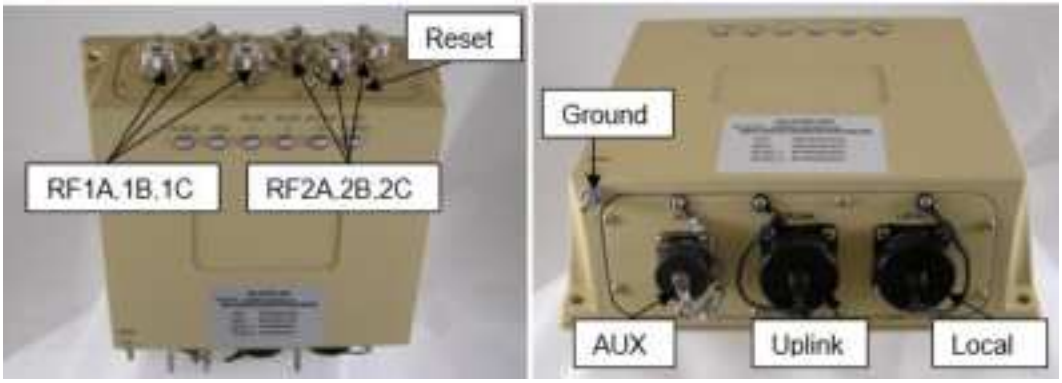


Figure 5: 3e-525N External Interfaces

Table 3: 3e-525N External Interfaces	
Interfaces	**Description**
Antenna Ports	Six antenna ports; Antenna ports RF1A, 1B, 1C are connected to Radio 1 Antenna ports RF2A, 2B, 2C are connected to Radio 2
Uplink (WAN Port)	The Uplink Port is used to connect the unit to the enterprise local network. This port accepts PoE compatible with 802.3at and 802.3af (PoE cable connection is illustrated in Section 2.1.2) and supports the 10/100/1000 BaseT Ethernet standard.
Local (Management Port)	The Local Port is used to access the device's web management GUI. It can only access the management interface and cannot access the wireless radio or the uplink data path. This port supports the 10/100/1000 BaseT Ethernet standard.
AUX	The AUX port includes Contact Alarm Inputs and Reset input for the 3e-525N. .
Ground	Proper connection to between Ground connection and ground is essential for the device to be compliant with emission requirements and to avoid lightning damage.
Reset Screw	The screw must be unscrewed, and an un-bended paper clip can be used to press the reset button as described below. The screw should be replaced after reset; the screw is watertight and should not be unscrewed more than once. It is recommended that you use the AUX port to reset the device rather than using the reset screw.

The accessory 3e-CPLR-1 in Table 18 is used to connect with the WAN or LAN port.

The pin definition of AUX port is shown in Figure 6.

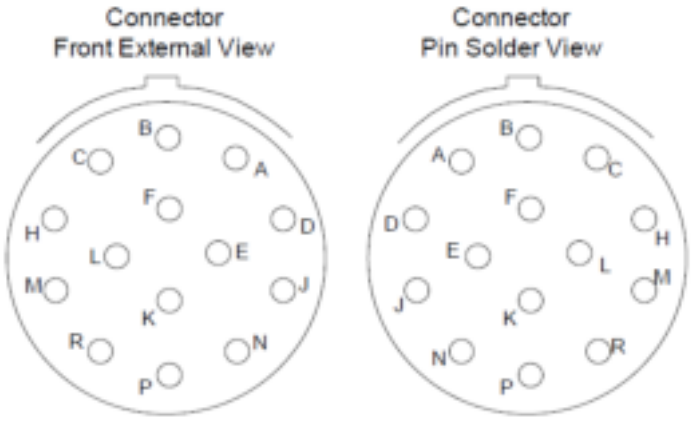


Figure 6: AUX Port Pin Definition

The functional description of AUX pins is shown in Table 4.

Table 4: 3e-525N AUX Port		
Signal Name	**Pin**	**Device**
Alarm 1 +	C	3e-525N
Alarm1 -	B	3e-525N
Alarm 2 +	M	3e-525N
Alarm 2 -	H	3e-525N
Reset	A	3e-525N
Reset Return	D	3e-525N

Connector 3e-CONN-A1 listed in Table 18 is used to connect with this AUX port on 3e-525N model. The Alarm functions are reserved for future use.

1.2.2.2 Power

3e-525N product operates with PoE, which requires the installation of a separate power injector that "injects" Direct Current (DC) into the Ethernet cable. These PoE devices should comply with 802.3at or 802.3af specifications. Standard versions of the 3e-525N product draws a maximum 14 Watts of power.

1.2.2.3 Indicator LEDs

The top panel of the unit contains a set of indicator LEDs (Figure 7) that help describe the state of various networking and connection operations. **Table 5** describes in detail what they represent.

Figure 7: Indicator LEDs

Table 5: Indicator LED Descriptions	
LED	**Description**
Power	The Power indicator LED informs you when the Access Point (AP) is on or off. If this light is on, the access point is on; if it is not on, the access point is off.
WAN	The WAN LED indicates the state of your connection to the organization's Ethernet LAN network. When the LED is on, the unit is connected to the network. When the

Table 5: Indicator LED Descriptions	
LED	**Description**
	LED blinks, Ethernet packets are being transmitted or received by the interface. When the LED is off, the AP does not have an active connection to the network.
WLAN1	When the LED is on, radio 1 is turned on. When the LED is off, radio 1 is turned off.
WLAN2	When the LED is on, radio 2 is turned on. When the LED is off, radio 2 is turned off.
Uplink SS (Signal Strength)	LED Off: Uplink is only connected through the WAN interface. Neither radio is used as an uplink bridge. The Uplink LED blinks in four rates (very slow, slow, fast, solid on) represents four levels of signal level (poor, fair, good, excellent) LED is red: The device becomes the root of mesh network.
FIPS/MODE	LED is solid green: the device is in FIPS mode. LED is yellow blinking over green: the device is in a periodic self-test. LED is red blinking: the device failed the self-test. LED is solid red: physical tempering of the device is detected.

NOTE: When the WLAN1, WLAN2, and FIPS/MODE LEDs blink simultaneously then the system is halted, it indicates that the software discovers a problem with the encryption algorithm or that the system configuration does not pass the integrity check.

1.2.2.4 Reset Function

The reset function in the AUX port or the Reset Screw has several purposes:

- Commanding a simple reboot,
- Commanding a restore to factory default configuration.

When the reset button is first pressed, the **WLAN1** LED will light up, providing feedback that the button has indeed been pressed. If one continues to depress the button, the LED will go dark after 5 seconds, light again after 10 seconds, and will return to showing WLAN radio activity after 15 seconds. If the button is pressed for more than 15 seconds, the button press is ignored, until released and subsequently pressed again.

For a simple reboot, hold the button for slightly more than 5 seconds, specifically until the **WLAN1** LED goes dark. Then release the button. The device will reboot, and the LEDs will indicate the normal pattern one sees just after power up.

NOTE: If you hold the button too long, you could accidentally restore factory defaults and wipe out your device configuration. To avoid this possibility, consider resetting the unit by removing power, or through the unit's web interface.

For a restore to factory defaults, press the button, then hold for at least 10 seconds, specifically until one sees the WLAN LED come on for the second time. Then release the button. The device will restore to the factory default state.

1.3 Wireless and Networking Basics

Wireless networking uses electromagnetic Radio Frequency (RF) waves to transmit and receive data. Communication occurs by establishing radio links between the wireless AP and devices configured to be part of the WLAN.

1.3.1 IEEE 802.11

The WiFiProtect product family incorporates Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wi-Fi standards and FIPS 140-2 security for wireless communication.

1.3.1.1 802.11a

The IEEE 802.11a standard is an extension to 802.11 which applies to WLANs and provides up to 54 Mbps in the 5 Gigahertz (GHz) band. Depending on radio design and RF channel issues, 802.11a devices can operate at rates between the 54 Mbps maximum and 6 Mbps. 802.11a uses an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS).

1.3.1.2 802.11g

The IEEE 802.11g standard is an extension to 802.11 which applies to WLANs and provides up to 54 Mbps in the 2.4 GHz band. Depending on radio design and RF channel issues, 802.11g devices can operate at rates between the 54 Mbps maximum and 6 Mbps. Much like the 802.11a standard, 802.11g uses an OFDM encoding scheme for data transmission.

802.11g is backwards-compatible with 802.11b and therefore, it is a popular component in WLAN construction. 802.11g broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band providing higher data transmission rates.

1.3.1.3 802.11n

802.11n is an extension to 802.11 that improves network throughput over 802.11a and 802.11g, with a significant increase in the maximum net data rate from 54 Mbps to 600 Mbps. 802.11n standardized support for features such as, MIMO, frame aggregation, and security improvements.

1.3.2 Wireless Network Topologies

The WiFiProtect product family supports a variety of network functions, depending on the model and configuration.

1.3.2.1 Access Point Operation

When an WiFiProtect product is used as an AP, the AP virtually connects wireless users to a host wired network. All wireless devices connected to the AP are configured on the same subnetwork as the wired network interface and can be accessed by devices on the wired network. Possible AP topologies include:

1) Standalone AP Network

a) An AP can be used as a standalone AP without any connection to a wired network. In this configuration, the AP simply provides a standalone wireless network for a group of wireless devices (Figure 8).

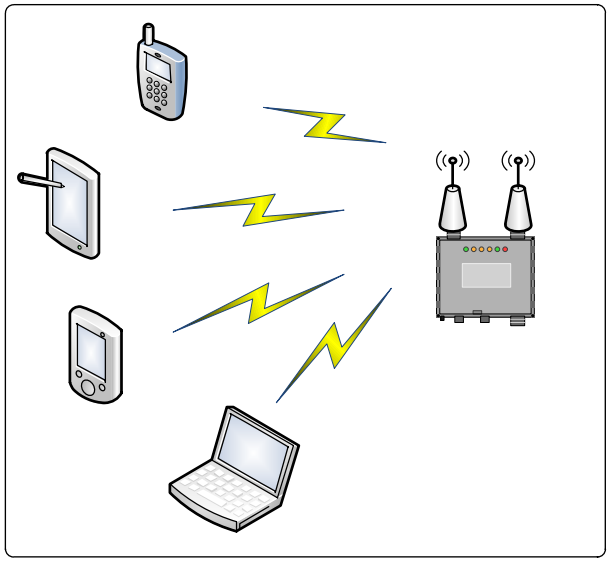


Figure 8: Standalone AP Network

2) Independent AP Networks

a) Multiple APs (Figure 9) can be connected to an existing Ethernet network to bridge between the wired and wireless environments. Each AP can operate independently of the other APs on the LAN. Multiple APs can coexist as separate individual networks at the same site with a different network identifier (ID), SSID.

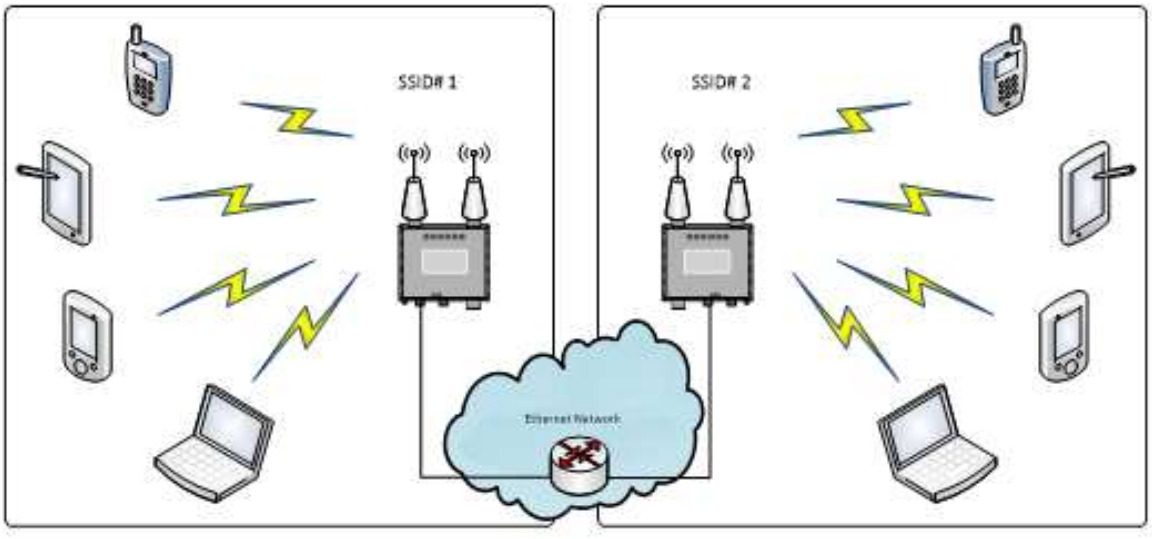


Figure 9: Multiple APs Connected to an Existing Ethernet Network

3) Integrated AP Networks

a) Integrated AP networks are the most prevalent topology choice. In this topology, multiple APs (Figure 10) are connected to a wired network and operate off of that network's Dynamic Host Configuration Protocol (DHCP) server to provide a wider coverage area for wireless devices, enabling the devices to "roam" freely about the entire site. The APs must use the same SSID.

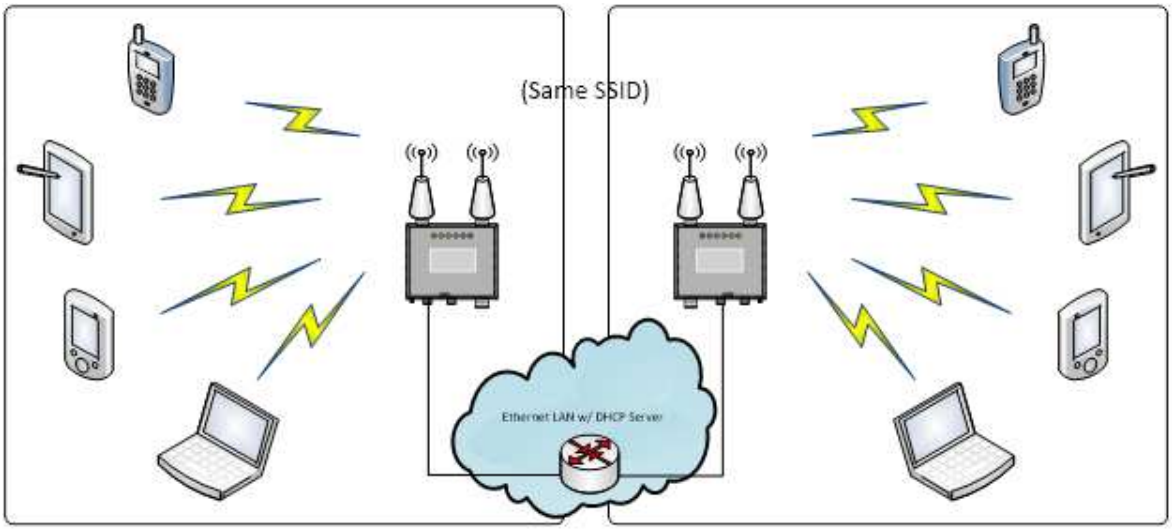


Figure 10: Multiple APs Connected to an Existing Ethernet Network with DHCP Server

1.3.2.2 Bridging Operation

The wireless bridging function of the WiFiProtect product family supports number of bridging configurations, including the following:

- Point-to-point bridging of two Ethernet links
- Point-to-multipoint bridging of several Ethernet links (mesh)
- Dual bridge configuration to connect networks with dissimilar radio, frequency, channel, and/or SSID (see Figure 11 below).

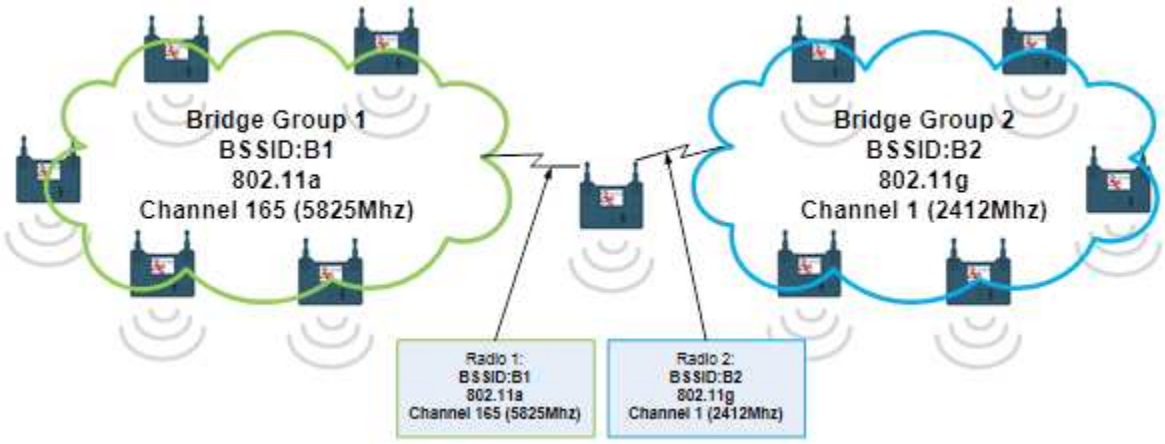


Figure 11: Dual Bridge Configuration

1.3.2.2.1 Dual Bridge Mode Operation

In 3e-525N products, there are two radios, which can work as bridges at different frequency bands. As shown in Figure 11, the two groups of bridges can work at two different frequency bands. The bridge in the middle uses two radios and works on different frequency bands to connect the two groups together. Since the two groups are using difference frequency bands, there will be less congestion in the bridge backhaul traffic when compared to using single frequency bands for all eleven bridges.

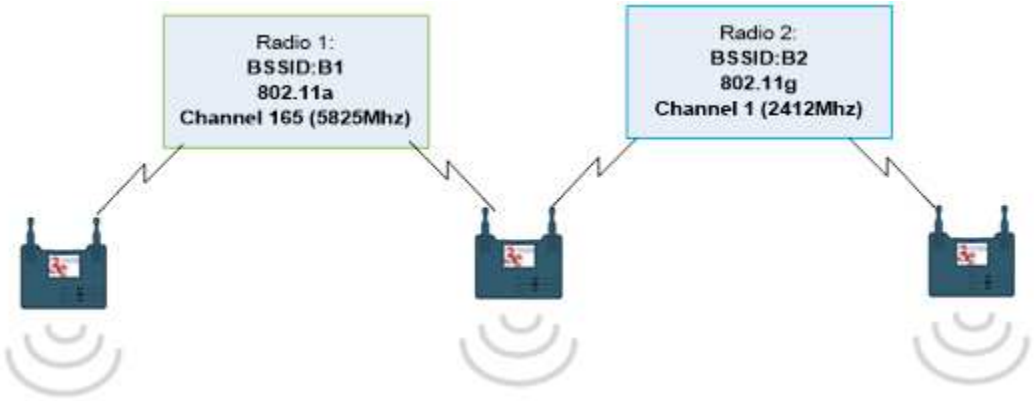


Figure 12: Bridge Relay with Different Frequency Bands

Figure 12 shows a bridge relay using different frequency bands. The bridge throughput will not reduce at each hop. If all bridges on the relay chain are using the same frequency bands for bridge, the bridge throughput put will be reduced for each additional hop.

1.3.2.3 Client Operation

In the client mode of operation, the device acts as a wireless endpoint providing a communication link from a local device into a WLAN. Because this requires only a single radio, the dual-radio AP 3e-525N is not typically used in client mode.

1.3.3 MAC Address Filtering

The Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the Open Systems Interconnection (OSI) Reference Model is divided into two sub-layers: The Logical Link Control (LLC) layer and the MAC layer. The MAC layer interfaces directly with the network media. Consequently, each type of network media requires a unique MAC address.

The WiFiProtect product family, if set up to use MAC address filtering, detects an attempt to connect by a client and compares the client's MAC address to those on a predefined MAC address filter list. Only client addresses passing the filtering rule are allowed to associate. MAC addresses are pre-assigned by the manufacturer for each wireless card.

1.3.4 DHCP Server

The DHCP function is accessible only from the local LAN port to be used for initial configuration. This simple DHCP server is for local configuration convenience and is not accessible through wireless ports.

NOTE: Installers should not rely on this server to allocate IP addresses for other devices in their network.

1.3.5 Data Encryption and Security

Authentication mechanisms are used to authenticate an operator accessing the WiFiProtect device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Bridging encryption can be established between WiFiProtect devices using AES-Cipher Block Chaining (CBC) or AES-Counter with CBC MAC (CCM) encryption (approved by the National Institute of Standards and Technology (NIST) for U.S. Government and Department of Defense (DoD) agencies).

AP encryption can utilize Wi-Fi Protected Access 2 (WPA2) or AES, depending on the mode of operation. WPA2 supports using a WPA PSK or a RADIUS Server for key management with AES-Counter-mode/CBC-MAC Protocol (CCMP).

1.3.5.1 Advanced Encryption Standard (AES)

The AES was selected by NIST in October 2000 as an upgrade from the previous Data Encryption Standard (DES). AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information. AES has the ability to use larger 192-bit and 256-bit keys, if desired.

802.11i and WPA2 employ AES-CCM, which is a combination of AES Counter Mode (CTR) per packet data encryption, combined with AES-CBC.

AES-CBC provides per packet data integrity/authentication of the entire packet including the Message Authentication Code (MAC) header.

1.3.5.2 WPA2 / 802.11i

WPA2 utilizes IEEE 802.11i, a Layer 2 specification that focuses on strengthening IEEE 802.11 security at the MAC sublayer. It is completely separate from and independent of Virtual Private Network (VPN) designs/architectures, which are often implemented at Layer 3. IEEE 802.11i includes specifications on encryption, authentication and key management in a multi-layered approach to security. IEEE 802.1X-based authentication mechanisms are used, with AES in CCMP mode, to establish an 802.11 Robust Security Network (RSN).

IEEE 802.1X defines a framework based on the EAP over LANs, also known as EAPoL. EAPoL is used to exchange EAP messages which execute an authentication sequence and for key derivation between a Station (STA) and an EAP entity known as the Authentication Server (AS).

IEEE 802.11i defines a four-way handshake using EAPoL for key management and group key derivation. Four major categories or primary functions of 802.11i are invoked within the WiFiProtect products:

- **EAP-TLS**: Extensible Authentication Protocol Transport Layer Security is typically supported by products receiving WPA2 certification.
- **IEEE 802.1X**: Known as port based network access control, 802.1X provides an authentication framework within 802.11i. 802.11i depends upon 802.1X to control the flow of MAC Service Data Units (MSDUs) between the Data Server (DS) and STAs by use of the IEEE 802.1X Controlled/Uncontrolled Port model. The 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an 802.1X authentication procedure completes successfully over the 802.1X Uncontrolled Port. 802.11 depends upon IEEE 802.1X and the EAPoL-Key 4-Way and Group Key Handshakes to establish and change cryptographic keys. Keys are established after authentication is complete.

- **4-Way Handshake**: The 4-way handshake defined in 802.11i achieves the following important goals within the security protocol:
    - It confirms the Primary Master Key (PMK) between the supplicant (client) and authenticator (AP)
    - It establishes the temporal keys to be used by the data-confidentiality protocol
    - It authenticates the security parameters that were negotiated
    - It provides keying material to implement the group key handshake within 802.11i
- **AES CCMP**: 802.11i and WPA2 employ AES-CCM, which is a combination of AES CTR per packet data encryption, combined with AES-CBC. AES-CBC provides per packet data integrity / authentication of the entire packet including the MAC header.

1.3.6 Ultra 3eTI Wireless VLAN

According to the IEEE, VLANs define broadcast domains in a Layer 2 network. Ultra 3eTI Wireless VLANs have the same attributes as physical LANs with the additional capability to group end stations physically to the same LAN segment regardless of the end stations' geographical location.

When wireless VLAN is enabled, an AP can be configured to have multiple SSIDs, so that it supports multiple wireless networks, with each network belonging to a VLAN. A wireless client communicates with the AP inside a wireless network defined by a SSID, so it does not know that the wireless VLAN exists. The mapping between the wireless network and the wireless VLAN happens inside the AP. Each wireless VLAN can have its own security level set. For example, the VLAN for an enterprise network access may use 802.11i with Extensible Authentication Protocol (EAP)-TLS authentication; while the VLAN for guest internet access may simply use 802.11i with Pre-Shared Key (PSK) (Figure 13).

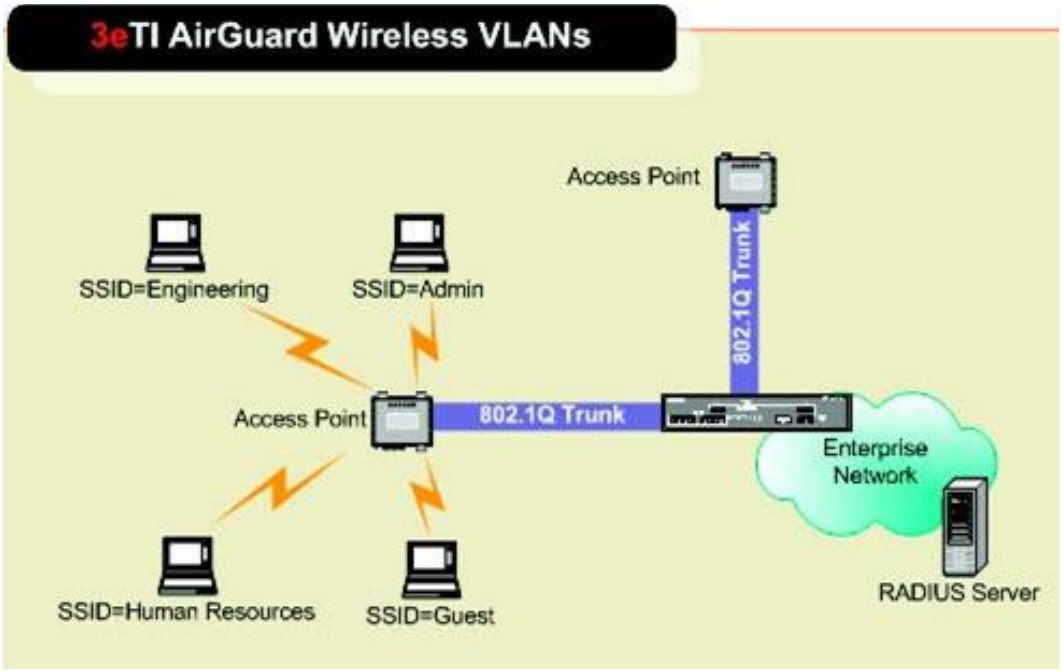


Figure 13: Wireless VLAN Communications

Optionally, the user can configure the WAN Ethernet port on a specific VLAN. In this case, only traffic with this specific VLAN ID can be sent out of the WAN Ethernet port and it also remains untagged. All Ethernet traffic coming into the WAN port is automatically tagged with the configured VLAN tag.

1.4 Device Management and Administration

After initial setup, maintenance of the system and programming of security functions should be performed by personnel trained in the procedure using the embedded web-based management screens. WiFiProtect devices support two categories of users.

There are two ways of managing 3e-520 series devices: locally and remotely

Local user management is done by locally accessing the 3e-520 series GUI through the LOCAL MGMT Ethernet port. Users created in the 3e-520 series local database have the highest privilege ('3e-local' user role), no other roles are possible. See Section 1.4.2 Local User Management for more details.

Remote user authentication and authorization (Remote A&A) is centrally managed at enterprise level. The 3e-520 series device uses the Lightweight Directory Access Protocol (LDAP) to authenticate username and password against an Active Directory Server. Users can be assigned to any of three user roles: '3e-local', '3e-CryptoOfficer', and '3e-administrator'. For more information see Section 1.4.1 User Roles and 2.8 Remote Authentication and Authorization.

1.4.1 User Roles

3e-520 series devices permit only '3e-local' roles for local access users (up to ten in local user database). It allows any of three user roles for remotely authenticated and authorized users: '3e-local', '3e-CryptoOfficer', and '3e-administrator'. '3e-local' users have the highest privilege, and can perform all cryptographic configurations for the module, which include: loading digital certificates and private keys for IPsec; configuration of 801.1X supplicant; setting firewall and deep packet inspection policies; create and manage users locally; uploading new firmware and bootloader; setting the password policy and performing self-tests on demand; and performing key zeroization. A '3e-CryptoOfficer' user can perform most functions permitted to '3e-local' minus the ability to create and manage users locally and configure 3e-520 series Remote A&A settings. A '3e-administrator' user has a more reduced set of permitted functions as listed on Table 6 User Role Services below.

The following table describes the 3e-520 series device user roles services, including purpose and functions, details about the service, and user roles:

Table 6: User Role Services

		User Roles		
Service and Purpose	Details	3e-local	3e-Crypto Officer	3e-administrator
Input of Keys	IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS Server.	X	X	
Create and manage users locally	Support up to 10 administrator users and 5 crypto officer users.	X		

		User Roles		
Service and Purpose	Details	3e-local	3e-Crypto Officer	3e-administrator
Configuring Remote A&A	Allow to configure remote A&A parameter	X		
Change password	Administrator changes his own password only.	X	X	X
Show system status	View traffic status and systems log excluding security audit log.	X	X	X
Manage audit logging	Select audit events to be logged. Configure remote audit logging. View audit event records.	X	X	
Key zeroization via reboot		X	X	X
Factory default	Delete all configurations and set device back to factory default state.	X	X	
Perform Self-Test	Run algorithm KAT through reboot.	X	X	X
Load New Firmware	Upload 3eTI digitally signed firmware.	X	X	
SNMP Management	Manage all SNMP settings including SNMPv3 encryption key.	X	X	X
HTTPS Management	Load HTTPS server certificate and private key.	X	X	
Key Generation	Create asymmetric key pairs and X509v3 Certificate Signing Request.	X	X	X

Note: User/roles created locally are independent of user/roles created at Remote A&A Server.

1.4.2 Local User Management

The 3e-520 series devices have a factory default setting of only one '3e-local' user role account enabled with the username 'CryptoOfficer' and a password of 'CryptoFIPS'. When in the factory default state, these credentials can be used to access the device and allow the user to change the default credentials and add new user accounts. When reverting to the factory default state, all user-defined accounts will be deleted and will have to be recreated. The device always requires at least one '3e-local' account to be active. If the user attempts to delete the last '3e-local' account, the user will be informed that this is not possible. When successfully logging in for the first time, every new user will be instructed that his/her password has expired, and he/she will need to enter new credentials before he/she can proceed. All the local User Management functionality is available to '3e-local' over the graphical user interface under the 'User Management' sub-heading on the left side of the screen.

2. Device Configuration

2.1 Quick Setup

In order to begin configuring your device, you will need to perform the following steps (details in the referenced sections):

2.1.1 3e-523N

1) Connect power to the unit:

a) Use a 5-12 VDC power supply (Section 0).

2) Connect your laptop to the Designated Management Interface – Local port:

a) Use a standard RJ-45 Cat6 Ethernet cable (Section 3.1).

3) Log in to the unit (Section 2.2.1):

a) URL: https://192.168.15.1 (requires secure HTTPS, TLS 1.2),

b) Dismiss the certificate warning dialog box,

c) Default Username is "CryptoOfficer" and the default Password is "CryptoFIPS".

4) You can now begin configuring the unit for operation (Section 2.2.2).

2.1.2 3e-525N

1) Connect power to the unit:

a) Connect a PoE injector using the Cat6 Ethernet/PoE cable via WAN port (Section 1.2.2.2).

2) Connect your laptop to the Designated Management Interface – Local port:

a) Use a Cat6 Ethernet cable (Section 4.1).

3) Log in to the unit (Section 2.2.1):

a) URL: https://192.168.15.1 (requires secure HTTPS, TLS 1.2),

b) Dismiss the certificate warning dialog box,

c) Default Username is "CryptoOfficer" and the default Password is "CryptoFIPS".

4) You can now begin configuring the unit for operation (Section 2.2.2).

Figure 14 shows the connections of 3e-525N installation. The UPLINK port is used to connect the unit to the organization's Local Area Network (LAN). For the 3e-525N, the uplink cable is run from the unit to the power injector. This POE power injector connects to Alternating Current (AC) power and provides a port to connect into the wired network. The Local Management port is used to access and manage the device's web management GUI only.

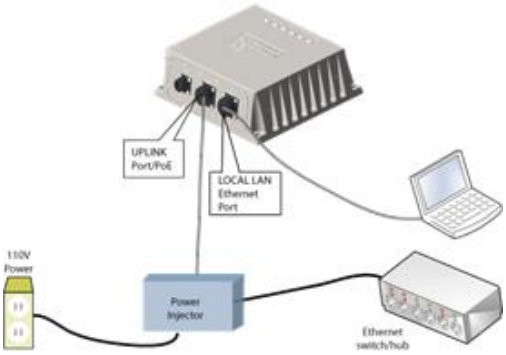


Figure 14: 3e-525N Quick Setup

2.2 Initial Device Configuration

The user can access the device's Web Management UI application either through the dedicated Local Ethernet port or the Uplink (WAN) Ethernet port. The access is identical over IP and HTTPS. For initial access to the device, the user shall use the dedicated Local Ethernet port since the WAN IP is not set up.

2.2.1 Initial Setup

The Designated Management Interface Local port on the unit connects you to the device's internal DHCP server, which will dynamically assign an IP address to your laptop so you can access the device for configuration. In order to connect properly to the unit on the Local (Management) port, the TCP/IP parameters on your laptop must be set as in Figure 15.

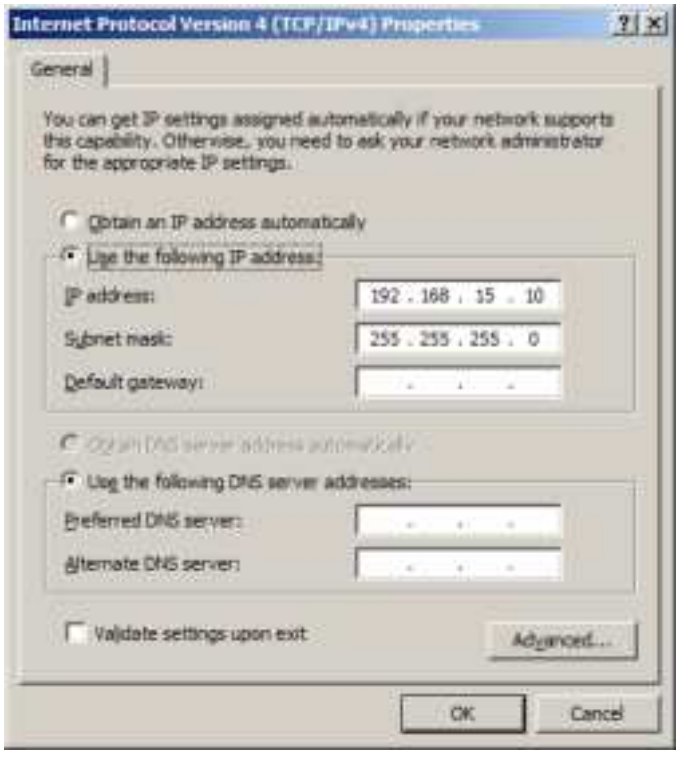


Figure 15: Local PC IP Address Configuration

Plug one end of an Ethernet cable to the Local (Management) port of the device and connect the other end to a RJ-45 Ethernet port on your laptop.

On your computer, pull up a browser window and type in the default Uniform Resource Identifier (URL) for the unit's Local LAN in the address line (https://192.168.15.1). Note that https is required to ensure a secure connection.

1) **Browser Notes:**

   a) SSL 2.0 must be disabled in browser configuration.

   b) The 3e-520 series product supports TLS 1.2, The recommended browser includes:

      i) Microsoft IE version 9 and later,

      ii) Mozilla Firefox version 27 and later,

      iii) Google Chrome 38 and later.

   c) When Two-Factor Authentication is enabled, only Microsoft IE and Edge support CAC authentication.

A warning window appears stating "There is a problem with this website's security certificate." Select and click "Continue to this website (not recommended)" to go to the 3e-520 series login page.

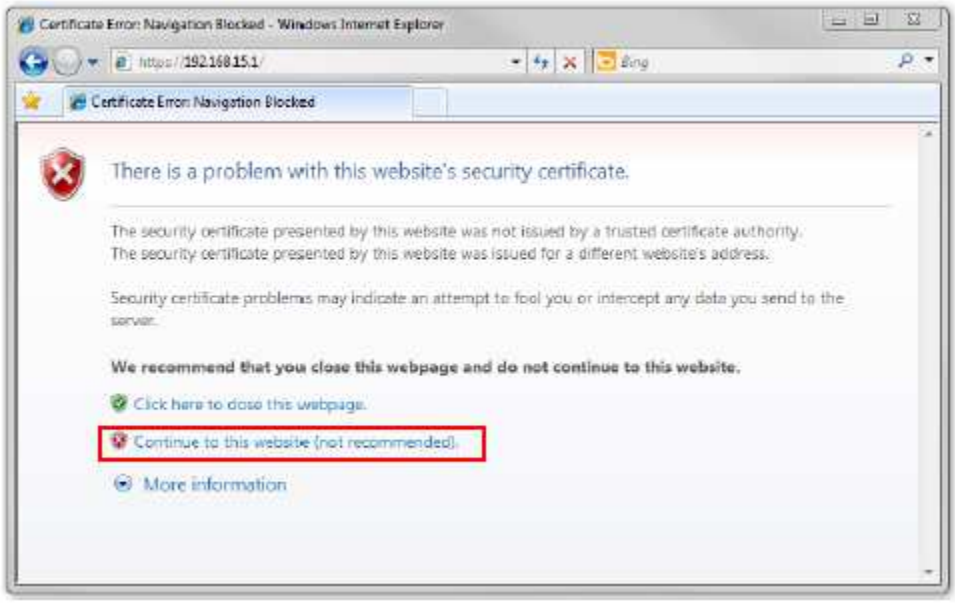


Figure 16: Certificate Error

Next, the **Login** window will appear.

2.2.2 Login

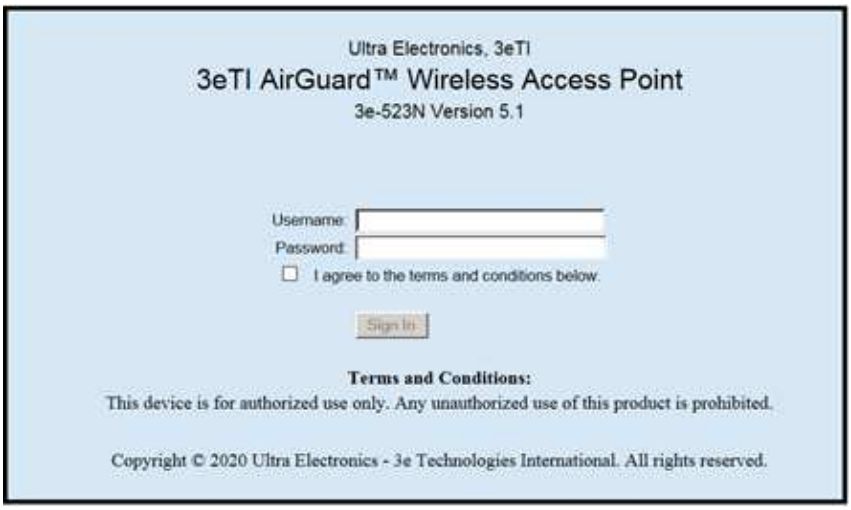


Figure 17: Login Screen

You will be asked for your Username and Password (Figure 18). The default Username is "CryptoOfficer" and the default Password is "CryptoFIPS" to give full access for setup configuration (Username and Password are case-sensitive). Please read the terms and conditions and check the checkbox, then click **Sign In** to continue configuration. Please note that you will be forced to change password after first login.

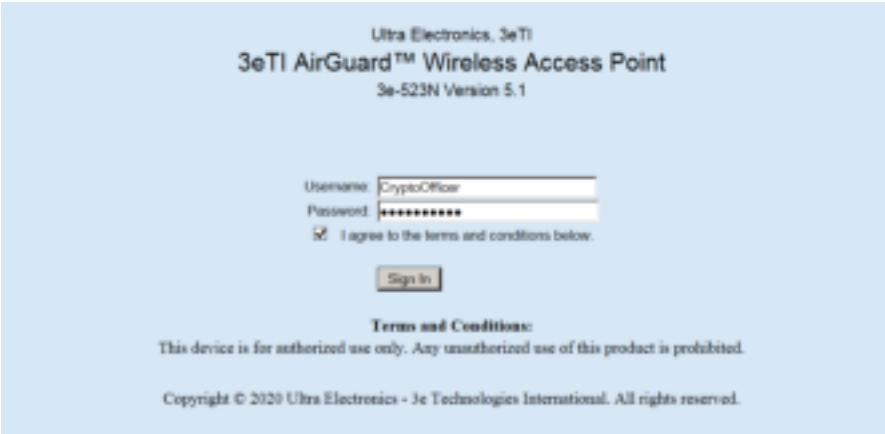


Figure 18: Login Screen with Defaults Username/Password

2.3 System Configuration

2.3.1 Configuration Information

For the initial configuration, the network administrator may need the following information:

- IP address – a list of IP addresses available on the organization's LAN that are available to use for assignment to the devices,
- Subnet Mask for the Uplink network,

- Default IP address of the Local Management port (https://192.168.15.1),
- DNS IP address,
- The MAC addresses of all wireless cards that will be used to access the network,
- The appropriate AES encryption key,
- SSID to identify all members of the WLAN.

Figure 19: Internet Explorer Successful Login Web Page

2.3.2 General

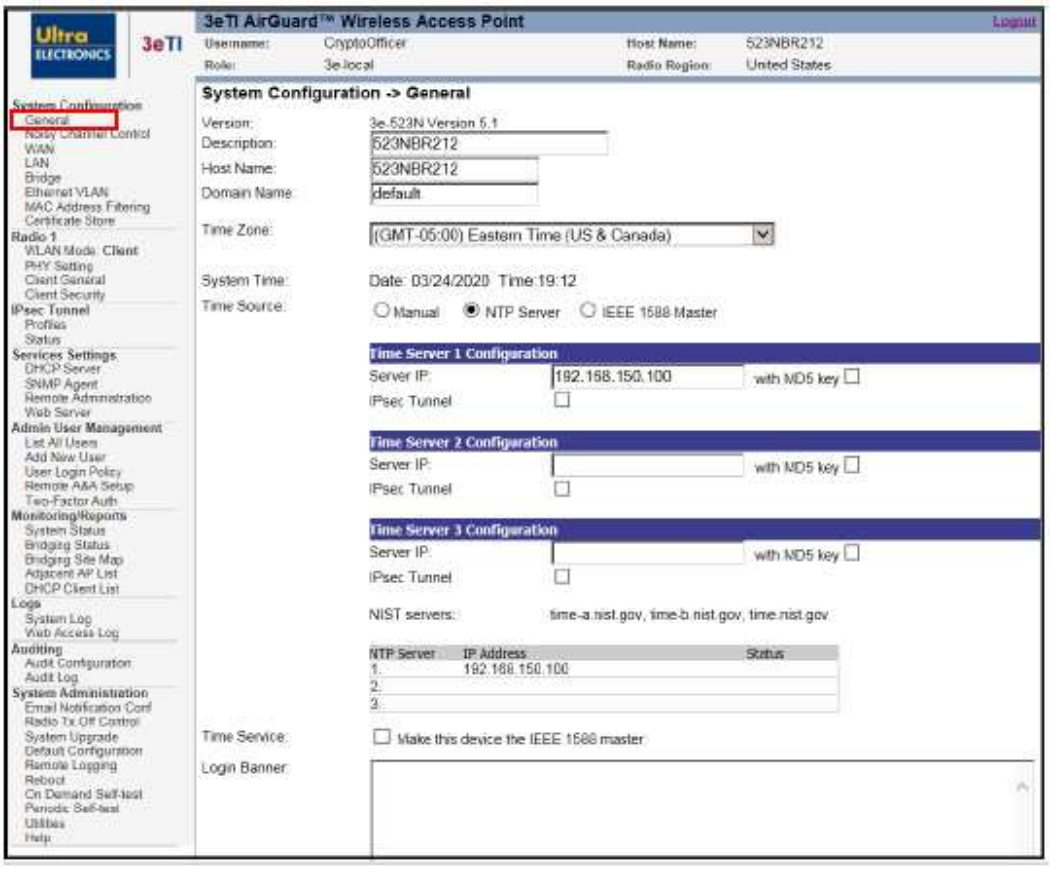


Figure 20: System Configuration – General

You will immediately be directed to the **System Configuration – General** screen (Figure 20). This screen lists the 3e-520 series firmware version number for your unit and allows you to enter a **Host Name, Domain Name,** and **Description** (a description of the physical location of the unit is useful when deploying units to remote locations). Defaults are "default location", "default", and "default" respectively.

You should also select the appropriate **Time Zone** for your location.

NOTE: Only the user with 3e-local and 3e-CryptoOfficer role can set the date and time.

The 3e-520 series is equipped with a real time clock that keeps System Time. This clock can be set manually or can be synchronized with an external time source using the Network Time Protocol (NTP). Set the System Time by selecting the appropriate Time Source radio button on the GUI.

If the System Time is incorrect, you need to modify the **Time Source** (default is Manual):

- **Manual:** Please enter the correct date in MM/DD/YYYY format, and the correct time in 24-hour HH:MM format. The system date must be set to a date later than 01/01/2005.

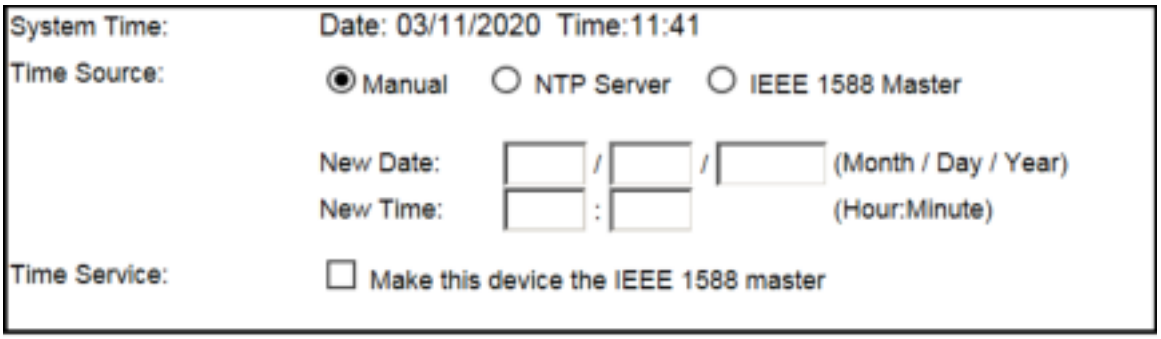


Figure 21: Manual Time Source

- **NTP Server:** Please enter at least one valid IPv4 or IPv6 address; examples are provided for your convenience. The correct time must be set up for X509v3 certificates to work properly, because certificates have a valid time frame associated with them.

  The device supports the NTPv3 protocol. An MD5 HMAC key can be provided when using NTPv3 in order to authenticate each NTP packet. Select the 'NTP Server' in order to synchronize with an external time source.

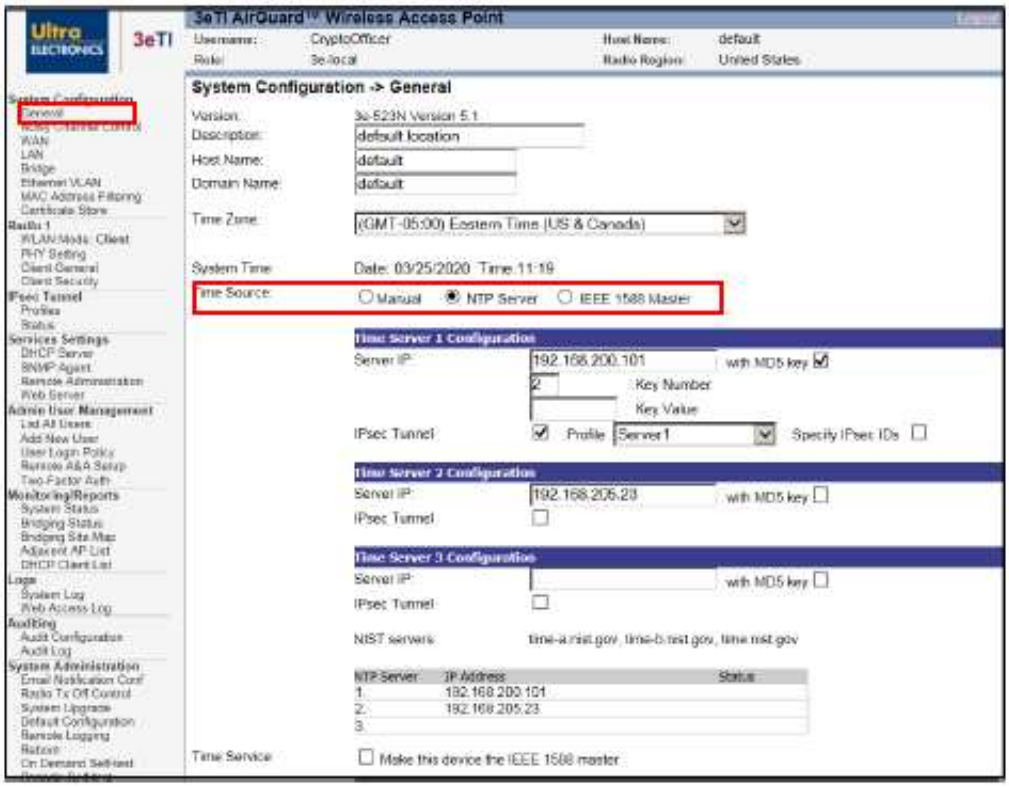


Figure 22: NTP Time Source

While the NTP protocol provides an authentication mechanism, it does not provide for confidentiality. Therefore, the device can be configured to tunnel all NTP packets through an IPsec tunnel. Select the "IPsec Tunnel" check box and provide a "Tunnel Profile" in order to protect time synchronization packets with IPsec.

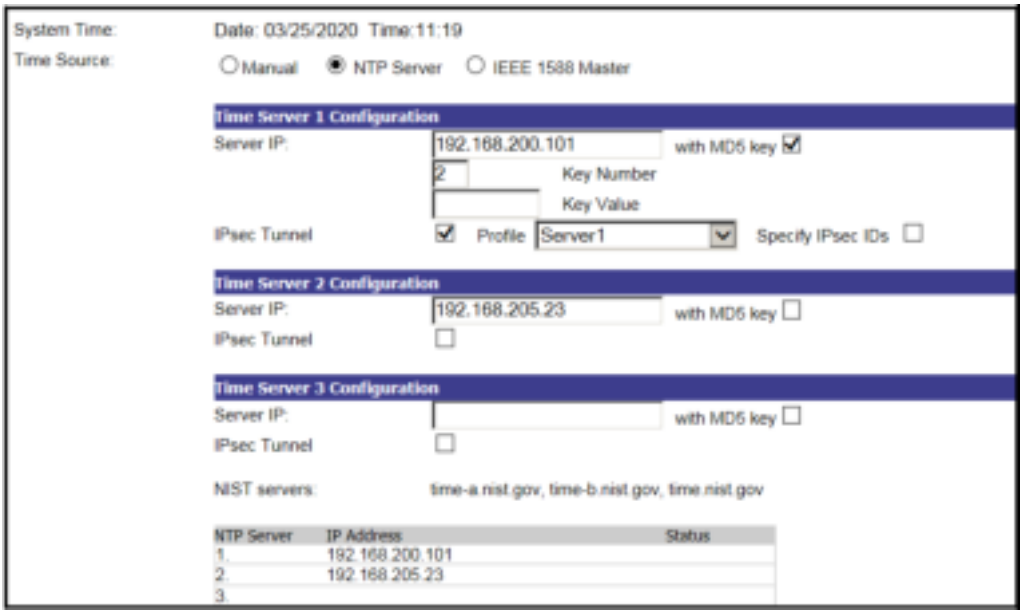


Figure 23: NTP Time Source with IPsec Protection

Note: IPsec Tunnel Profiles must be configured before IPsec can be used to protect NTP packets. See Section 0 in order to configure an IPsec Tunnel Profile.

Note: Compliance with Common Criteria (PPWLAN) requires that all NTP traffic be transmitted within IPsec tunnels.

The 3e-520 series initiates the IPsec protocol when building and IPsec tunnel to an NTP server. During the authentication phase of the protocol, the 3e-520 series (Initiator) will specify to which of the NTP server's (Responder's) identities it wants to communicate with. Most NTP servers will have one IPsec identity bound to the NTP server's IP address. By default, the 3e-520 series will talk to this identity. There are instances where an NTP server may host multiple IPsec identities. In this case, the desired identity can be specified by checking the "Specify IPsec IDs" check box and supplying an IPsec identity.

Note: When selecting an IPsec profile that uses Public Key authentication, the 3e-520 series will validate the supplied IPsec ID against the NTP server's X509v3 certificate. The NTP server's X509v3 certificate must contain the identity as either the subject or one of the subject alternative names.

- **From IEEE 1588 Master:**

  You can select a **Time Source** to be synchronized to an IEEE 1588 Master when one of the 3e-520 series device is designated as the IEEE 1588 Master (Figure 24: **IEEE 1588 Master Time Source & Login Banner**

). IEEE 1588 Time Synchronization is a standard protocol for synchronizing clocks connected via a network to provide fault-tolerant synchronization among heterogeneous networked clocks.

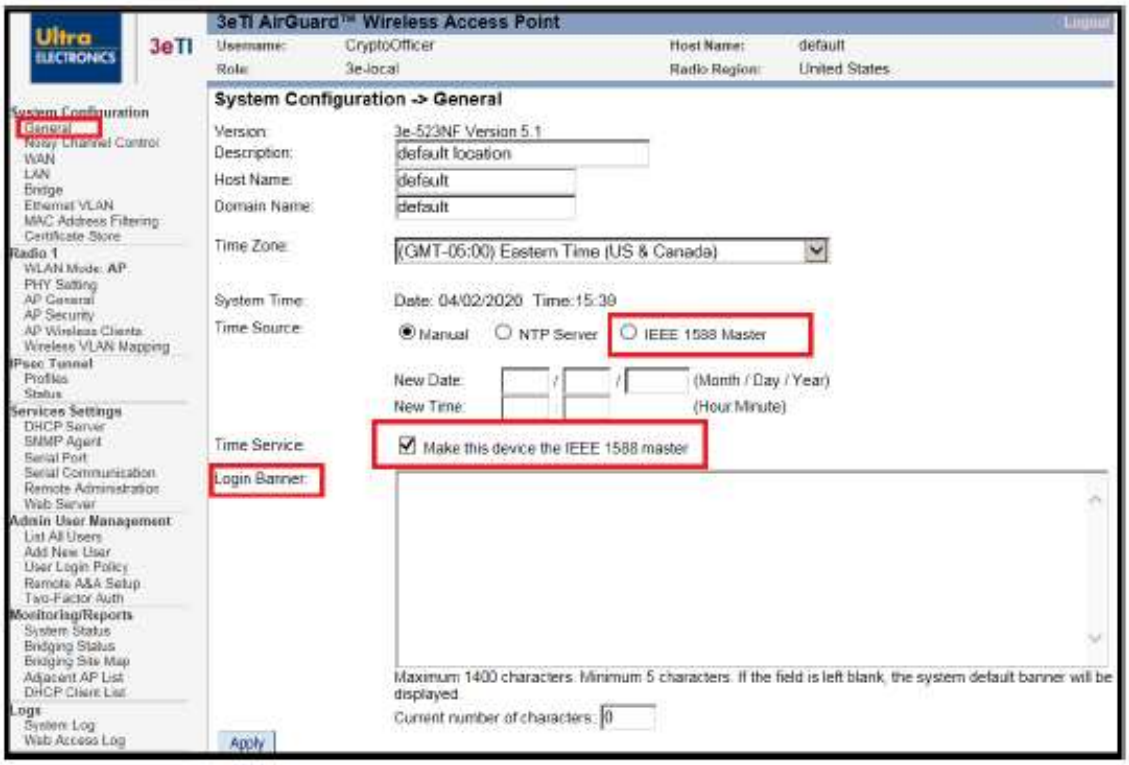


Figure 24: IEEE 1588 Master Time Source & Login Banner

You can modify the terms and conditions in the **Login Banner** which is displayed on the Login screen. The default is **"This device is for authorized use only. Any unauthorized use of this product is prohibited."**

When you are satisfied with your changes, click **Apply**.

2.3.3 Noisy Channel Control

The **System Configuration – Noisy Channel Control** screen (Figure 25) allows the installer the ability to manually eliminate channels from the 802.11 channel list. It provides a convenient listing of recent radar activity for each channel to assist the user. However, we strongly recommend that an RF spectrum site survey be performed to determine potentially noisy or radar-affected channels that should be added to this list.

The channels selected on this screen will not be available for selection when configuring radio channels. Some channels may not be available for selection if Dynamic Frequency Selection (DFS) is required.

NOTE: This noisy channel list persists until it is explicitly removed from the **System Configuration – Noisy Channel Control** screen. The list will not be cleared automatically, even if the device is reset to the "Factory Default" configuration. This configuration applies to the system rather than each radio.

Click **Apply** to confirm your selection.

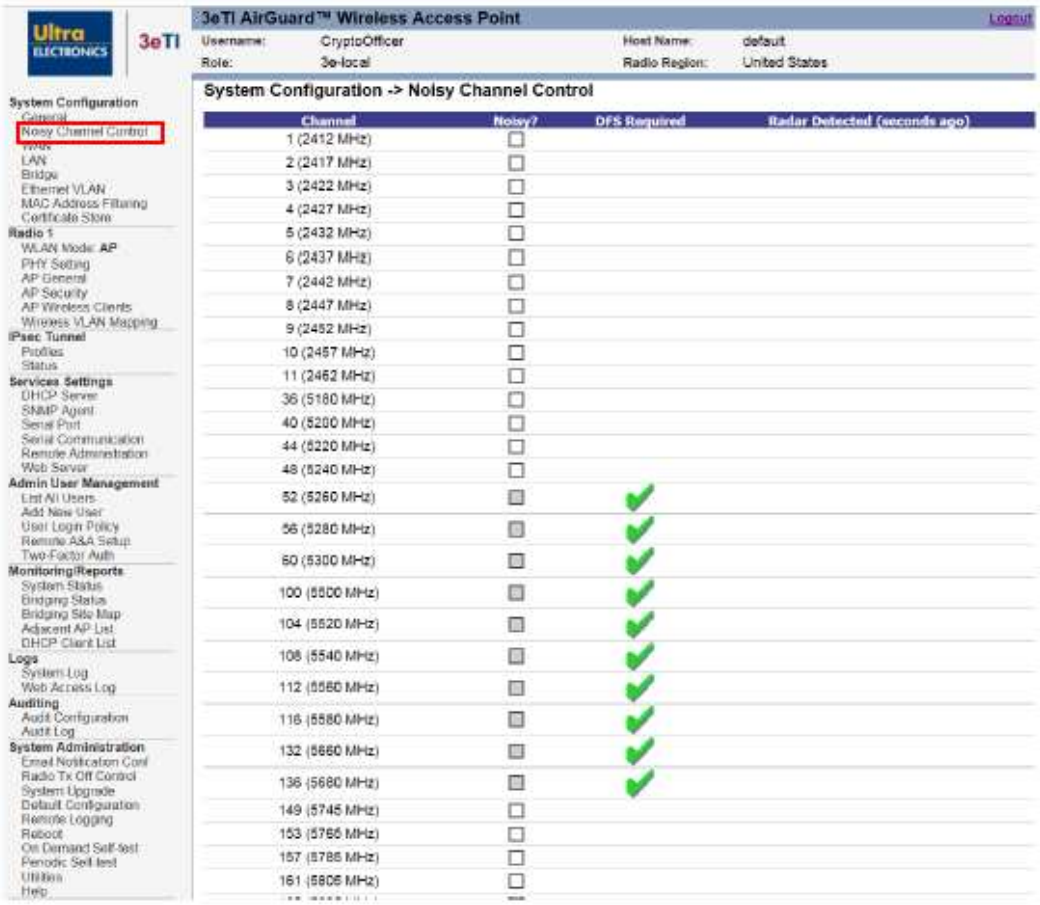


Figure 25: System Configuration – Noisy Channel Control

2.3.4 WAN

The **System Configuration – WAN** screen is shown in Figure 26.

You can select the specific link speed and duplex configuration of the **WAN/LAN Link**. By default, this will be automatically negotiated.

If using an **IEEE 802.1Q VLAN tag** on this port, please enter its value; a value of 0 indicates no VLAN support and is configured by default.

2.3.4.1 IPv4 Address

Unless you are using DHCP to obtain an IP address, you should **Specify a static IP address** in order for the device to be managed from the wired LAN. You will need to specify **IP Address**, **Subnet Mask**, **Default Gateway**, and if necessary, Domain Name System **(DNS) 1 and DNS 2**. Defaults are 192.168.254.254, 255.255.255.0, 192.168.254.1 respectively (with DNS fields blank).

NOTE: After changing the static network address you will no longer be able to access the device from this port using the default IP address. In order to log into the unit through the WAN port, you will need to change the browser URL to reflect the new IP address and log in again.

NOTE: If **Using DHCP to obtain an IP address** is selected, a new IP address will be automatically assigned to the WAN port after clicking **Apply**. In order to log into the unit through the WAN port, the new IP address needs to be obtained. Either contact your Network Administrator, or set up "Remote Logging" (see Section 2.13.5) before configuring the WAN to use DHCP.

Click **Apply** to accept changes.

2.3.4.2 IPv6 Address

IPv6 addresses can be configured disabled, automatically or statically. By default, the IPv6 Addresses is disabled. If **Automatic Configuration** is selected, you can choose to use **Stateless Autoconfiguration** or **DHCPv6**. If you select **Stateless Autoconfiguration**, the device will attempt to configure itself automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages.

NOTE: A 64-bit prefix is required for this configuration.

If IPv6 stateless address autoconfiguration is unsuitable for an application, a network may use stateful configuration with the Dynamic Host Configuration Protocol version 6 (**DHCPv6**).

If **Static Configuration** is selected, you will need to specify **IPv6 Address**, **Default Gateway**, and if necessary, **DNS 1 and DNS 2**. Enter all IPv6 addresses in the standard format of eight groups of four hexadecimal digits separated by colons. An IPv6 address can also be abbreviated with the following standard rules:

- Omit leading zeroes in a 16-bit value.
- Replace one group of consecutive zeroes by a double colon.

Enter a **Prefix Length** appropriate to your application (see RFC 6177 for guidance). It is set to a value of 48 by default.

Click **Apply** to accept changes.

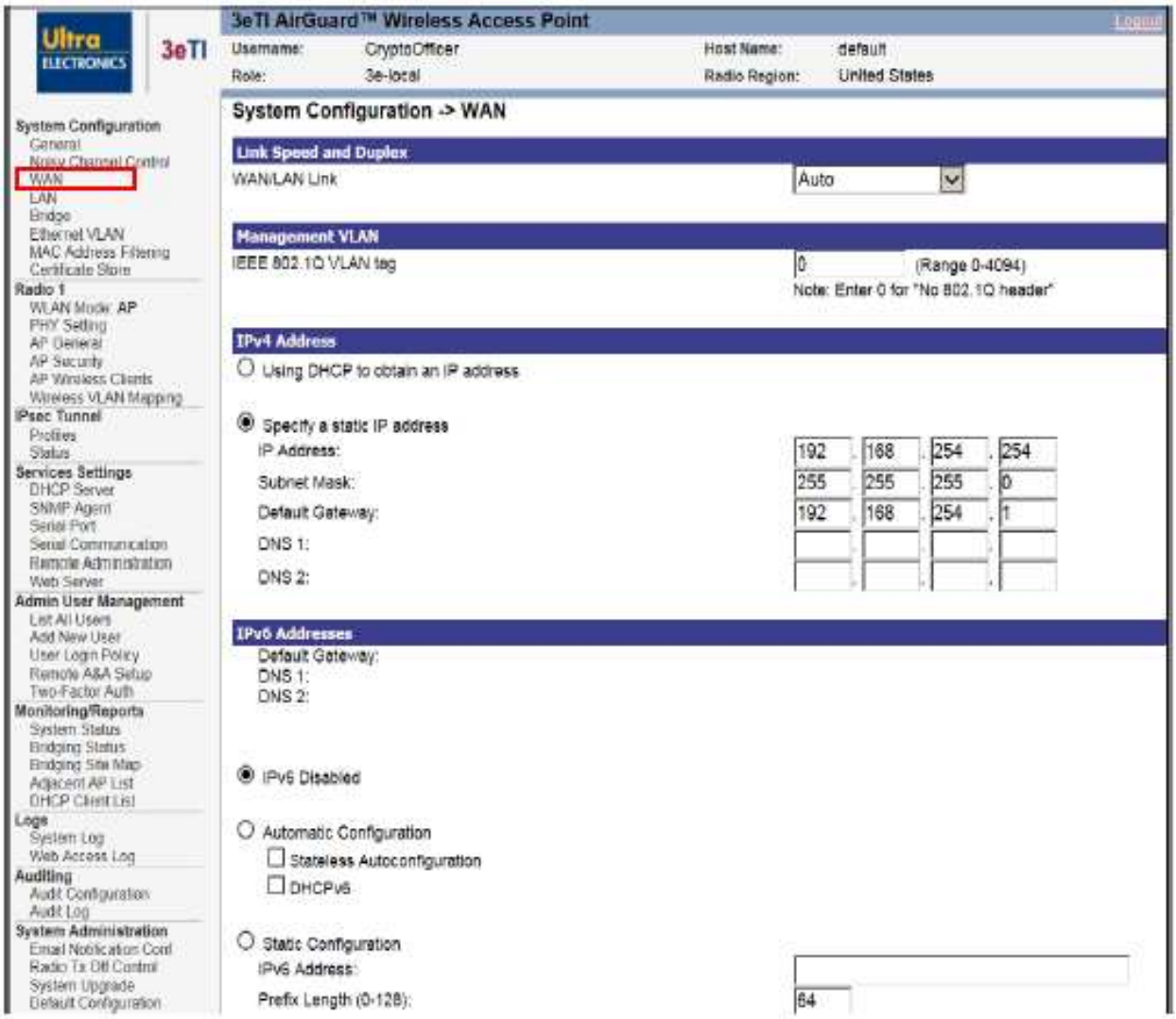


Figure 26: System Configuration – WAN

2.3.5 LAN (Local Management)

The **System Configuration – LAN** (Local Management) screen (Figure 27) configures the **IPv4 Address** and **Subnet Mask** for the Local Management port, which provides local access for configuration (defaults are 192.168.15.1 and 255.255.255.0 respectively). It is not advisable to change the private LAN address during initial setup, or any other time that you wish to remain connected to the Local LAN.

WARNING: The default value for the LAN IP address is 192.168.15.1. Normally this value should not be changed. If the value is changed and forgotten, the user will lose access to the device through the Local Management port.

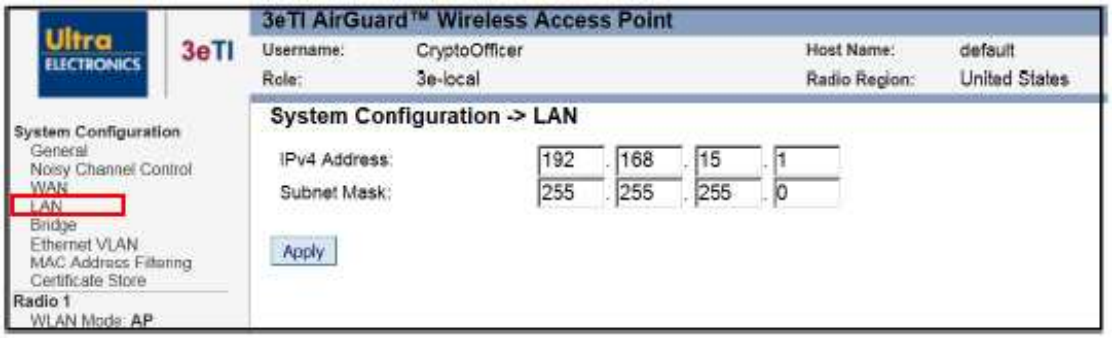


Figure 27: System Configuration – LAN (Local Management)

2.3.6 Bridge

RSTP (Rapid Spanning Tree Protocol) requires each bridge in the network to be assign with a priority index. The bridge with lowest priority index will be assigned as root after the tree topology converges.

The **System Configuration – Bridge** screen (Figure 28) allows you to assign bridge priority to the device. The device's **Bridge Priority** is set to a midrange value (32768) by default. For example, the intended root bridge is assigned a priority of 100, while the rest of mash bridges holds the default priority of 32768.

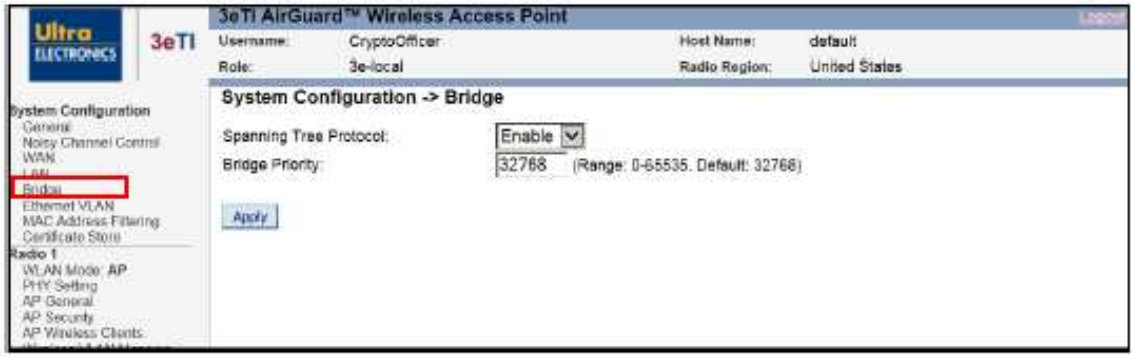


Figure 28: System Configuration – Bridge Priority

2.3.7 Ethernet VLAN

By clicking the link **Ethernet VLAN** under System Configuration, Ethernet VLAN configuration screen will show up. Figure 29 shows the Configuration Screen for Ethernet VLAN configuration.

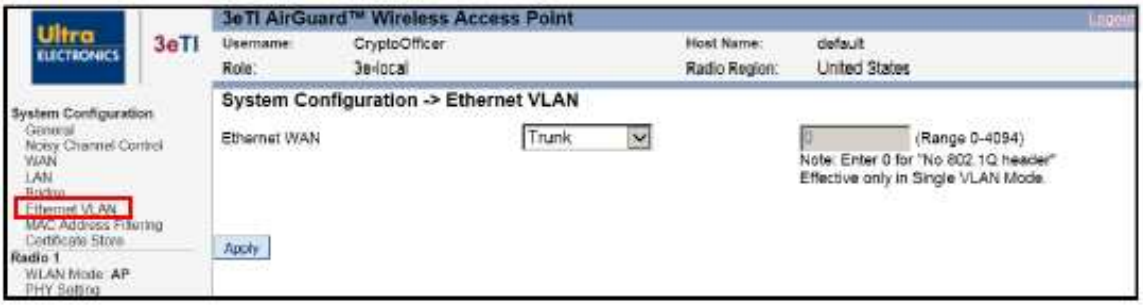


Figure 29: System Configuration – Ethernet VLAN

The WAN Ethernet interface can be configured as VLAN truck or a single VLAN in 3e-520 series as shown in Figure 29. In 3e-523N series, the WAN Ethernet interface is always in VLAN trunk mode. In trunk mode, packets are sent and received unmodified.

2.3.8 MAC Address Filtering

The **System Configuration – MAC Address Filtering** screen (Figure 30) is used to configure MAC address filtering for the unit.

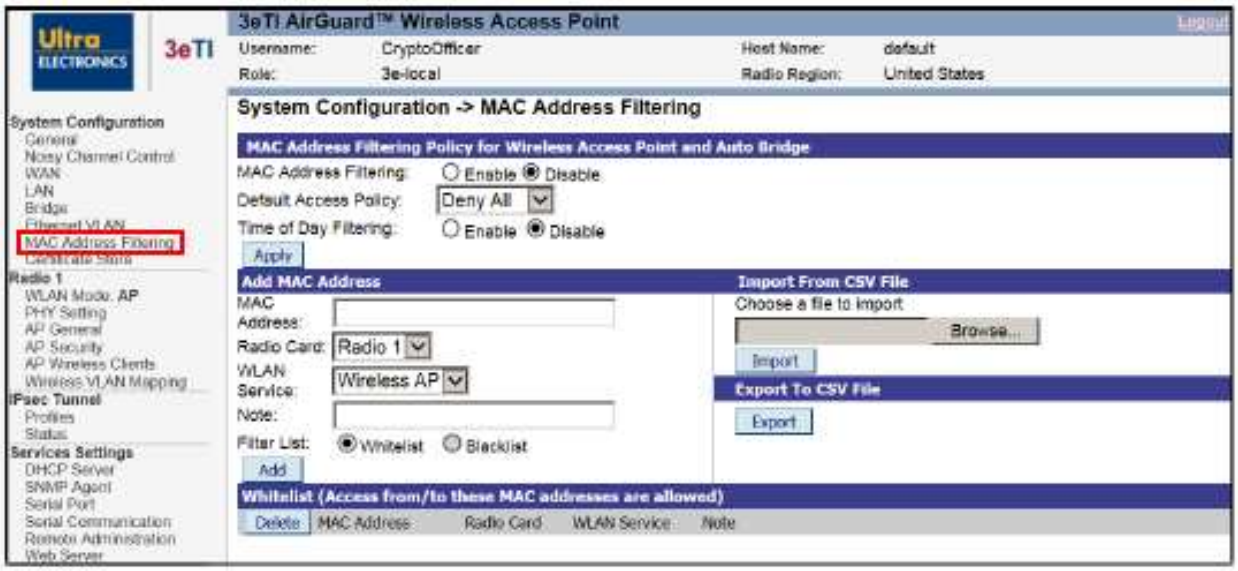


Figure 30: System Configuration – MAC Address Filtering

If **MAC Address Filtering** is Enabled (it is disabled by default) and the **Default Access Policy** is **Deny All** (default), only those devices with a MAC address, which has been entered in the MAC Address listing will be able to communicate with the AP. To configure this **Whitelist**, input the MAC addresses of all the devices that WILL be authorized to access this AP with the **Default Access Policy** set to **Deny All.**

If **MAC Address Filtering** is Enabled and the **Default Access Policy** is **Accept All**, those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the AP. To configure this **Blacklist**, input the MAC addresses of all the devices that will NOT be authorized to access this AP with the **Default Access Policy** set to **Accept All.** Figure 30 depicts a Blacklist where all clients with proper credentials can connect to the AP except the device with MAC address 000B6B560C1F.

To **Add MAC Address** to the filtered list, enter the address in standard IPv4 or IPv6 format. You can select the applicable radio card(s) and WLAN service, then add a note if desired to help document the listing. Each of these settings can be independently configured for each listed address, and is displayed in the list as shown in Figure 30.

Table 7: Add MAC Address Settings			
Settings	**Options**	**Description**	**Default**
Radio Card	All Radio 1 Radio 2	Select the applicable radio(s) for Mac filtering list item.	Radio 1
WLAN Service	Wireless AP Wireless Bridge	Select the applicable WLAN Service Wireless Bridge is available only if **All** radios are selected for filtering.	Wireless AP

Click **Add** to include the selected MAC Address on the list.

You can enter **Whitelist** (default) and **Blacklist** addresses by setting the **Default Access Policy** accordingly while entering each MAC address.

NOTE: that only one list will be active and visible at any time, as determined by the current **Default Access Policy**. If both lists exist, you can select which list to view using the **Filter List** selection.

You may find it useful to go to the **Radio 1** (and/or **Radio 2**) **- AP Wireless Clients** screen and copy the MAC address of selected Wireless Clients, then paste them into the **System Configuration – MAC Address Filtering** screen (Figure 30).

You also have the option to **Import From CSV File** – browse to select a file with MAC Address, Radio Card, WLAN Service and Note fields to be added to the displayed list. At any time, you can also export the displayed list by clicking on the **Export To CSV File** button.

By default, MAC filtering lists are applied 24 hours a day, 7 days a week. By enabling 'Time of Day Filtering', the device will apply the MAC filtering list only during the specified times.

Enable Time of Day Filtering: By enabling Time of Day Filtering, you can select the Day of the week, start and End time to apply the MAC address Filtering rule for Blacklist or Whitelist.

In Figure 31, the Blacklist filter is only applied on Friday. The Start Time and End Time are represented in Coordinated Universal Time (UTC). In the example configuration, the wireless client with MAC address 000B6B560C1F can connect to the AP every day of the week except on Friday.

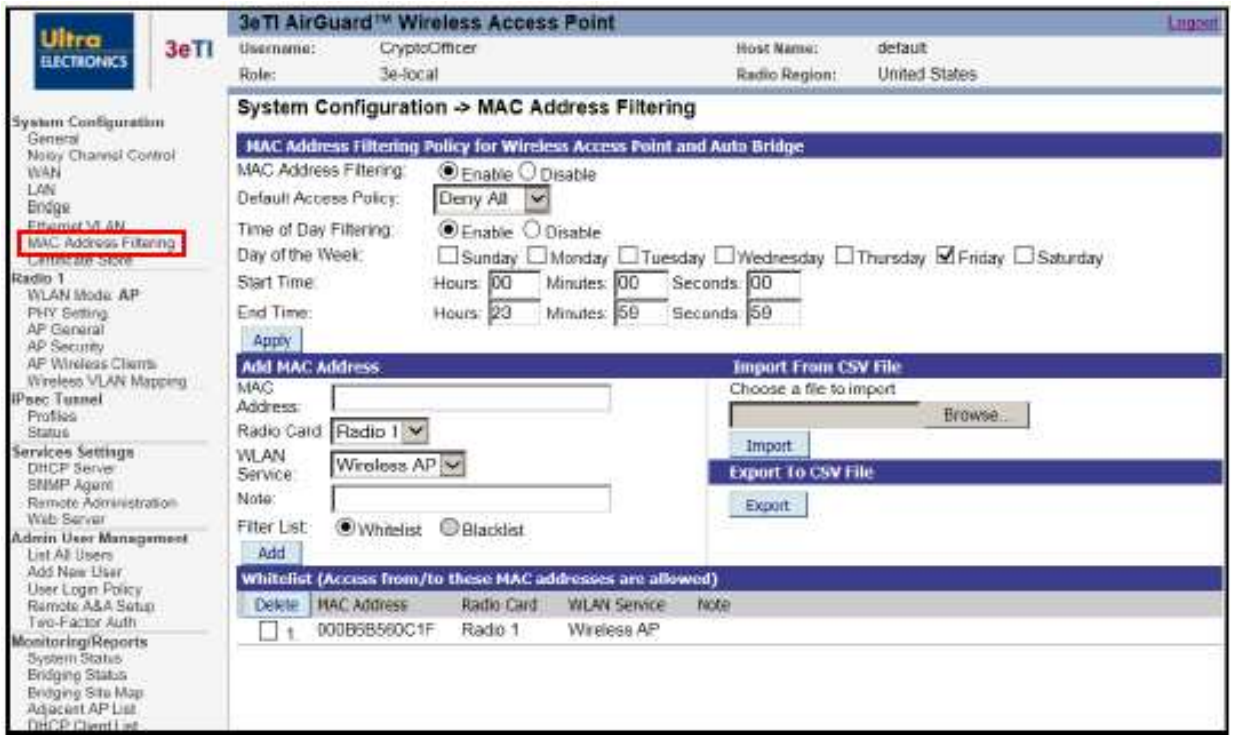


Figure 31: Enable Time of Day for MAC Address Filtering

The Time of Day Filtering works in conjunction with the Access Point Client Session LifeTime (see Section 2.4.4 for details on setting the Client Session LifeTime). When a client is successfully associated with the Access Point, it is afforded the session lifetime independent of the time of day filtering. Only when the session lifetime has expired will the client be asked to re-associate and at that point the time of day filtering will be applied.

2.3.9 Certificate Store

The 3e-520 series devices use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec VPN, Remote User Authentication and web server applications.

Figure 32 shows the **System Configuration – Certificate Store** screen. All certificates used in the 3e-520 series products are centrally managed via the Certificate Store webpage, the certificate store which handles the following certificates:

- Certificate/key for web server https,
- Certificate/key for IPsec credential,
- Intermediate and trusted root certificate to verify peer certificates, e.g., radius server, IPsec peer, LDAP server.

The 3e-520 series devices generate its own public and private key pairs and create a Certificate Signing request (CSR) to apply for a certificate from the Certificate Authority (CA). The certificate returned from the CA can be installed on the device over the management interfaces.

The 3e-520 series devices utilize 3eTI FIPS certified OpenSSL module to generate a CSR with the common identify information (organization name, common name, locality, and country, etc.) and other device-

specific information such as MAC address and IP address when applicable. All CSRs and their associated private keys are centrally stored and managed in the device KeyStore.

If the user is deploying a 3e-520 series device into a system that already has a public key infrastructure and a certificate authority that can only accept CSRs, then the 3e-520 series device can be used to generate the required CSR. The 3e-520 series device produces a PKCS#10 compliant CSR in Base64 encoding.

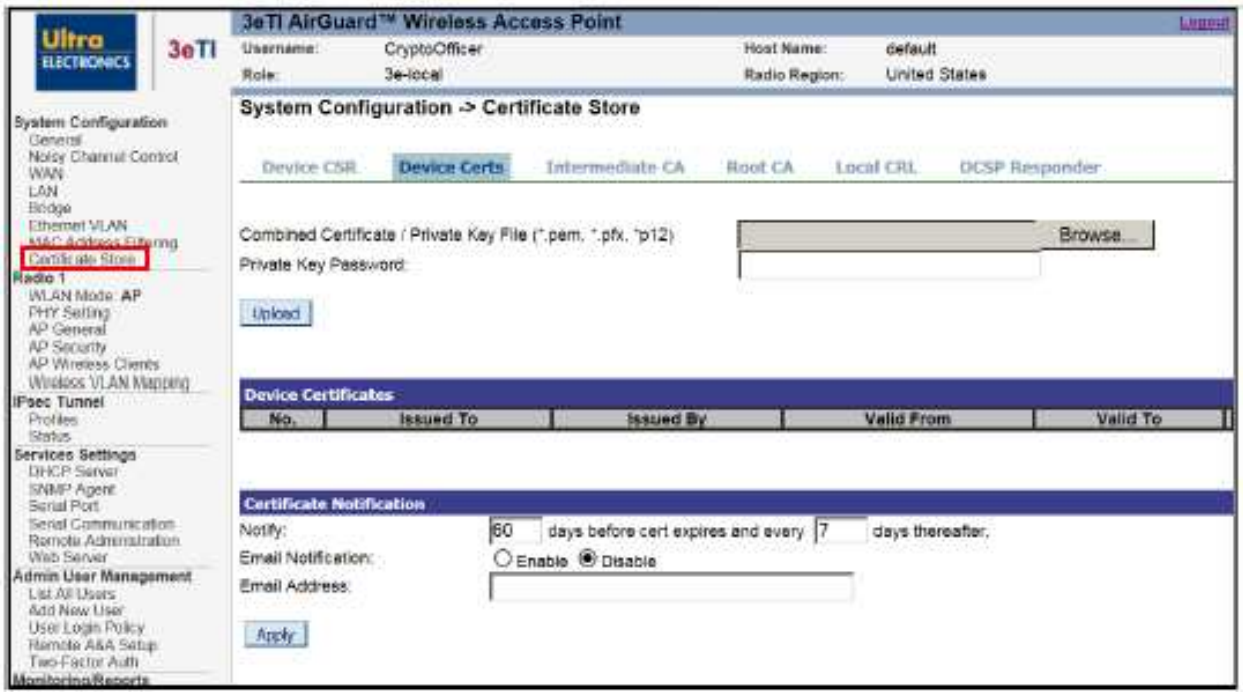


Figure 32: System Configuration – Certificate Store

2.3.9.1 Device CSR

To generate a CSR, click on the **'Device CSR**' tab under the '**Certificate Store**' sub-heading on the left side of the screen. Fill in the appropriate details and click '**Apply**'

A CSR is generated by an applicant when applying for a digital identity certificate to a Certificate Authority (CA). The 3e-520 series device generates a block of encoded text containing the information that will be included in a certificate such as organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. A private key is also created at the time the CSR is generated; this key can be exported separately but will not be included in the CSR itself.

A PKI's certificate authority will be able to sign the CSR, which can then be loaded back into the 3e-520 series device, along with the associated private key.

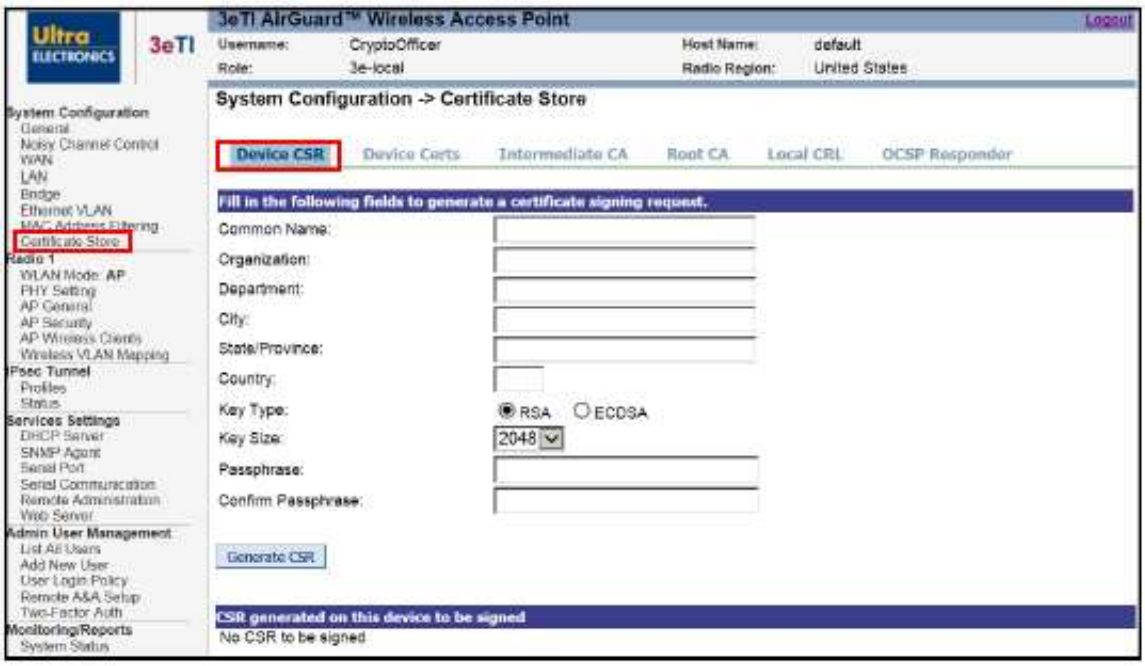


Figure 33: Certificate Store Device CSR

Note: The CSR feature will rarely be used since most institutions will load their own certificates generated by their CAs.

Note: The following characters are not allowed in the Common Name field:

<>~!@#$%^*/()? ,&

Characters <>~!@#$%^*/()?.,& are not allowed in the Organization, Department, City, State/province, and Country fields.

Common Name: Enter a fully qualified domain name.

Organization: Full legal name of your organization.

Department: Name of department.

City: The city where organization is located.

State/Province: The state or province where your organization is located. This should not be abbreviated.

Country: The two-letter ISO code for the country where your organization is located (e.g., US, GB, FR, etc.).

Key Type: Select from RSA or ECDSA options.

Key Size: Select from 2048 or 4096 options.

Passphrase: Enter an alphanumeric passphrase (0-128 characters long).

Confirm Passphrase: re-enter passphrase.

Once all information has been entered correctly on the CSR page, press the 'Generate CSR' button. The new CSR will be displayed under the 'CSR generated on this device to be signed' section of the screen. It

will display confirmation of CSR generation; from here the user is offered options to 'View CSR', 'Export CSR', and 'Delete CSR', as well as an option to upload a signed certificate.

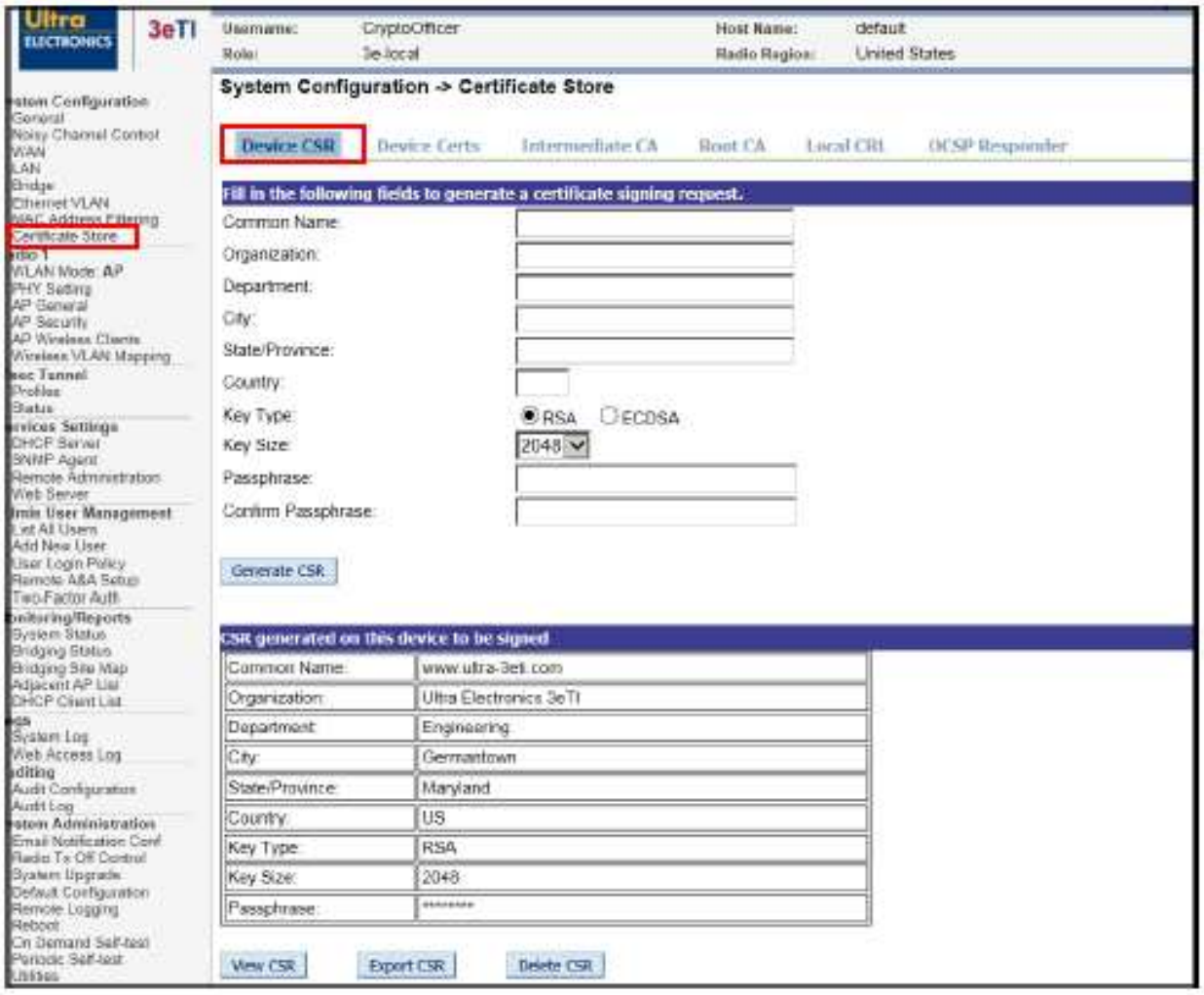


Figure 34: CSR Generation

2.3.9.2 Device Certs

The Device Certs page allows users to upload combined certificate/private key to the 3e-520 series device. The certificate/private key file must be in the *.pem, *.pfx or *.p12 formats. The page lists certificates uploaded to the 3e-520 series device. To view a list of certificates in store click on the Device Certs tab in the Certificate Store page.

This page also allows user to view the contents of a certificate or delete a particular certificate altogether.

You can also enable the Email Notification to notify CryptoOfficer in the email address with preset days before the certificate is expired.

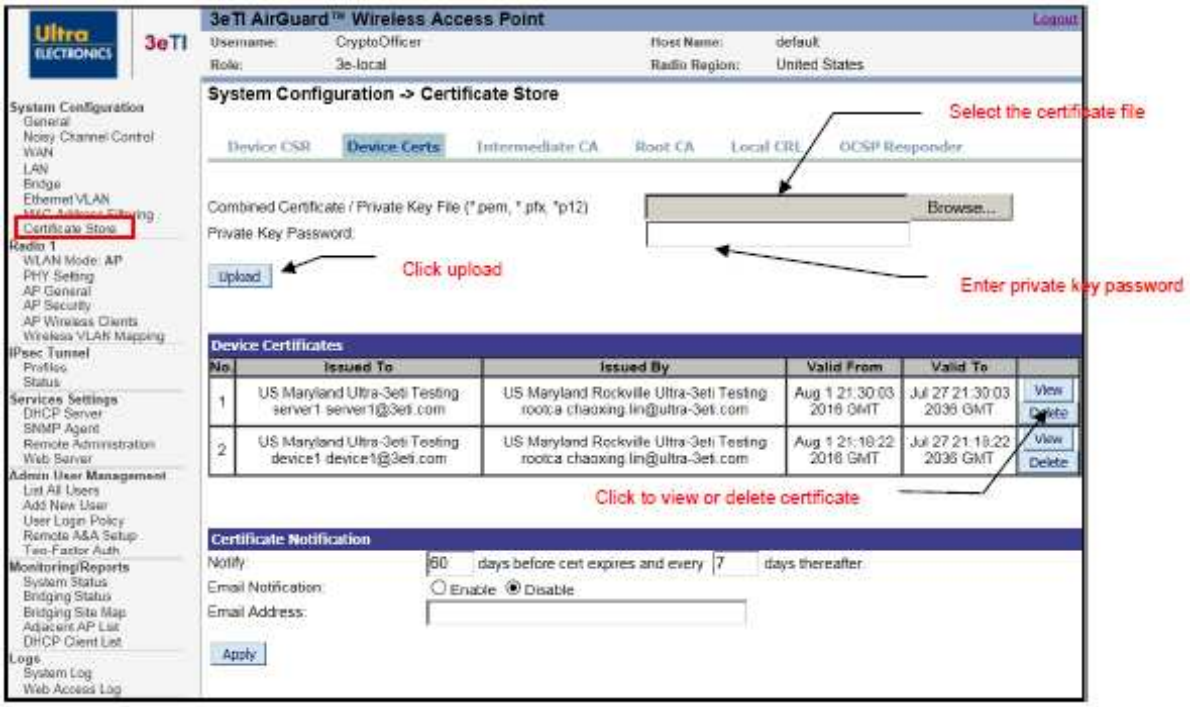


Figure 35: Device Certs

2.3.9.3 Intermediate CA

The Intermediate CA page allows users to upload Intermediate CA certificates to the 3e-520 series device. The certificates can be in the *.pem, or *.der format. The page lists certificates uploaded to the 3e-520 series device. To view a list of certificates in store click on the Intermediate CA tab in the Certificate Store page.

This page also allows user to view the contents of a certificate or delete a particular certificate altogether.

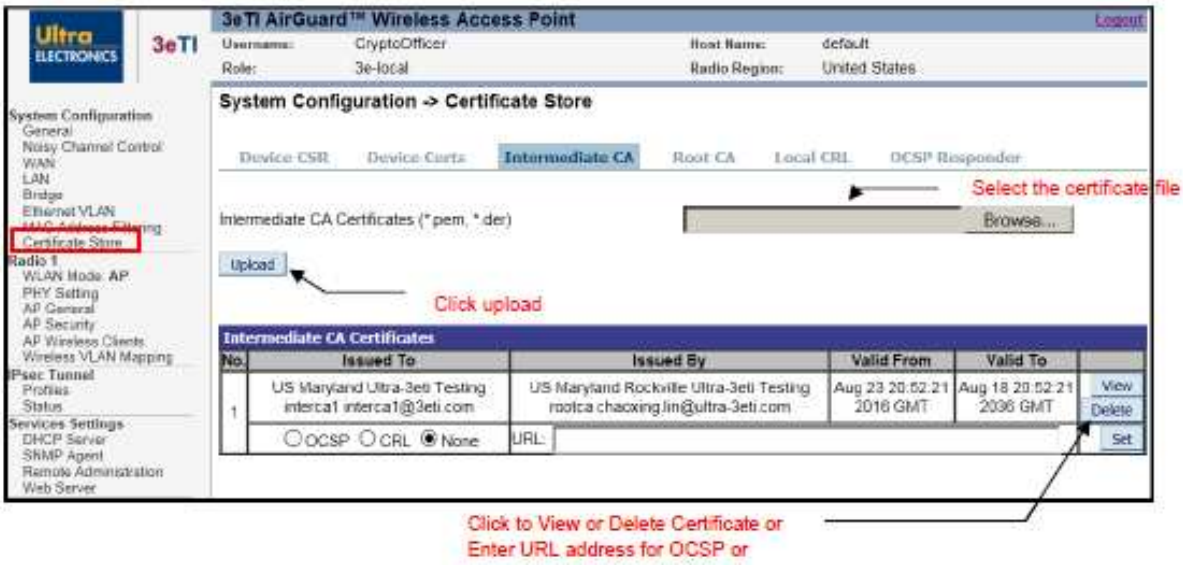


Figure 36: Intermediate CA Certificate Upload

2.3.9.4 Trust Root CA

The Trust Root CA page allows users to upload Trust Root CA certificates to the 3e-520 series device. The certificates can in the *.pem, or *.der format. The page lists certificates uploaded to the 3e-520 series device. To view a list of certificates in store click on the Trust Root CA tab in the Certificate Store page.

This page also allows user to view the contents of a certificate or delete a particular certificate altogether.

Figure 37: Trust Root CA

2.3.9.5 Local CRL

The Local CRL page allows users to upload Local CRL certificates to the 3e-520 series device. The certificates can be in the *.pem, or *.der formats. The page lists certificates uploaded to the 3e-520 series device. To view a list of certificates in store click on the Local CRL tab in the Certificate Store page. This page also allows user to view the contents of a certificate or delete a particular certificate altogether.

Figure 38: Local CRL

2.3.9.6 OCSP Signer

The OCSP Signer tab allows users to upload OCSP Signer certificates to the 3e-520 series device. The certificates can be in the *.pem, or *.der formats. The page lists certificates uploaded to the 3e-520 series device. To view a list of certificates in store click on the OCSP Signer tab in the Certificate Store page. This page also allows user to view the contents of a certificate or delete a particular certificate altogether.

Figure 39: OCSP Signer

2.4 3e-520 Series Radio Configuration

2.4.1 Introduction

The radios of the 3e-520 series can be configured as Access Point, Mesh Access Point, Mesh Point or Client modes.

2.4.1.1 Access Point Mode

When a radio is configured as Access Point mode, the radio allows other Wi-Fi client devices to connect to a wired network. The uplink of the AP can be connected to a router for wired network. In Access Point mode, the AP interface can be configured to map up to 8 VLANs. Each VLAN is mapped to one SSID. Packets in the air between AP and wireless clients contain no VLAN tag. Packets from a wireless client associated with a given SSID are tagged by the AP, according to the configured mapping between SSID and VLAN. The VLAN tagging happens after the packets are received by the radio. VLAN tags in packets sent to wireless clients are removed by the AP before packets are transmitted to wireless clients.

2.4.1.2 Mesh Access Point Mode

When a radio is configured as Mesh Access Point mode, the radio acts as a bridge interface which can be bridged into a Mesh network. It also acts as an AP interface which allows Wi-Fi client devices association with the same SSID and encryption key.

2.4.1.3 Mesh Mode

When a radio is configured as Mesh Mode, the bridge interface always acts as VLAN trunk. Packets in and out of bridge are sent unmodified, so there are no VLAN-related configurations for the bridge interface.

2.4.1.4 Client Mode

When a radio is configured as Client Mode, the radio interface acts as a Wi-Fi client device. It will scan the available APs and connect to the nearest AP which has the same SSID and encryption key as configured.

2.4.1.5 WAN Interface

The WAN Ethernet interface can be configured as VLAN truck or a single VLAN in the 3e-525N series. In 3e-523N series, WAN Ethernet interface is always in VLAN trunk mode. In trunk mode, packets are sent and received unmodified. Refer to Section 2.3.7 for WAN VLAN configuration.

2.4.1.6 Web Management Interface

Web management traffic can come from a Local Management port or a non-local port on the management VLAN. Refer to Section 2.3.7 for management VLAN configuration.

2.4.2 Radio WLAN Mode Configuration

The **Radio – WLAN Mode** screen (Figure 40: Radio – WLAN Mode) allows you to set the operating mode to one of the following:

- Access Point,
- Mesh Access Point,
- Mesh Point,
- Client.

NOTE: For devices like the 3e-525N, which has two radios, each radio needs to be configured separately.

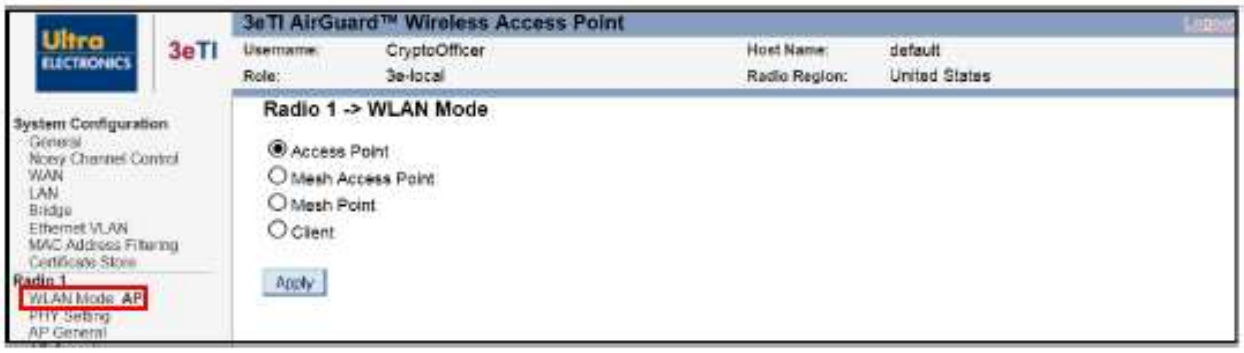


Figure 40: Radio – WLAN Mode

2.4.3 Radio PHY Setting Configuration

The **Radio – PHY Setting** link is used for configuration of the radio's Physical Layer (PHY) parameters.

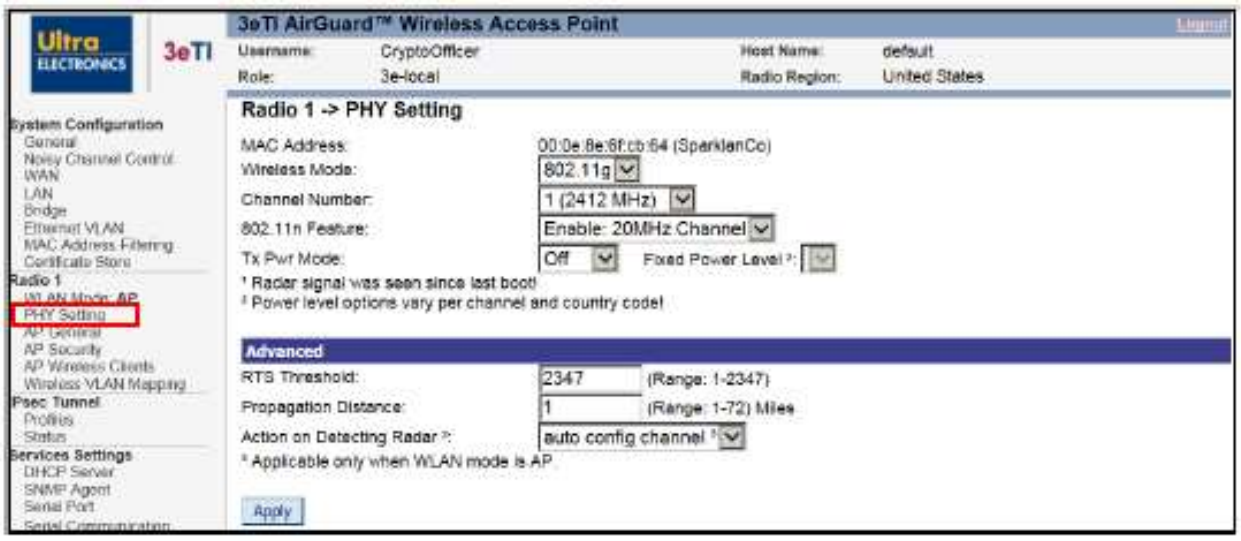


Figure 41: Radio 1 – PHY Setting

2.4.3.1 Wireless Mode

Select the wireless mode from the drop-down list. You can choose from the following options:

- 802.11a,
- 802.11g.

See Section 2.4.3.3 to configure 802.11n.

Note: The 3e-523E-900 product uses only 802.11b mode, restricted channels, translated into the 902-928MHz range, and restricted Tx Pwr Mode settings. It is not possible for the user to select modes, channels, or transmit power settings other than what is described in Appendix D.

See Appendix D. for specific details regarding the 3e-523E-900.

2.4.3.2 Channel Number

Table 8 shows all the channel numbers in frequency band for 802.11g and 802.11a. When multiple APs are used in the same area, it is important not to assign adjacent channels to these APs. For example, assigning channels 1, 6 and 11 to three APs will keep the transit frequencies of the three APs widely separated. This will reduce the interference between the access points.

NOTE: The country code may restrict the channels available for selection.

See Appendix D. for specific details regarding the 3e-523E-900 operation

Table 8: Frequency Channel Numbers	
Wireless Mode	**Channel No.**
802.11g	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)
802.11a	36 (5.18 GHz) 40 (5.2 GHz) 44 (5.22 GHz) 48 (5.24 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)
NOTE: Actual available channels vary based on each country's RF regulations. The channels above are only available and do not require DFS detection in the U.S.	

2.4.3.3 802.11n Feature Setting

802.11n can be set to:

- Disabled,
- Enable 20 MHz channel,
- Enable 40- MHz channel,
- Enable 40+ MHz channel.

40- MHz option is to bundle channel with lower frequency band. **40+ MHz** option is bundle channel with higher frequency band.

2.4.3.4 Transmit Power Settings

The Transmit (Tx) Power (Pwr) Mode (**Tx Pwr Mode**) can be set to Off, Fixed and Auto (it set to Off by default). Setting the Tx Pwr mode in Auto giving the largest range of radio transmission available under normal conditions. As an option, the AP's broadcast range can be limited by setting the **Tx Pwr Mode** to fixed and choosing a **Fixed Power Level** from 1 to 6 (1 being the lowest power and shortest distance).

If you want to prevent RF transmission, set **Tx Pwr Mode** to off. This will not turn off RF transmissions from any associated wireless devices, but they will not be able to communicate with the device when the **Tx Pwr Mode** is off.

See Appendix D. for specific details regarding the 3e-523E-900 operation

2.4.3.5 RTS Threshold

The Request to Send (RTS) Threshold is the number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.

2.4.3.6 Propagation Distance

Propagation distance is an estimate of the radio distance to the nearby devices. It is used to estimate propagation delays between devices. It will not affect the device's transmitter power and therefore affect the distance of reachability.

2.4.3.7 Dynamic Frequency Selection (DFS) Configuration

DFS is a spectrum-sharing mechanism that allows wireless LANs (WLANs) to coexist with radar systems. It automatically selects a frequency that does not interfere with certain radar systems while operating in the 5 GHz band. In 3e-520 series, when radar signal is detected, the access point can be configured to either to select a different frequency band or to stop Wi-Fi transmission.

2.4.4 Access Point Configuration

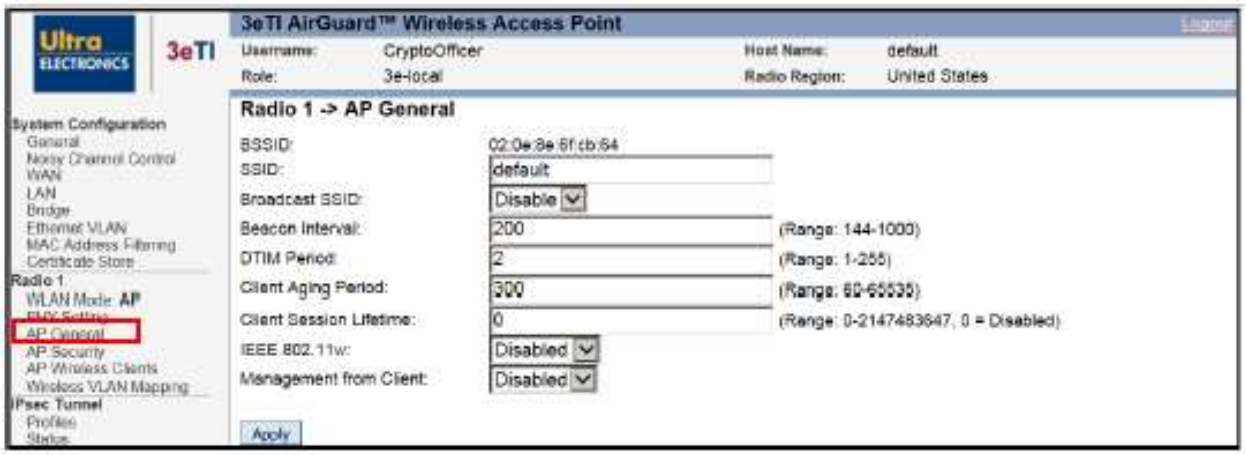


Figure 42: Radio – AP General

2.4.4.1 AP General

The **AP General** settings options included on this screen are shown in Figure 42 and described further in Table 9.

NOTE: These settings should ONLY be changed by a professional installer.

Table 9: Radio Settings		
Settings	**Options**	**Description**
Broadcast SSID	Enabled/disabled	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the AP does not send probe responses to probe requests with unspecified SSIDs.
Beacon Interval	144-1000 (TU)	The time interval in time unit (TU) which the 802.11 beacon is transmitted 1 TU = 1.024 milliseconds.
DTIM	1-255	The number of beacon intervals that broadcast and multicast traffic is buffered for a client in power save mode.
Client Aging Period	0-65535 (seconds)	If the client is inactive for the period specified than it will be dissociated.
Client Session Lifetime	0-2147483647 (seconds)	The time a client session will last. After a client session lift time, a client will need to re-associate with the AP again.
IEEE 802.11w	Disable /Optional /Required	Disable: only accept client with 802.11w disabled. Optional: accept client with 802.11w either enabled or disabled Required: only accept client with 802.11w enabled.
Management from Client	Disabled / Enabled	Disabled: Wireless clients are prevented from accessing the Management (WEB) interface. Enabled: Wireless client can access the Management (WEB) interface. Default is Disabled.

NOTE: For backward compatibility, when a 3e-525N AP is deployed together with old 3e-525A-3 APs, the 802.11w needs to be disabled.

2.4.4.2 AP Security

Figure 43: Radio – AP Security

The **Radio – AP Security** screen (Figure 43) displays a default factory setting of no encryption (Key not Set), for security reasons the unit will not communicate with any clients unless the encryption is set.

2.4.4.2.1 FIPS 802.11i

For the 802.11i setting, you must enable either PSK Settings or 802.1x (RADIUS) Settings. If you do not plan on deploying a RADIUS server, PSK mode is the security mode.

2.4.4.2.1.1 Pre-shared Key with Passphrase or Master Key

The pre-shared key can be of the following format:

- Pre-Shared Key with Master key: 64 hexadecimal digits,
- Pre-Shared Key with Passphrase: 8-63 bytes of characters are composed of any combination of upper- and lower-case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

2.4.4.2.1.2 Encryption Suite and Re-keying

Re-keying time is the frequency in which new encryption keys are generated and distributed to the client. The more frequent re-keying, the better the security. For highest security, select the lowest re-keying interval. Once you have selected the options you will use, click **Apply**.

2.4.4.2.2 802.1X / RADIUS (Common Criteria Compliant Mode)

If a RADIUS Server will be used, select 802.1x and input the Primary RADIUS Server and Request for Comments (RFC) Backend security settings. Use of a RADIUS Server for key management and authentication requires that you have installed a separate certification system, and each client must have been issued an authentication certificate.

Table 10: 802.1X Configuration	
Fields	**Directions**
RADIUS Server Type	Select the RADIUS server type between: IETF and 3eTI. IETF is the default
Primary RADIUS Server IP Address	Enter Primary RADIUS Server IP Address
Backup RADIUS Server IP Address	Enter Backup RADIUS Server IP Address
Shared Secret	Enter Share Secret for the RADIUS Sever with minimum 10 characters.
Backend Password	Enter Backend Password
Backend Key	Enter Backend Key in 32 hexadecimal digits
Backend Key again	Re-enter the Backend Key

The 3e-520 series can provide increased protection of the communication with the RADIUS authentication server by configuring an IPsec tunnel with the authentication server over which the RADIUS protocol will travel. Click the IPsec Tunnel check box and provide an IPsec Tunnel Profile in order to protect RADIUS communication with IPsec.

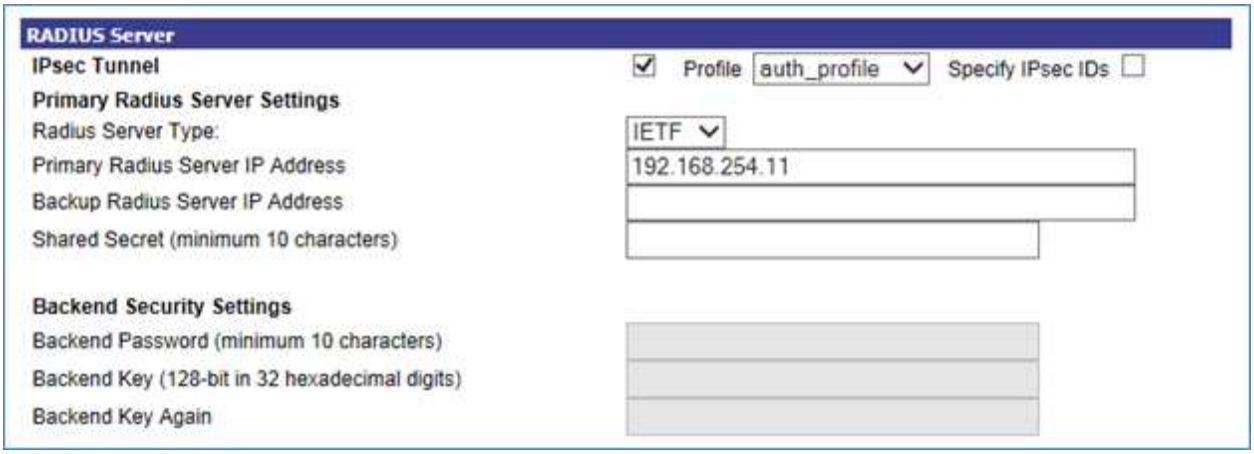


Figure 44: RADIUS Configuration with IPsec Protection

Note: IPsec Tunnel Profiles must be configured before IPsec can be used to protect RADIUS packets. See Section 0 in order to configure an IPsec Tunnel Profile.

Note: Compliance with Common Criteria (WLANEP) requires that all RADIUS traffic be transmitted within IPsec tunnels.

The 3e-520 series initiates the IPsec protocol when building and IPsec tunnel to a RADIUS server. During the authentication phase of the protocol, the 3e-520 series (Initiator) will specify to which of the RADIUS server's (Responder's) identities it wants to communicate with. Most RADIUS servers will have one IPsec identity bound to the RADIUS server's IP address. By default, the 3e-520 series will talk to this identity. There are instances where a RADIUS server may host multiple IPsec identities. In this case, the desired identity can be specified by checking the "Specify IPsec IDs" check box and supplying an IPsec identity.

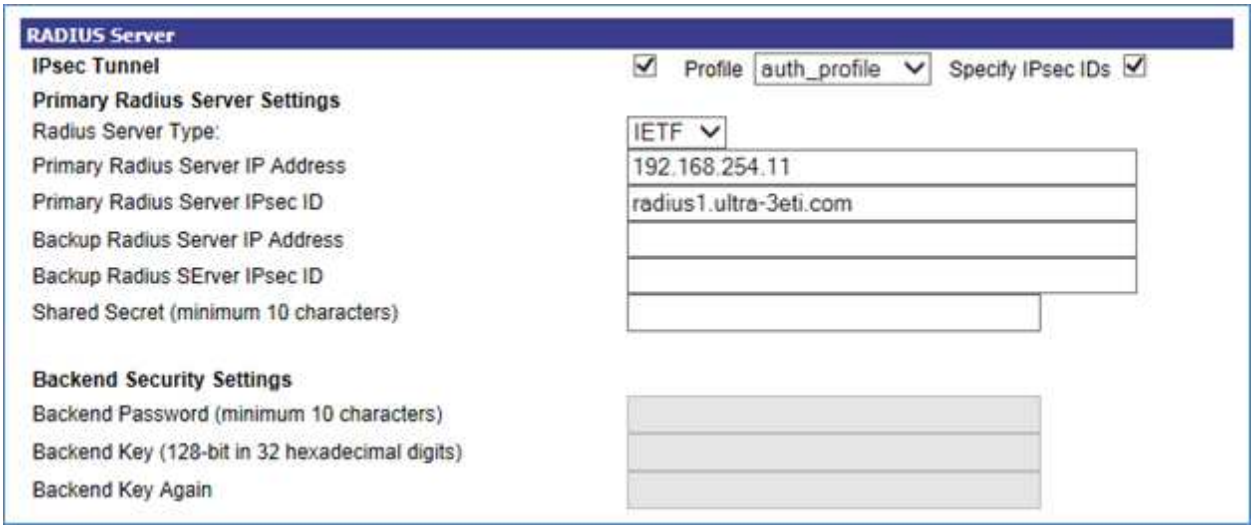


Figure 45: RADIUS Configuration with IPsec ID

Note: When selecting an IPsec profile that uses Public Key authentication, the 3e-520 series will validate the supplied IPsec ID against the RADIUS server's X509v3 certificate. The RADIUS server's X509v3 certificate must contain the identity as either the subject or one of the subject alternative names.

After all the fields are entered correctly, click on the **Apply** button.

2.4.4.3 Access Point Wireless Clients

The **Radio – AP Wireless Clients** screen (Figure 46) shows the clients that are currently associate to the AP for that radio. Please note that the device will support up to 64 wireless clients per AP radio interface.

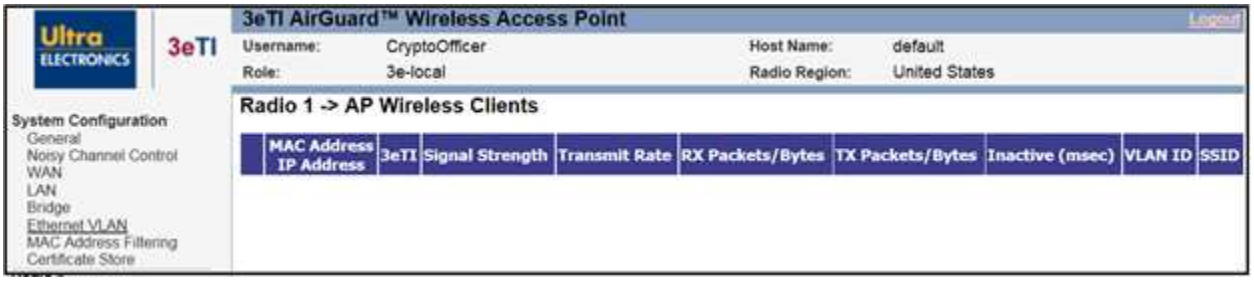


Figure 46: Radio – AP Wireless Clients

2.4.4.4 Wireless VLAN Mapping

In the 3e-520 series, by enabling **Wireless VLAN Mapping**, VLAN tag would be added to the packets of wireless client and be forwarded to their dedicated VLAN network. Figure 47 shows configuration for **wireless VLAN mapping**.

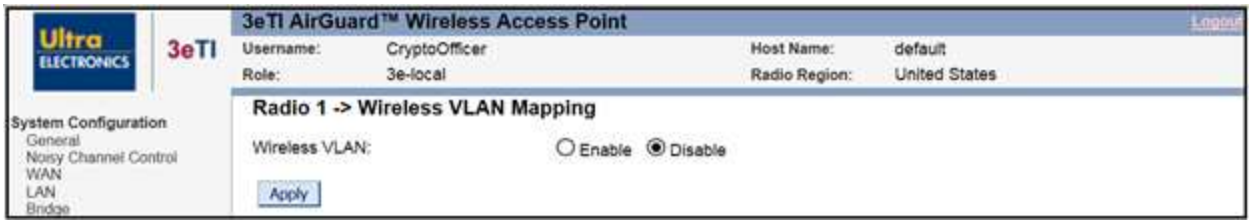


Figure 47: Radio – Wireless VLAN Mapping

2.4.4.4.1 Enable Wireless VLAN

To enable VLAN mapping, hit the **Enable** button and the **Apply** button. After enabling Wireless VLAN Mapping, you can create multiple wireless VLAN from the lower portion of the **Radio – Wireless VLAN Mapping** screen (Figure 48 shows the VLAN mappings is enabled).

The AP General SSID was configured on the **Radio – AP General** screen (Figure 42) can be set to enable or disable. When enabled, the packet coming in through this SSID will not have VLAN tags.

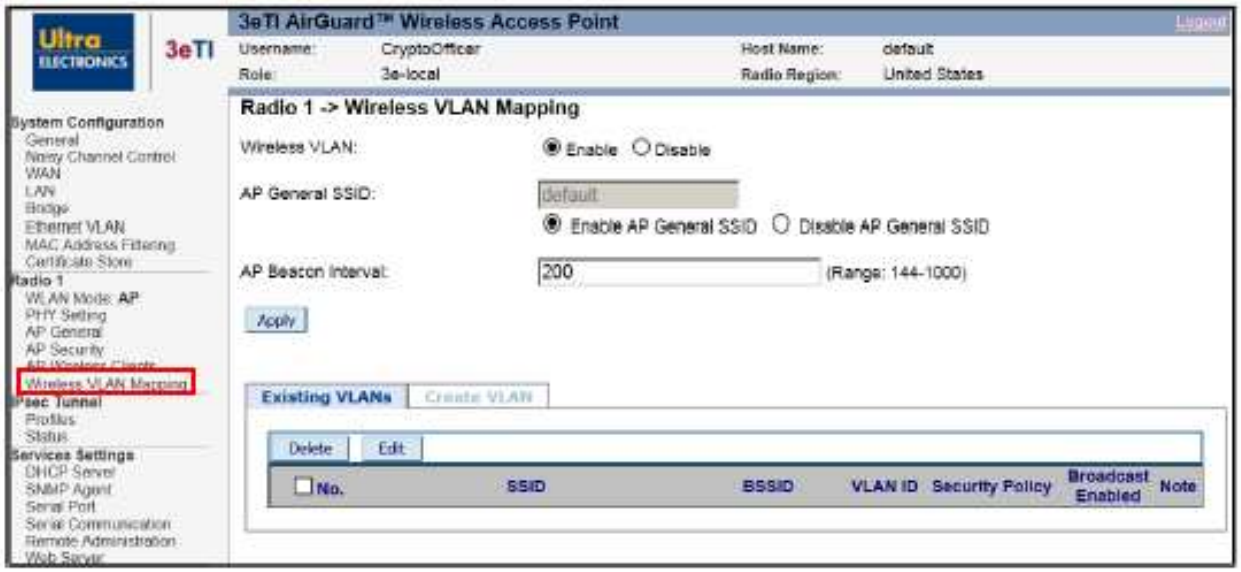


Figure 48: Radio – Wireless VLAN Mapping – Enable Wireless VLAN

2.4.4.4.2 Create VLAN

Click on the **Create VLAN** tab to create VLANs for each SSID.

Figure 49 shows the VLAN configuration screen in Create VLAN page. Each SSID can be associated with a different VLAN tag. That VLAN tag will be added to the Ethernet package when coming into the AP and be removed when sent out through the radio. A VLAN tag configuration of "0" will eliminate the VLAN modification for the SSID.

The detail SSID AP configuration is the same as the **Radio – AP General** configuration (Section 2.4.4). The detail SSID security authentication configuration is the same as in **Radio – AP Security** configuration (Section 2.4.4.2) excludes Pre-Shared Key with Passphrase option.

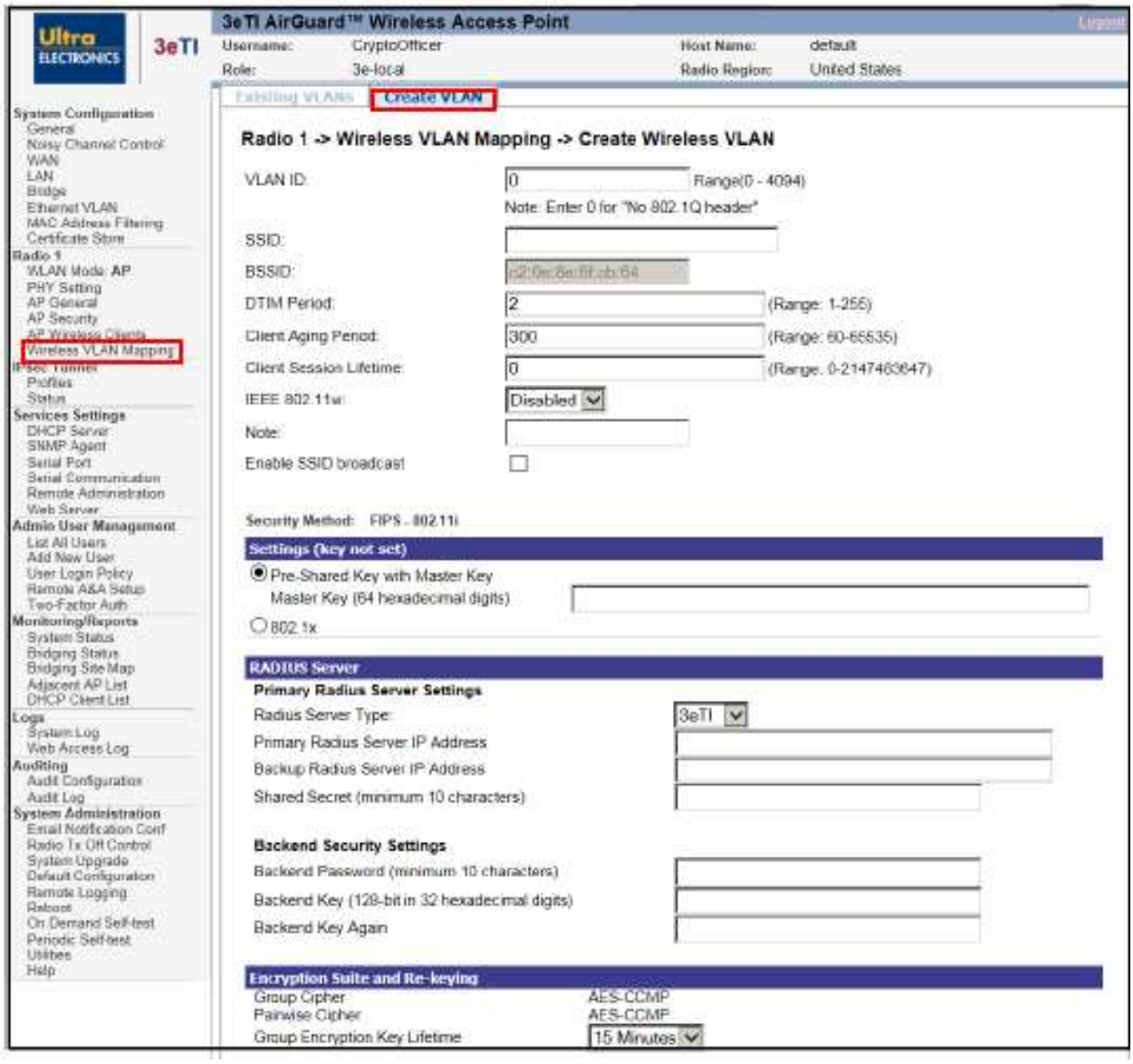


Figure 49: Radio – Wireless VLAN Mapping – Create Wireless VLAN

1) **Notes and Tips**:

   a) In 3e-520 series, VLAN 1 is always tagged. VLAN 0 can be used for untagged VLAN.

   b) If the WAN Ethernet interface is put in "Single VLAN" mode and its VLAN ID is different than the "Management VLAN", the device is not manageable through the WAN port. In this scenario, manage the device through the LAN port when the user is around the device.

   c) If the WAN Ethernet interface is put in "Single VLAN" mode and its VLAN ID is different than "Sensor VLAN", the video traffic is not reachable through the WAN Ethernet port. In this scenario, configure the AP radio to have one SSID mapped to the "Sensor VLAN" and access video traffic through this SSID when the user is around the device.

   d) In (b) and (c) above, the user can always access the device or video traffic through the wireless bridge remotely.

   e) When the device is deployed in an outdoor environment, it may be desirable to disable/block the Ethernet WAN port. This can be achieved by putting "Ethernet WAN" in "Single VLAN" mode and configuring a non-existing VLAN ID. This way, no traffic will be sent out from this Ethernet WAN port.

   f) It is always recommended to manage the device through the LAN virtual interface (192.168.15.1) when local access is available for the device. The LAN virtual interface is helpful especially when:

      i) A device IP address is unknown,

      ii) The device has not obtained an IP address from a DHCP server,

      iii) The Management VLAN is tagged.

2.4.5 Mesh Point Configuration

2.4.5.1 Wireless Mesh Introduction

In the Mesh mode of 3e–520 series, wireless mesh is used to set up a backhaul mesh network connection. Wireless mesh provides a mechanism for APs to collaborate, which enables extension of the Basic Service Set (BSS) of a standalone AP and connection of two separate LANs without installing any cabling.

The wireless bridge function supports a number of bridging configurations. Some of the most popular settings are discussed in this section:

- Point-to-point bridging of two Ethernet links
- Point-to-multipoint bridging of several Ethernet links.

Meshing is a function that is set up in addition to basic AP setup. If you will be using the unit solely as a bridge, some of the settings you may have selected for AP use will not be necessary.

If setting up as a Mesh during initial setup, you can use the LAN Port directly wired by Ethernet cable to a laptop to set the appropriate settings. The management screens that you may need to modify, regardless of what type of bridging mode you choose, are in the **Radio – Mesh Point** section of the navigation bar. These include:

- Wireless Mesh General,
- Auto Bridge Security.

2.4.5.2 Wireless Mesh General

The **Radio – Wireless Mesh General** screen (Figure 50) contains wireless bridging information. This screen is important in setting up your bridge configuration.

Figure 50: Radio – Wireless Mesh General

From a mesh network, the wireless mesh sniffs for beacons from other wireless mesh nodes and identifies APs that match a policy such as SSID and channel.

Instead of simply adding the APs with the same SSID/channel to the network, a three-way association handshake is performed in order to control network access.

To make a unit the root node, set the bridge priority lower than any other node in the network. This done on the **System Configuration – Bridge** screen (Section 2.3.6).

Table 11 describes the auto bridging general setting options.

Table 11: Wireless Mesh General Setting Options

Settings	Options	Description
SSID	Numbers and Letters	Can be any set of letters and numbers (up to 32) assigned by the network administrator. This nomenclature has to be set on the wireless bridge and each wireless device in order for them to communicate.
Broadcast SSID	Disable/Enable	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the bridge does not send probe responses to probe requests with unspecified SSIDs.
Beacon Interval	144-1000 (TU)	The time interval in time unit (TU) which the 802.11 beacon is transmitted 1 TU = 1.024 milliseconds.
Max Auto Bridges	1-16	The maximum number of auto bridges allowed. This number defines how many neighbor bridges (with the same Basic Service Set Identifier (BSSID)) the radio is allowed to associate with. Based on application, a smaller number will allow higher bridge throughput.

Table 11: Wireless Mesh General Setting Options		
Settings	**Options**	**Description**
RSSI Window Size	1-100	RF signal fluctuates over time and the fluctuation varies in different operating environments. This parameter serves to smooth Received Signal Strength Indicator (RSSI). The RSSI that applications use will be an average of last window-size RSSI samples. The sampling rate depends on the beacon interval of the neighbor mesh node. This helps stabilize the network. For fixed location deployment, higher values are suggested for both window size and beacon interval. Lower value is recommended while adjusting antenna or distributing mobile mesh devices.
Signal Strength Threshold	50% 45% 40% 35% 30% 25% 20% 15% 10% None	On creating a bridge link, if the signal strength is less than this threshold, the link will not be created. After a link is created, it will not be destroyed even after the signal goes below this threshold. This helps to stabilize the network.
Link Sensitivity	50% 45% 40% 35% 30% 25% 20% 15% 10% None	After a link is created, signal strength is mapped to RSTP path cost. Because RF signal fluctuates, path cost needs to be adjusted accordingly. However, adjusting path cost too frequently will cause network instability. This field serves as a threshold to adjust path cost. Path cost is adjusted if signal strength increases/decreases by this value since the last adjustment. If the value is set to none, every link act like 100% signal and there will be no path cost adjustment later on. It is strongly recommended that the same value is set on all other nodes in the same network.
Ignore Mesh Signature	Yes/No	Mesh node puts a signature in Beacon IE (Information Element). Only node with matching SSID and encryption algorithm will have match signature. Select Yes to ignore this signature so that it is backward compatible. Select No if you don't need backward compatibility.
Remote AP's MAC Address	Read Only	Displays the BSSID of remote bridges that were added on the Wireless Bridge - Radio screen.

2.4.5.3 Bridge Monitoring

In the upper right-hand corner of the **Radio – Wireless Mesh General** screen (Figure 50) there is a **Monitoring** button. If you click on this button, a pop-up window will appear (Wireless Bridge Information in Figure 51). If you select **Enable refresh**, you can set the **Bridge refresh interval** from 5 seconds to 30 minutes. Refreshing the screen allows you to see the effect of aiming the antenna to improve signal strength.

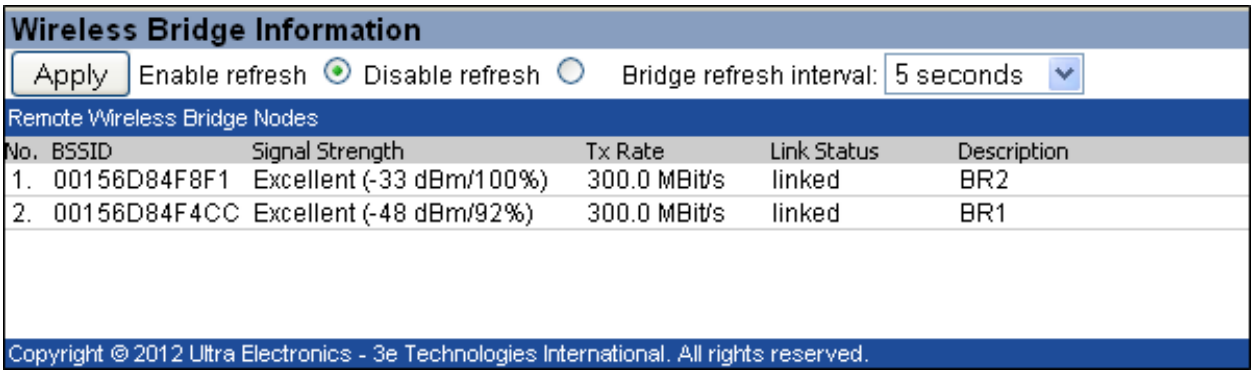


Figure 51: Wireless Bridge Information (Monitoring)

2.4.5.4 Auto Bridge Security

The **Radio – Auto Bridge Security** screen (Figure 52) is used to configure static encryption keys for the wireless bridge. This is an important screen to set up to ensure that your bridge is working correctly. In order for communication to occur, the encryption key that you use on this screen must be the same for any bridge radios connected to your Mesh network.

The **Encryption Type** can be configured as:

1) **Static AES with 128-bit, 192-bit or 256-bit Encryption Key; or**
2) **Static AES-CCMP with 128-bit, 192-bit or 256-bit Encryption Key.**

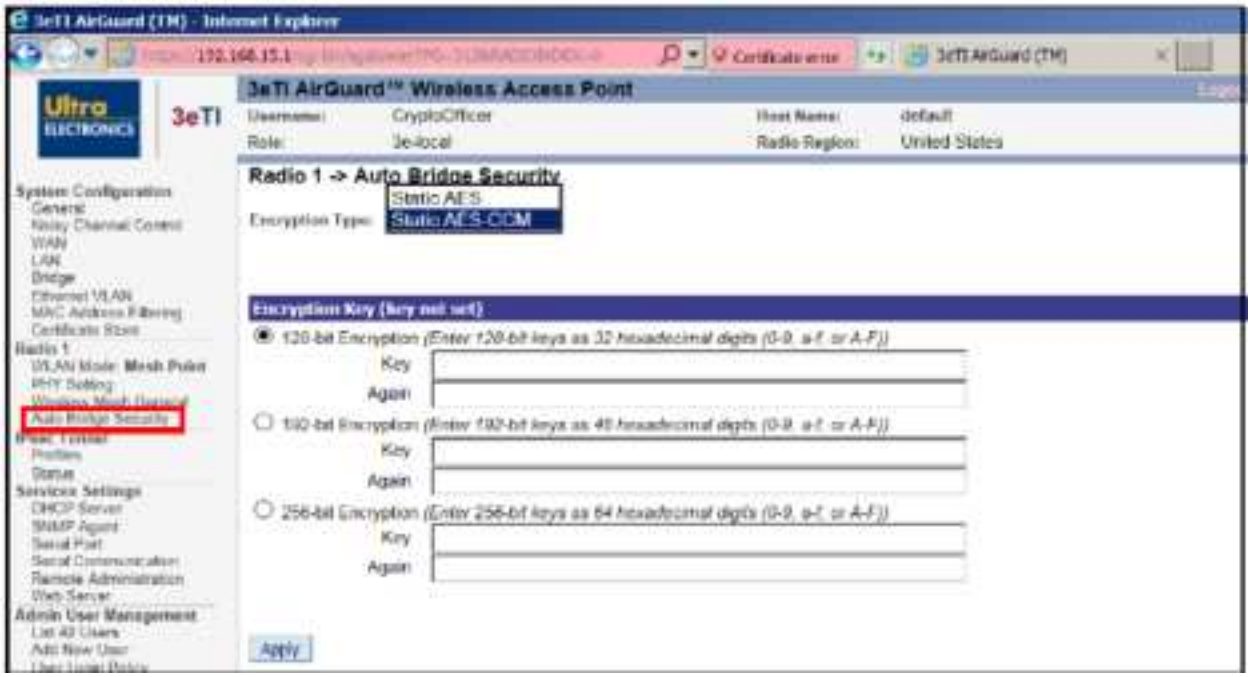


Figure 52: Radio – Auto Bridge Security

2.4.6 Wireless Client Configuration

The radios in the 3e-520 series can be configured as wireless clients to connect with an AP. The client mode of a radio cannot be combined with either bridge or AP mode.

2.4.6.1 Radio PHY Setting in Client Mode

The **Radio – PHY Setting** screen is shown in Figure 53. It is used to setup physical layer parameters of the radio. The client radio will scan all the channels to find out the available APs. On the **Radio – Client General** screen (Figure 54) the desired AP can be selected. The **wireless mode**, **channel number** and **802.11n Feature** are not configurable and grayed out.

For setting the RTS Threshold and Propagation Distance follow the instructions in Section 2.4.3.

Figure 53: Radio – PHY Setting

2.4.6.2 Client General

The **Radio – Client General** screen is shown in Figure 54. Radio will automatically scan all the channels to find any available APs in the area. The desired AP's SSID will be put in the **SSID** field that will send association and authentication packets to the nearby Access Point. You can Enable the IEEE 802.11w when the AP requires to use 802.11w to enhance further protection to a set of robust management frames by the Protected Management Frames (PMF) service. The 802.11w is configured on a per-SSID basis and disabled by default.

Clicking on the **Scan** button will refresh the list of all the APs in the area. The SSID does not have to be the one being detected. Some APs may be configured not to broadcast its SSID.

The **Status** field shows status of the connection between the client and the AP. The client and AP will not associate with each other until the **Radio – Client Security** screen (Figure 55) is configured correctly.

Figure 54: Radio – Client General

2.4.6.3 Client Security

The **Radio – Client Security** screen is shown in Figure 55. The client authentication security is carried out on this screen. The **Security Type** can be configured as **WPA2-PSK-PASSPHRASE, WPA2-PSK-CCMP** or **WPA2-EAP-TLS-CCMP**.

WPA2-PSK-PASSPHRASE: The 8-to-63 characters should be entered in the **Passphrase** field.

WPA2-PSK-CCMP: The 64 hexadecimal digits should be entered in the **Master Key** field.

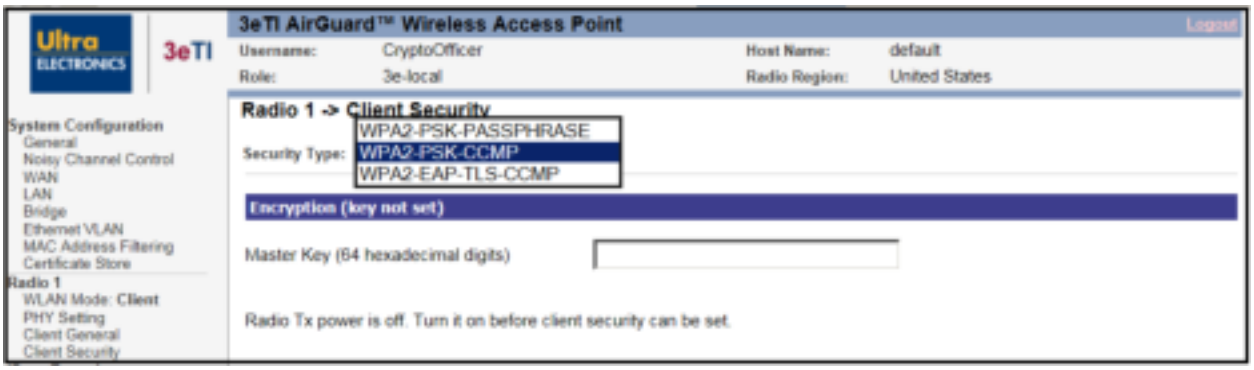


Figure 55: Radio – Client Security Type

WPA2-EAP-TLS-CCMP: As shown in Figure 56, by selecting client security type WPA2-EAP-TLS-CCMP, use a pre-loaded certificate from the list and provide a **Login Name** can be configured on this screen.

Figure 56: Radio – Client Security – WPA2-EAP-TLS-CCMP

A device certificate and root CA must be loaded from Certificate Store (details in Section 2.3.9 and Figure 57). Then click on **Apply** to save the client security.

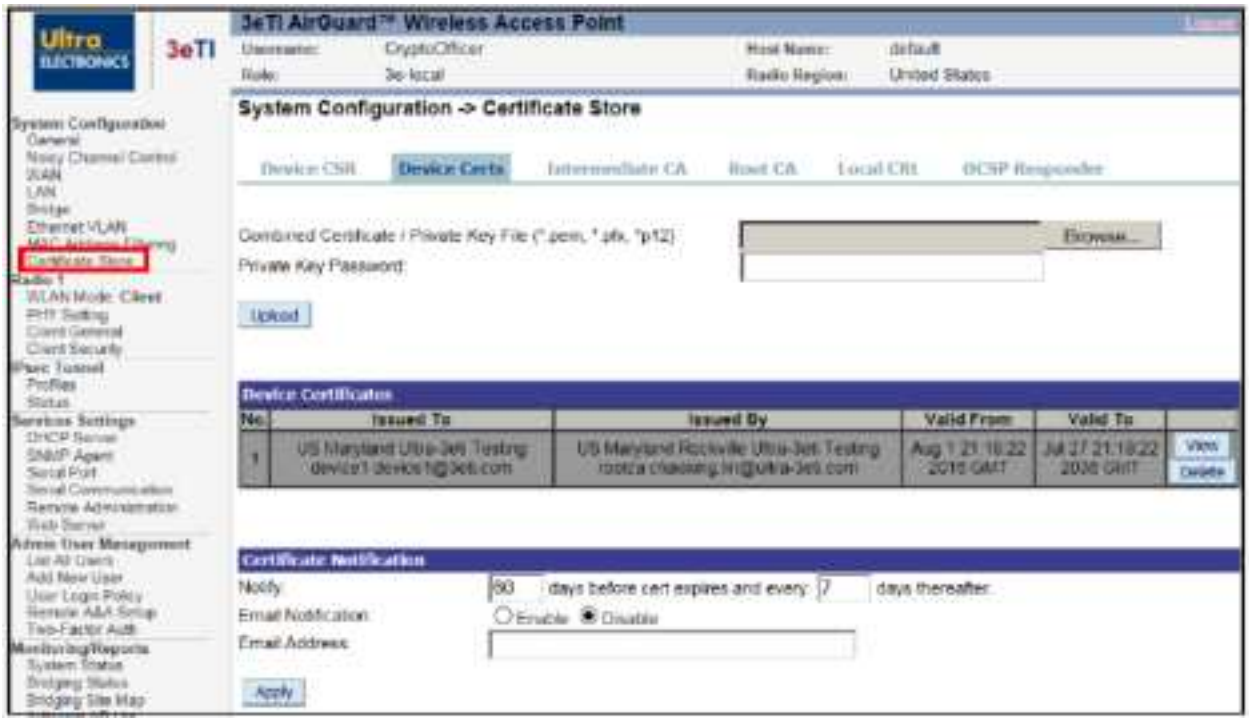


Figure 57: Certificate Store – Loading Client Certificates for WPA2-EAP-TLS-CCMP

2.5 IPsec Configuration

IPsec tunnels can be configured to protect communication between the 3e-520 series and external services such as a RADIUS authentication server, NTP server or Remote Audit Log server. IPsec tunnels are used for a trusted channel to external servers in Common Criteria configuration. In order to use IPsec, at least one IPsec Tunnel Profile must be configured. Each profile specifies a cipher suite, authentication method, credentials and rekey timers. Once an IPsec Profile is configured it can be applied to a service. IPsec Security Policy Database (SPD) is dynamically configured, based the trusted paths IPsec is used to protect. For example, IPsec tunnel is configured to protect a remote syslog trusted path. In this instance, records are written into the SPD to protect packets passing between the 3e-525/523 and the remote syslog server based on source address, destination address, protocol and port number. When protecting remote syslog trusted path, the SPD will have one record matching ingress UDP traffic with source address and port corresponding to the remote syslog server. Additionally, the SPD will have one record matching egress traffic, with destination address and port, corresponding to the remote syslog server. Traffic passing through the security boundary and matching either of these two records will be classified as "PROTECTED" using IPsec transport mode. Traffic that does not match any records in the SPD will be allowed to "BYPASS" the security boundary unperturbed. Additional records are written into the SPD when additional trusted paths are configured for IPsec protection (i.e., RADIUS server, NTP …). Traffic that does not match any records in the SPD will be "DISCARDED".

The device supports IPsec tunnel and transport modes which allows packet payloads to be encrypted. The device requires no administrative configuration and negotiates either depending on the peer.

2.5.1 IPsec Tunnel Profiles Configuration

An IPsec Tunnel profile must be configured in order to enable secure communications between the 3e-520 series device and a remote log server or an NTP server. Once configured, the profile will then be available from NTP Server and the Audit Configuration sections (see Figure 23: NTP Time Source with IPsec Protection and Figure 85: Remote Audit Logging). The 3e-520 series device supports up to 8 tunnel profiles. To create an IPsec Tunnel profile, click on the 'Profiles' menu under 'IPsec Tunnel' on the left of the screen. This page shows the IPsec Profiles configuration options and provides a list of all configured profiles.

2.5.1.1 Profile Settings

Add a new IPsec tunnel profile by filling out the following profile settings and clicking the "**Add**" button. Refer to Table 12: IPsec Tunnel Profile Settings for more setting details.

New Profile Name: Enter profile name, string must be between 3 and 16 alphanumeric characters, _ and. is allowed.

Cipher Suites: Select from Auto Negotiated, Suite B GCM 128, Suite B GCM 256, AES CBC 128, or AES CBC 256 (see Section 2.5.1.2 and Table 13 for more detail).

Authentication: Select Pre-Shared or Public Key. If the "Public Key" is selected, then a pre-loaded certificate should be selected from the drop-down list. Please note that the certificate list is populated by the certificates loaded via "Certificate Store" which is covered in Section 2.3.9.

Pre-Shared Key: if using Pre-Shared Authentication, enter key here.

Rekey Timers: Enter rekey time in minutes for IKE SA and IPsec SA (20-144min range). Enter IPsec SA life rekey timer in kilobytes and kilo packets within the ranges listed (0 for unlimited).

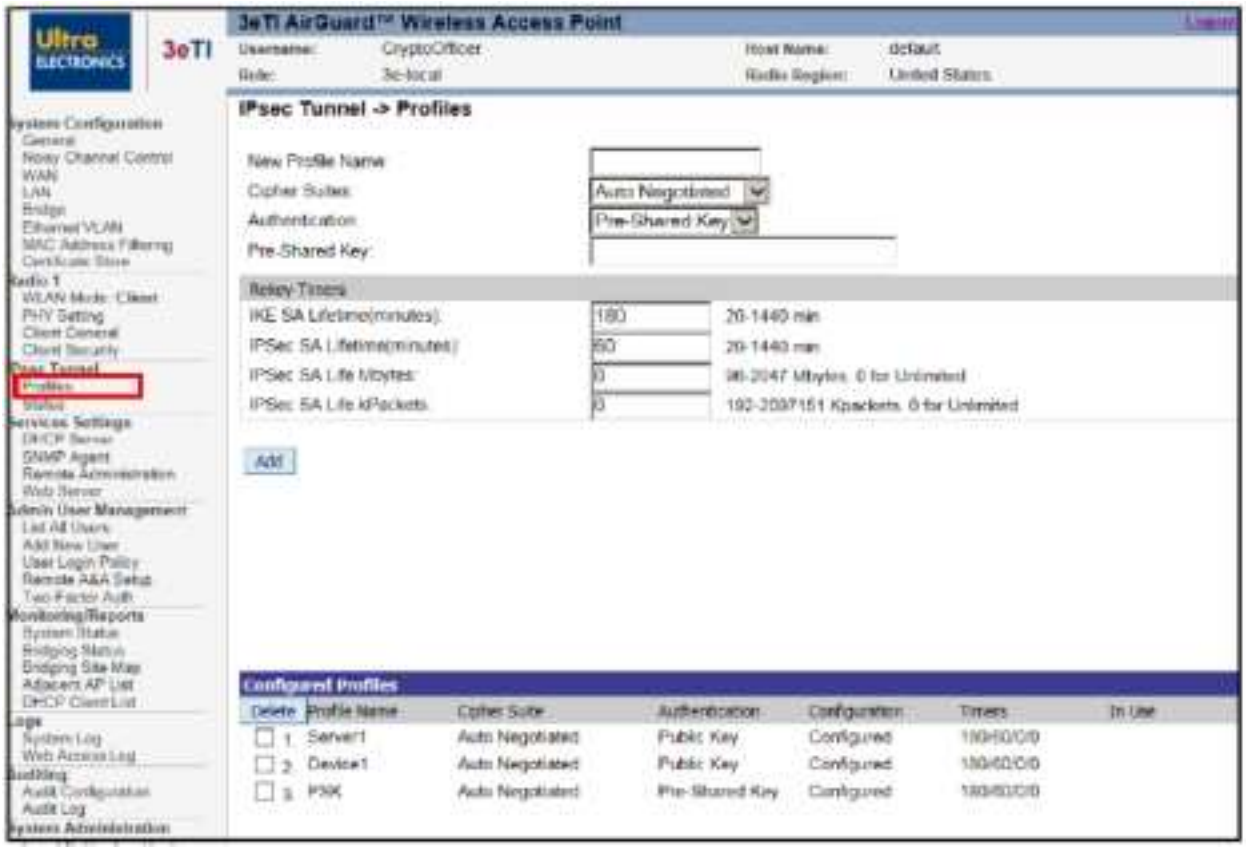


Figure 58: IPsec Tunnel Profiles

Configured Profiles: this section lists all configured profiles and allows the user to select a profile for deletion.

Table 12: IPsec Tunnel Profile Settings

Settings	Options	Description
New Profile Name	String from 1 to 16 characters	Free formed string to name the profile. Up to 8 profiles can be added and each name must be unique. There is not default value.
Cipher Suite	Auto Negotiated Suite B GCM 128 Suite B GCM 256 AES CBC 128 AES CBC 256 Suite B GMAC 128 Suite B GMAC 256	Cipher suites used during IKEv2 Phase 1 as well as ESP Phase 2 cipher negotiation. See Table 13: Cipher Suites for details. The default value is "Auto Negotiated".
Authentication	Pre-Shared Key Public Key	Authentication method used during IKEv2 Phase 1 Security Association establishment. The default value is Pre-Shared Key

Table 12: IPsec Tunnel Profile Settings		
Settings	**Options**	**Description**
Pre-Shared Key	• String from 16 to 32 characters long enclosed within double quotation marks • Hex string of 8 to 63 characters	The Pre-Shared Key used during the IKEv2 Phase 1 Security Association establishment. The key can be entered as a hex string or a double quoted string that is hashed into the resulting key. The device conditions the text-based pre-shared keys using the SHA1,SHA-256, and SHA384 hash algorithm.
IKE SA Lifetime	From 20 to 1440 minutes	The number of minutes an IKEv2 Phase 1 Security Association can be active before it is automatically re-authenticated. The default value is 180 minutes
IPsec SA Lifetime	From 20 to 1440 minutes	The number of minutes an IPsec ESP Child Security Association (Phase 2) can be active before it is automatically rekeyed. The default value is 60 minutes.
IPsec SA Life Kbytes	From 96 to 2047 Kbytes. 0 indicates Unlimited	The number of bytes that can be transmitted over an IPsec ESP Child Security Association (Phase 2) before it is automatically rekeyed. The default value is 0 indicating Unlimited.
IPsec SA Life kPackets	From 192 to 2097151 kPackets. 0 indicates Unlimited	The number of packets that can be transmitted over an IPsec ESP Child Security Association (Phase 2) before it is automatically rekeyed. The default value is 0 indicated Unlimited.

2.5.1.2 IPsec Cipher Suites

The 3e-520 series supports a number of different encryption standards and protocols, including the four Suite B cryptographic suites as defined in RFC 6379.

The order in which the protocols appear gives the preference order of use within the 'Auto Negotiated' mode. Otherwise, if one of the Suite B modes is chosen, the denoted protocols are used for that given mode.

Table 13: Cipher Suites

Mode	IKEv2				ESP (Hardware encryption)	
	Encryption	**Integrity**	**Pseudo Random Function**	**Diffie Hellman Group**	**Encryption**	**Integrity (where applicable)**
Standard (Auto Negotiated)	aes256cbc aes128cbc	sha512 sha384 sha256 sha1	Same as negotiated integrity	ecp521 ecp384 ecp256 modp2048 modp1536 modp1024	aes256gcm128 aes256ccm128 aes256gcm96 aes256ccm96 aes256gcm64 aes256ccm64 aes256cbc aes128gcm128 aes128ccm128 aes128gcm96 aes128ccm96 aes128gcm64 aes128ccm64	sha512 sha384 sha256 sha1

Mode	IKEv2				ESP (Hardware encryption)	
	Encryption	Integrity	Pseudo Random Function	Diffie Hellman Group	Encryption	Integrity (where applicable)
					aes128cbc	
Suite B GCM 128	aes128cbc	sha256	sha256	ecp256	aes128gcm128	-
Suite B GCM 256	aes256cbc	sha384	sha384	ecp384	aes256gcm128	-
AES CBC 128	aes128cbc	sha256	sha256	ecp256	aes128cbc	sha256
AES CBC 256	aes256cbc	sha384	sha384	ecp384	aes256cbc	sha384
Suite B GMAC 128	aes128cbc	sha256	sha256	ecp256	NULL	aes128gmac
Suite B GMAC 256	aes256cbc	sha384	sha384	ecp384	NULL	aes256gmac

2.5.2 IPsec Tunnel Status

To check the status of IPsec tunnels, click on the 'Status' menu under the IPsec heading on the left side of the screen. This page (Figure 59) lists current status of all IPsec Tunnels configured in the 3e-520 series device.

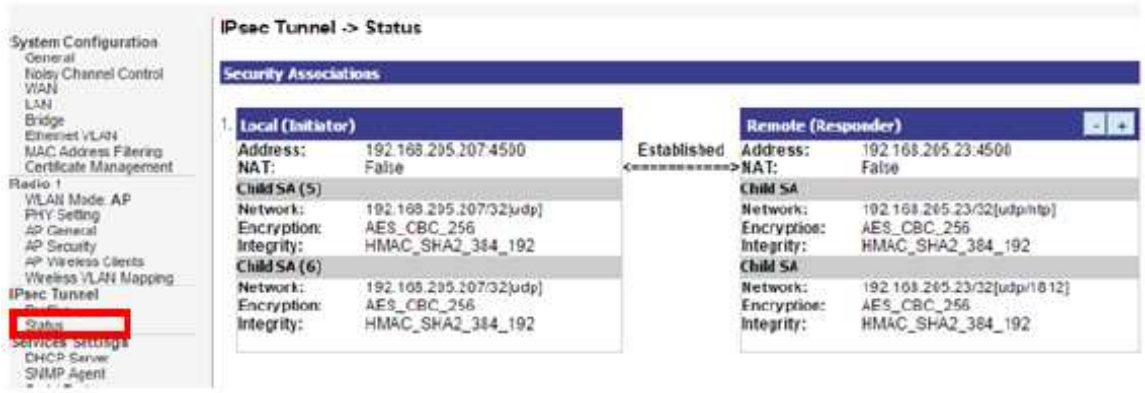


Figure 59: IPsec Tunnel Status

2.6 Services Settings

2.6.1 DHCP Server

The **Services Settings - DHCP Server** screen (Figure 60) is used to configure the DHCP server function accessible from (only) the Local LAN port. The DHCP server function is used for initial configuration of the management functions.

DHCP Server is Enabled by default. You can disable the DHCP server function, if you wish, but it is not recommended. You can also set the range of IPv4 addresses to be assigned; **Starting IP Address** defaults to 192.168.15.10, **Ending IP Address** defaults to 192.168.15.240.

The **Lease Period** (after which the dynamic address can be reassigned) can also be varied; the default setting is 1 Day.

Figure 60: Services Settings — DHCP Server

2.6.2 SNMP Agent

The **Services Settings – SNMP Agent** screen (Figure 61) allows you to configure the Simple Network Management Protocol (SNMP) Agent for the device. By default, the SNMP Agent is set to disable (both SNMPv1/SNMPv2c and SNMPv3 protocol are **unchecked** shown in Figure 61). The SNMP Manager function interacts with the SNMP Agent to execute applications to control and manage object variables in the AP. Common forms of managed information include number of packets received on an interface, port status, dropped packets, and so forth. The SNMP is a simple request and response protocol, allowing the manager to interact with the agent to either:

- **Get** - Allows the manager to **Read** information about an object variable,
- **Set** - Allows the manager to **Write** values for object variables within an agent's control.

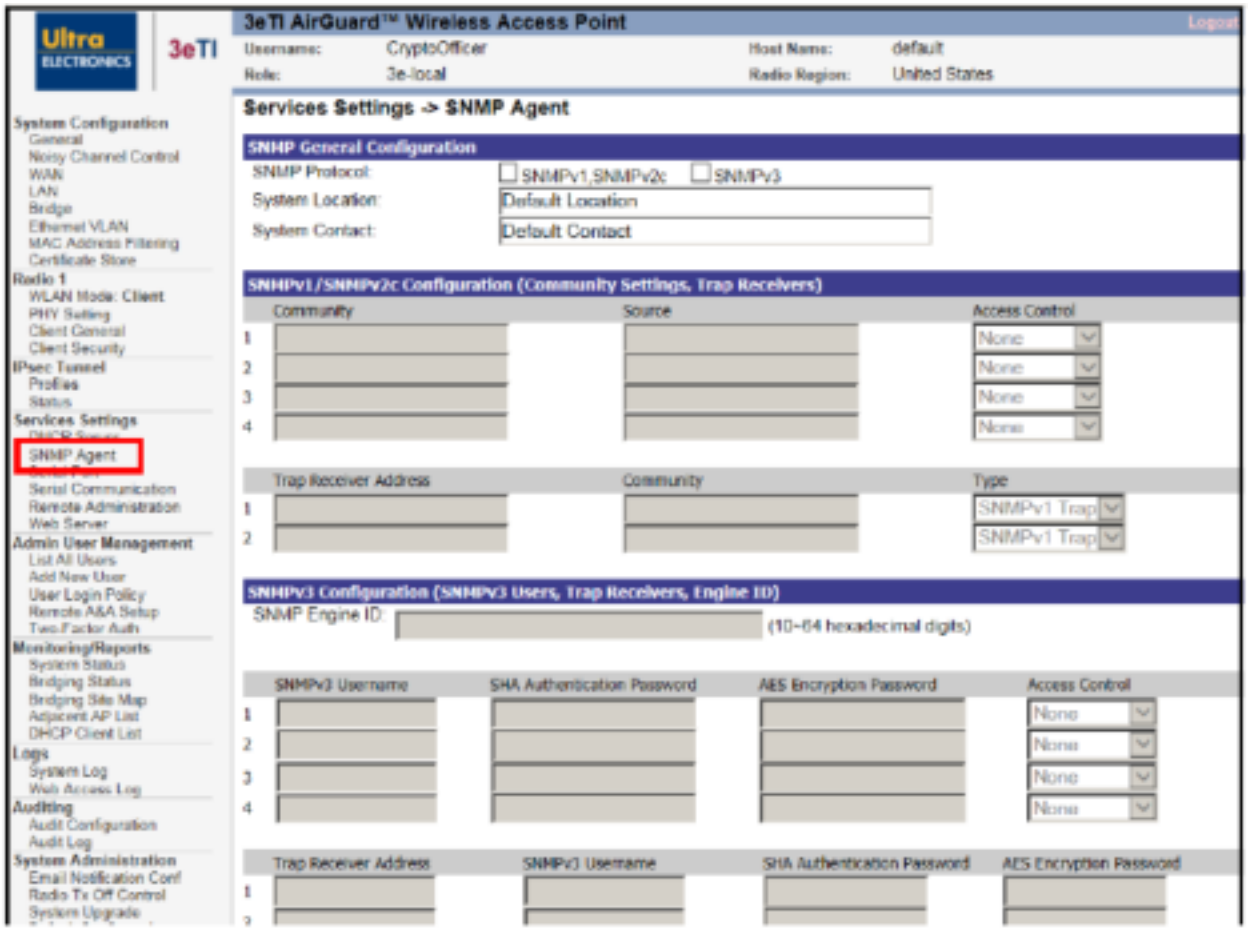


Figure 61: Services Settings — SNMP Agent

WiFiProtect 3e-520 series products support multiple versions of SNMP protocols: SNMPv1, SNMPv2c and SNMPv3. You can disable any SNMP protocols by unchecking the SNMP protocol version.

The **SNMP General Configuration** section shown in Figure 61 allows you to configure what versions of SNMPs to be enabled in the device, and enter **System Location** and **System Contact** information to help identify the device. Only SNMPv3 supports secure SNMP connections to the device, as described below.

When the SNMPv1, SNMPv2c protocol option is checked (enabled), you can enter the **Community Settings** and **Trap Receivers** in the **SNMPv1/SNMPv2c Configuration** section:

1) **SNMPv1/SNMPv2c Community Settings:**

   a) **Community** – Authentication of clients is performed (only) by a "community string", in effect a type of password. It is transmitted in plain text, and so provides only limited security.

   b) **Source** – The source IP addresses from which the SNMP manager is allowed to access this device.

   c) **Access Control** – Defines the level of management interaction permitted. Select between **None**, **Read Only** (Get), and **Read Write** (Set). The default setting is **None**.

2) **SNMPv1/SNMPv2c Trap Receivers:**

a) **Trap Receiver Address** – The IP address of the trap receiver that receives SNMP traps from this device.

b) **Community** – The community string to be used in reporting SNMP traps.

c) **Type** – The type of SNMP traps. Select between **SNMPv1 Trap** and **SNMPv2 Trap**. The default setting is **SNMPv1 Trap**.

When the SNMPv3 protocol option is checked (enabled), you can set up secure SNMPv3 access in the **SNMPv3 Configuration** section.

3) **SNMPv3 Engine ID:**

a) SNMPv3 requires that an application know the unique identifier (**snmpEngineID**) of the remote SNMP protocol engine in order to retrieve or manipulate objects maintained on the remote SNMP entity. You can enter a unique hexadecimal string of 10 - 64 characters for the **Engine ID** or leave this field to be blank so that the default **Engine ID** is used. The default **Engine ID** is automatically generated based on the device MAC address in accordance with RFC 2571:

i) First 4 octets – The first bit is set to 1. The rest is the Internet Assigned Numbers Authority (IANA) Enterprise number 8433 assigned for 3eTI.

ii) Fifth octet – Set to 3, indicating the MAC address is specified in the next 6 octets.

iii) Last 6 octets – MAC address of the device WAN port.

4) **SNMPv3 Secure Users:**

a) **SNMPv3 Username** – The username for the secure SNMPv3 connection. A minimum of eight characters in length.

b) **SHA Authentication Password** – Only Secure Hash Algorithm (SHA) authentication is supported. Enter a cryptographically strong password, one that contains characters from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

c) **AES Encryption Password** – Only Advanced Encryption Standard (AES) encryption is supported. Enter a cryptographically strong password, one that contains characters from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

d) **Access Control** – Defines the level of management interaction permitted. Select between **None**, **Read Only** (Get), and **Read Write** (Set). The default setting is **None**.

5) **SNMPv3 Trap Receivers:**

a) **Trap Receiver Address** – The IP address of the trap receiver that receives SNMPv3 traps from this device.

b) **SNMPv3 Username** – The username for sending SNMPv3 traps. A minimum of eight characters in length.

c) **SHA Authentication Password** – The SHA authentication password for sending SNMPv3 traps. Enter a cryptographically strong password, one that contains characters from all of the

following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

d) **AES Encryption Password** – The AES encryption password for sending SNMPv3 traps. Enter a cryptographically strong password, one that contains characters from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

Click **Apply** to save configuration changes.

NOTE: Please contact 3eTI support for SNMP Management Information Base (MIB) information.

2.6.3 Serial Port (3e-523N Only)

The **System Configuration – Serial Port** screen (Figure 62) allows you to control the type and format of the serial data to be transmitted and received, if the serial port is available, enabled and configured. Refer to section Appendix C. Serial I/O Interface Board for wiring definition of the signals.

NOTE: To enable this serial port, you must enable serial communications under **Services Settings – Serial Communication** (Figure 63).

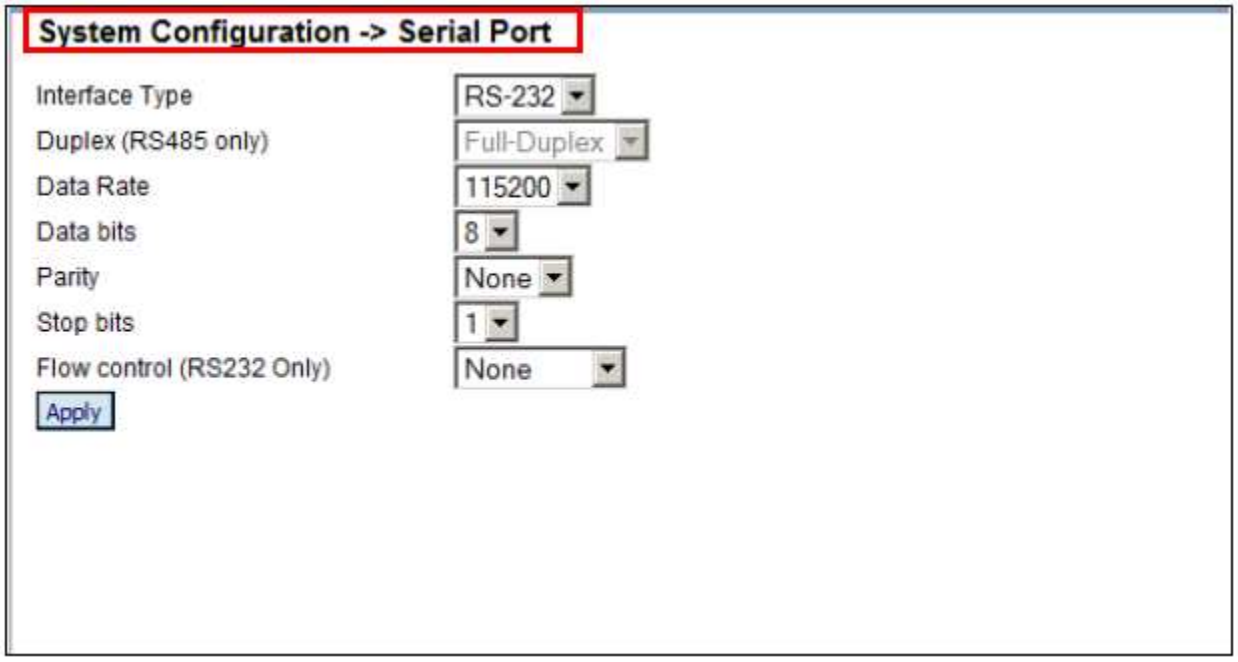


Figure 62: System Configuration – Serial Port

Table 14: Service Settings – Serial Communication			
Settings	**Options**	**Description**	**Default**
Interface Type	RS-232 RS-422 RS-485	Select the interface type for the serial I/O port.	RS-232
Duplex (RS485 only)	Full-Duplex Half-Duplex	In full duplex mode data is transmitted and received simultaneously. In half duplex mode data is transmitted or received but not at the same time.	Full Duplex
Data Rate (bits per second)	115200 57600 38400 19200 9600 4800 2400 1200	Select the data rate required.	115200
Data bits	8 7 6 5	Select the number of data bits to be transmitted or received.	8
Parity	None Odd Even	Select parity to be used.	None
Stop bits	1 2	Select number of stop bits to be used.	1
Flow control (RS232 only)	None Hardware	When hardware flow control is selected, RTS and CTS are used.	None

2.6.4 Serial Communication (3e-523N Only)

The **Services Settings - Serial Communication** section (Figure 63) displays the status and configuration of the current serial port mode of operation. You can choose to **Enable** or **Disable** (default) serial communications and select a serial **Port Profile**.

NOTE: See **System Configuration – Serial Port** Section 2.6.3 to configure the serial interface.

2.6.4.1 Raw Socket

This is the default setting, and allows serial devices connected to two 3e–523 devices to communicate across the network. It supports bidirectional, multiple unicasting and peer-to-peer communications. Enter MAC addresses (formatted as 00:11:22:33:44:55) for the radios of the remote nodes that will communicate via the Raw Socket.

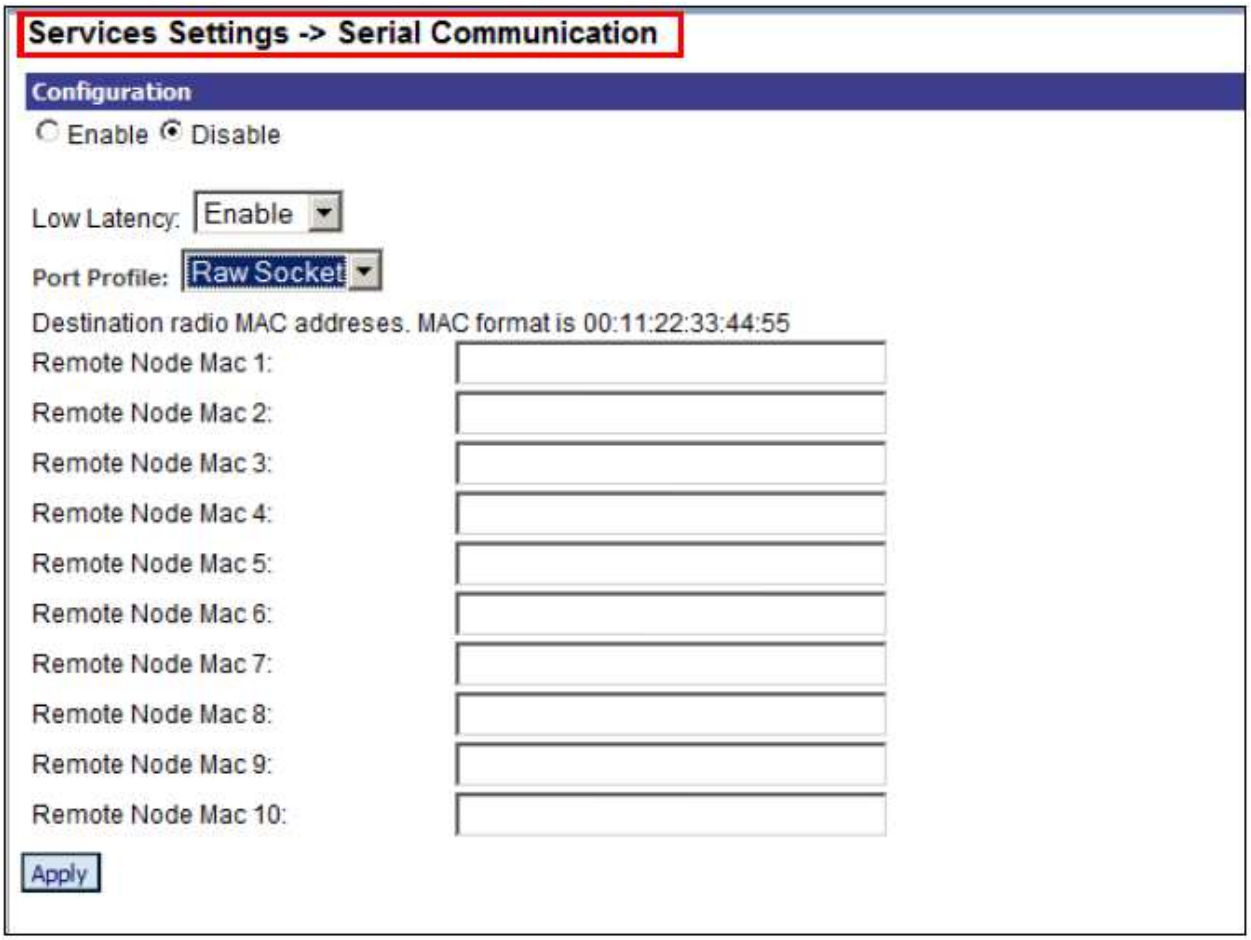


Figure 63: Services Settings – Serial Communication – Raw Socket

2.6.4.2 TCP Socket

This Port Profile provides a direct IP connection using Transmission Control Protocol (TCP). When using TCP sockets your serial server **Operation Mode** can be configured as a **Server** (default) or **Client** (Figure 64).

If the 3e–520 series device is configured as a TCP **Server**, other network devices can initiate a TCP connection with the serial device connected to the serial port. Network devices initiating connections must be configured with the IP address of the serial device and the TCP port number associated with its serial port. The **TCP Port** can be configured as needed in this screen (default is 18000).

If the 3e–520 series device is configured as a TCP **Client,** it will automatically establish a bidirectional TCP connection between the serial device and a server (or other networked device); enter the associated **Remote IP Address** (default 192.168.254.254) and **TCP Port** to configure this connection.

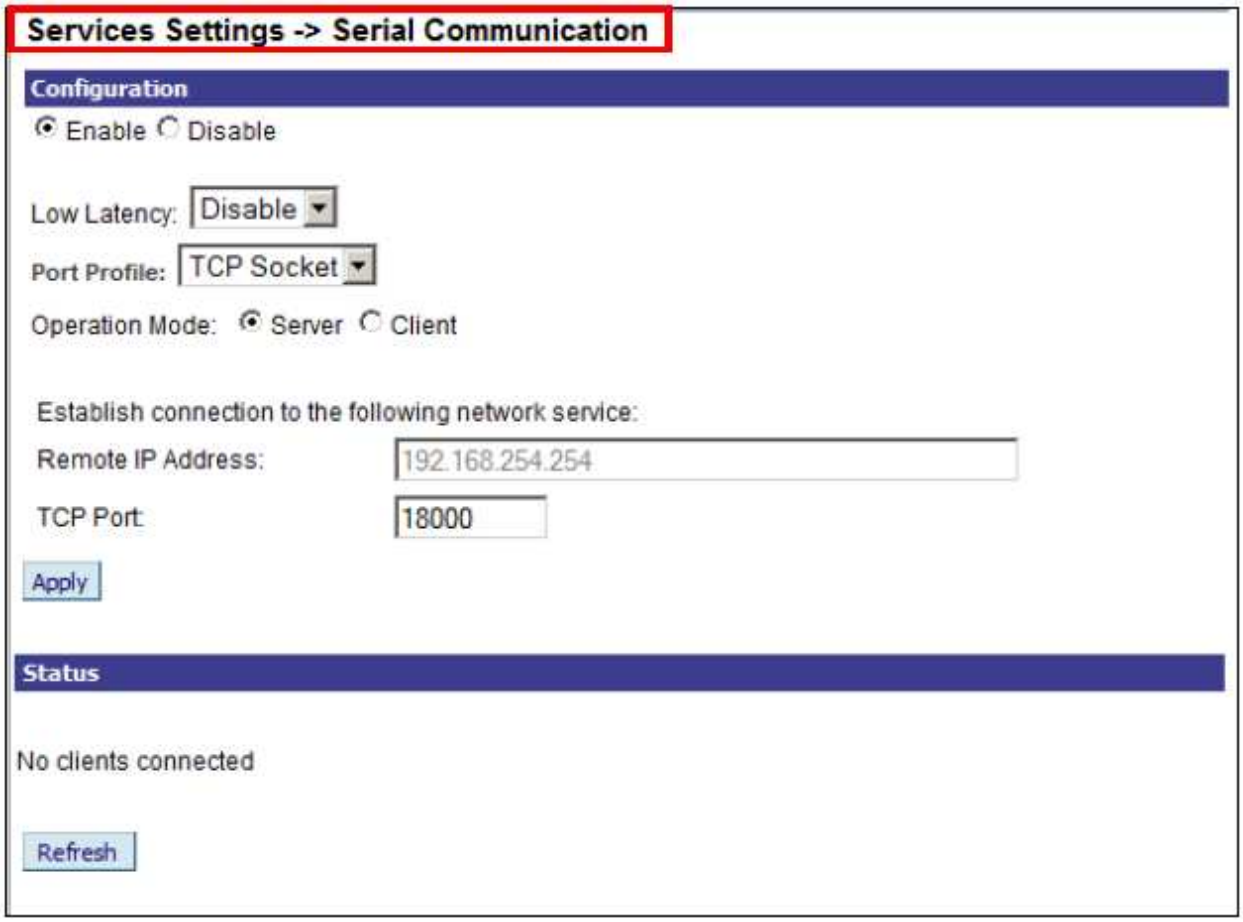


Figure 64: Services Settings – Serial Communication – TCP Socket

2.6.5 Remote Administration

The **Services Settings – Remote Administration Access Control** screen (Figure 65) allows you to set up access control policies for remote administration via HTTPS, SNMP and Internet Control Message Protocol (ICMP) protocols. In the factory default configuration, the **Remote Administration Access Control** option is set to **Disable Filtering** and hence remote administration is allowed for any source IP address and MAC address.

When the **Remote Administration Access Control** option is set to **Enable Filtering**, the device validates the source IP and/or MAC addresses of administrative queries and control requests to ensure that the message request is from an approved node. This enables secure remote administration from selected IP and/or MAC addresses.

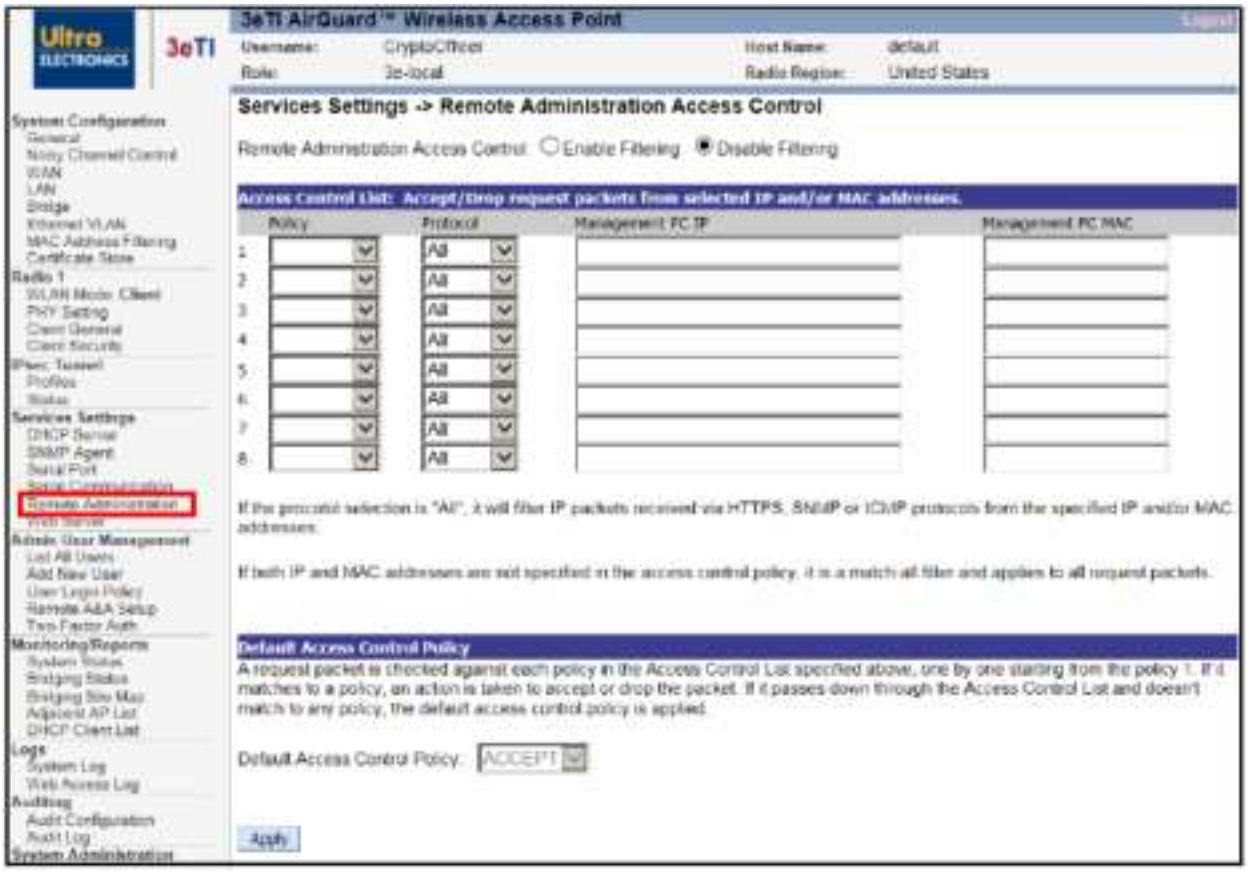


Figure 65: Services Settings — Remote Administration Access Control

Up to 8 Access Control policies can be specifically defined in the Access Control List, with the following fields for each entry:

- **Policy** – **ACCEPT** or **DROP** a request packet if it matches this access control policy.
- **Protocol** – The protocol field can be **HTTPS**, **SNMP**, **ICMP** or **All**. If the protocol field is "All" (default), the access control policy is used to match for all HTTPS, SNMP and ICMP protocols.
- **Management PC IP** – This is the actual IP address of a management Personal Computer (PC), which shall be an IPv4 unicast IP address in the form xxx.xxx.xxx.xxx, such as 192.168.202.100.
- **Management PC MAC** – This is the actual MAC address of a management PC, which shall be a unicast MAC address in the form XX:XX:XX:XX:XX:XX, such as 00:23:69:24:BF:80. You can also enter a MAC address in the form XX-XX-XX-XX-XX-XX as it is displayed in the output of the Windows "ipconfig /all" command; it will be automatically converted to the form XX:XX:XX:XX:XX:XX.

NOTE: The management PC and the device must be connected to the same LAN if MAC address filtering is used.

For each access control policy entry, both **Management PC IP** and **Management PC MAC** fields are optional. You can leave either or both of the fields blank, with the following application cases:

- **Management PC IP Only** – This is an IP address filter. Only the source IP of request packets is checked.

- **Management PC MAC Only** – This is a MAC address filter. Only the source MAC of request packets is checked.
- **Management PC IP and MAC** – This is an IP address and MAC address filter. Both the source IP and source MAC of request packets are checked.
- **Both Management PC IP and Management PC MAC are unspecified** – This is a match-all filter. The access control policy applies to any request packet.

You can select the **Default Access Control Policy** to be one of these two values:

- **ACCEPT** – Always accept a request packet when it does not match any access control policies defined in the Access Control List. This is the default value.
- **DROP** – Silently drop a request packet when there is no specific access control policy which matches it.

The ordering of access control policies is important. A request packet is checked against each policy in the Access Control List in turn, starting at policy 1, and if it matches that access control policy, then an action is taken to accept or drop the request packet. If it passes down through the Access Control List and does not match to any policy, the **Default Access Control Policy** is applied.

When you click the **Apply** button to save your setup, a confirmation dialog box will pop-up reminding you to double check your setup to ensure that your configuration allows remote administration from selected IP and/or MAC addresses, including the IP/MAC of your current management PC.

2.6.6 Web Server

The **Services Settings – Web Server** screen (Figure 66) allows you to use the uploaded certificate for a secured Web Server access.

A Web Server Certificate can be uploaded from **Certificate Store** under **System Configuration**. After loading a certificate, from the **Web Server** page, then you can select the preloaded web server certificate from the dropdown list and click on **Apply**. The default web server certificate cannot be deleted.

Figure 66: Services Settings — Web Server

2.7 Admin User Management

Users can access the device through either dedicated local Ethernet port or the WAN Ethernet port. The Management UI treat users identically regardless of the access ports.

2.7.1 List all Users

The **Admin User Management – List All Users** screen (Figure 67) lists the CryptoOfficer and any accounts configured for the unit. You can edit or delete users from this screen. You can also unlock the account which was locked.

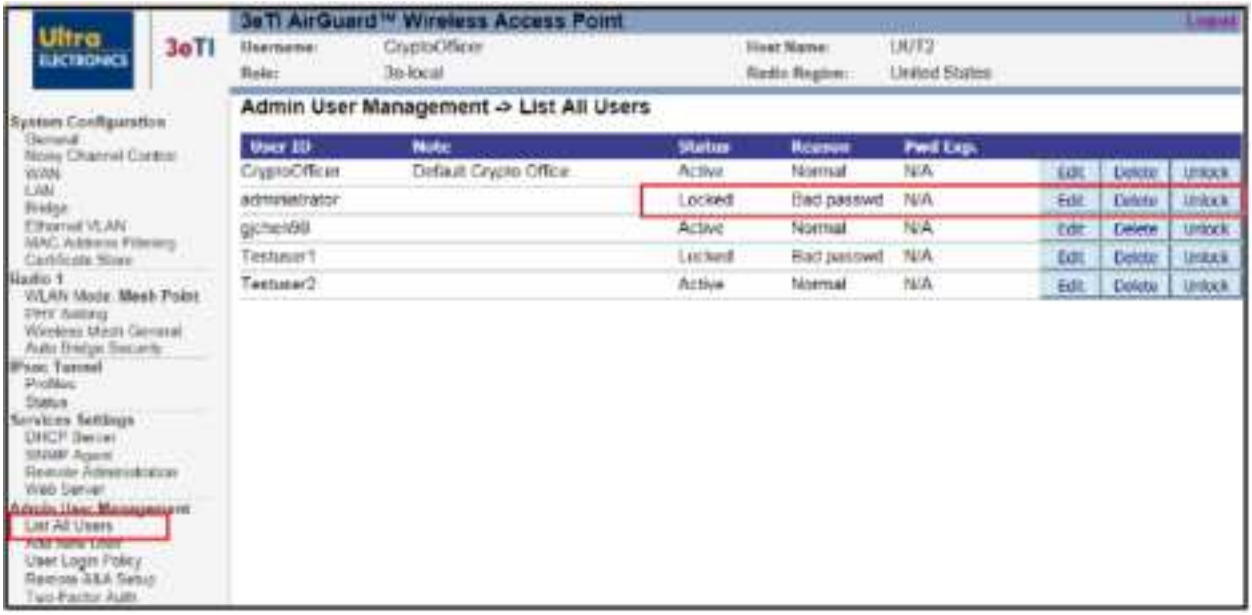


Figure 67: Admin User Management — List All Users

If you click on **Edit**, the **Admin User Management - Edit User** screen (Figure 68) appears. On this screen you can edit the **User ID, Password,** and **Note** fields. Default values are "CryptoOfficer", "CryptoFIPS", "Crypto Officer" and "Default Crypto Office" respectively. If the password complexity is enabled, your password should come from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

The Password Complexity Check and the Minimal Password Length are established on the **Admin User Management – User Login Policy** screen (Figure 71).

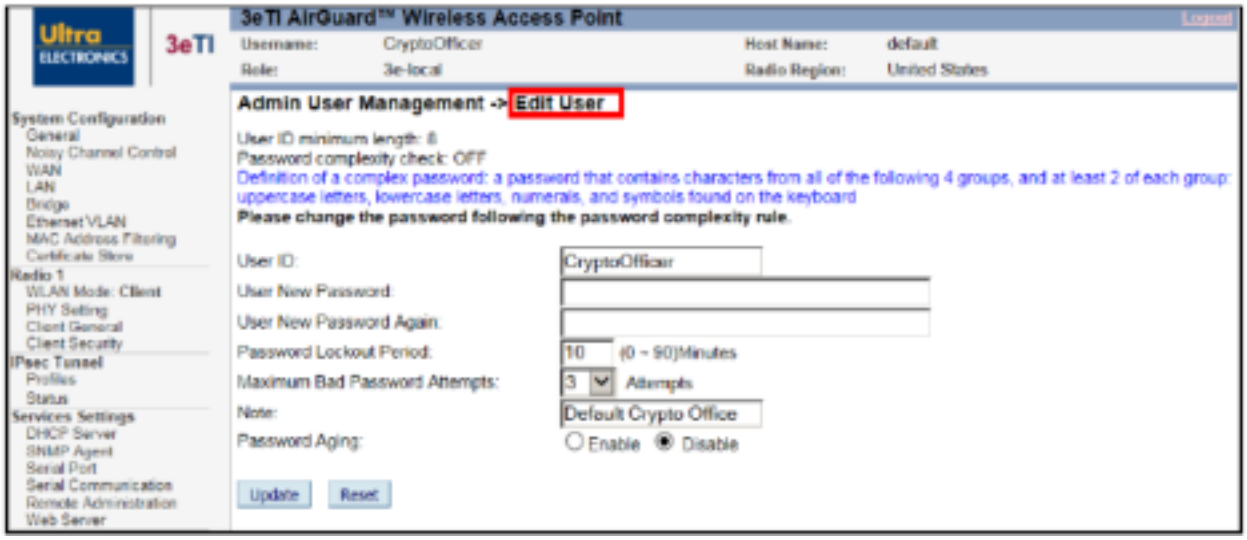


Figure 68: Admin User Management — Edit User

2.7.2 Add New User

The **Admin User Management – Add New User** screen (Figure 69) allows you to add new users with 3e-local role and configure the associated **User ID, Password,** and **Note** fields. To ensure password complexity, your password should come from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

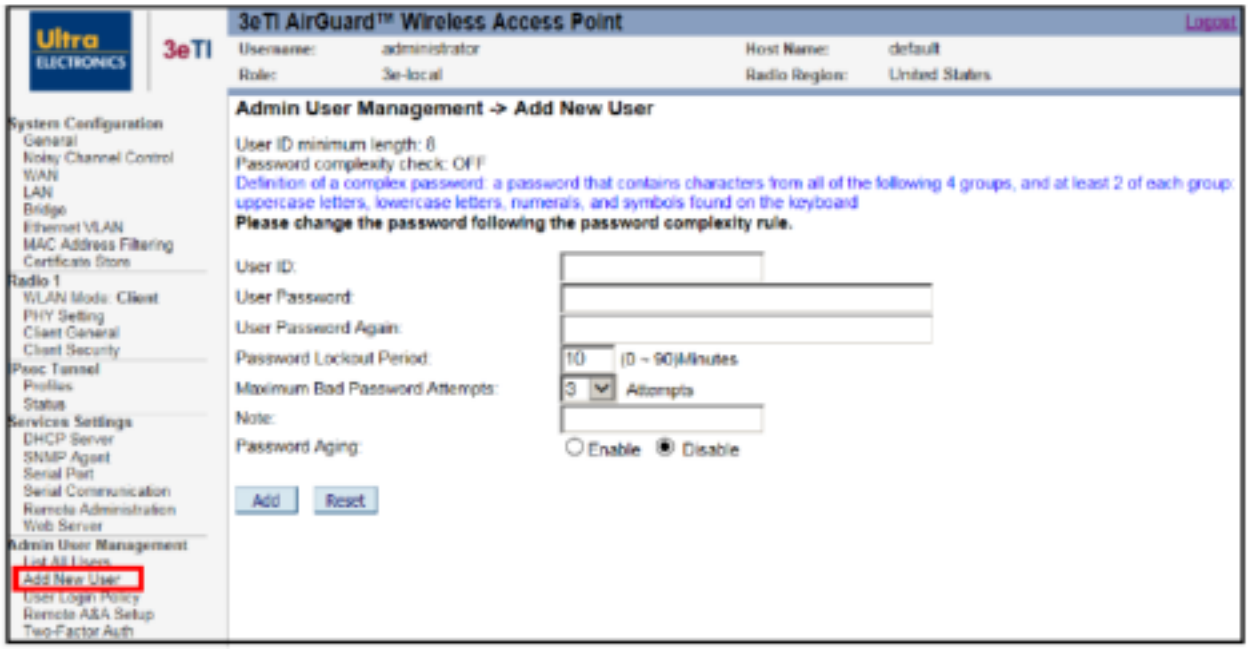


Figure 69: Admin User Management — Add New User

- **User ID:** User-defined unique user identification string
- **User Password**: User-defined user authentication string. Password can be composed of any combination of upper- and lower-case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(" or ")".
- **Password Lockout Period:** The password lockout period defines the number of minutes the user must wait after failing the maximum bad password attempts before he/she can try logging in again. The default value is 10 minutes
- **Maximum Bad Password Attempts:** The maximum bad password attempts define the number of failed authentication attempts before the lockout period is triggered. The default value is 3 attempts.
- **Password Aging:** By enabling the password aging feature (Figure 70), there will be a maximum time limit for the user's password after which the user will be required to change it. The default value is disabled.

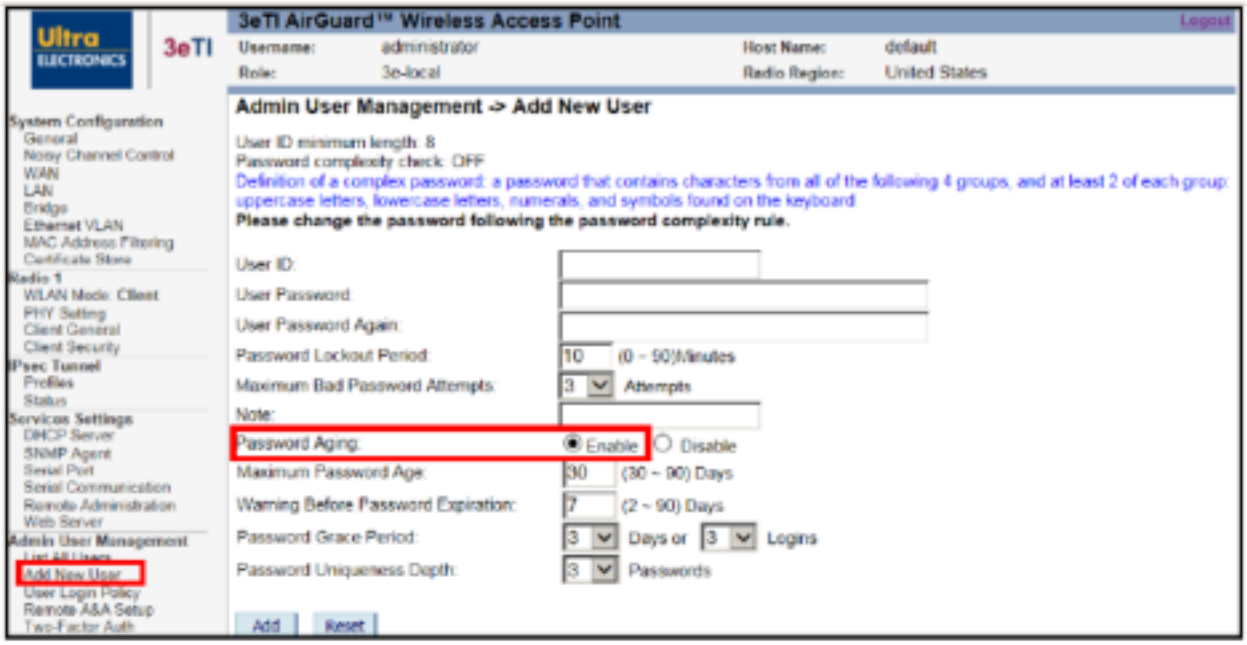


Figure 70: Password Aging

- **Maximum Password Age:** If this account is inactive for this number of days, the account will be considered as disabled. The user will be forced to change his password to re-enable the account. The default password age value is 30 days.
- **Warning Before Password Expiration:** The user will be warned this number of days before his/her password expires. The default value is 7 Days.
- **Password Grace Period:** The user will have a grace period of this number of day or successful logins after the password expires in order to change the password. After the grace period, the user interface will be locked except for the Edit User page forcing the user to change the password. The default grace period is 3 Days or 3 Logins.
- **Password Uniqueness Depth:** The user will be prevented from using this number of pervious passwords. The default value is 3 previous passwords.

2.7.3 User Login Policy

The **Admin User Management - User Login Policy** screen (Figure 71) allows you to configure options governing user login policy and associated device functionality. The "User Login Policy" applies to all local users.

Figure 71: Admin User Management — User Login Policy

You can choose to Enable or **Disable** (default) the **Password Complexity Check.** The definition of a complex password is a password that contains characters from all of the following 4 groups and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard.

Additional Options can be configured:

- **Minimum Password Length:** Enter a value between eight (8) and 30 characters; the default is 8. Note that password lengths of up to 30 characters are supported. Passwords that are longer than 30 characters will be truncated when creating a user or changing passwords for an existing user,
- **Login Session Timeout:** Enter a value between three (3) and 60 minutes; the default is 10. If the admin user session is inactive for more than the timeout amount, then the login session automatically terminates.
- **Display Successful Login Count in Past:** Enter a value between one (1) and 365 days; the default is 7 days. The successful login count will be displayed within the period of the time is set after successful login to the Web GUI.

NOTE: If you make changes to the password rules, all users will be required to change their passwords, even those users' passwords that already meet the new password rules. Because the password information is encrypted, the device cannot determine whether any existing passwords meet the new criteria.

The default for the **Account Lockout Email Notification** is set to "Disable". If enabled, the system will send an email to the email address listed to inform that person that a user has been locked out of the system. To configure the email notification settings, go to the **System Administration – Email Notification Configuration** screen (Figure 87).

2.8 Remote Authentication and Authorization

The 3e-520 series devices offer both local and remote user authentication. Local authentication is done via username and password. When the user accesses the 3e-520 series device URL, he/she inputs username and password, the 3e-520 series device authenticates the user with its local on-device username/password then authorizes the user based on local user privilege policy.

When there are multiple 3e-520 series devices in a deployment, it becomes cumbersome to manage user add/delete/change password locally on each device. For this type of scenario, the 3e-520 series devices offer a centralized authentication and authorization framework. User's authentication and privileges can be centrally managed at enterprise level and uniformly enforced. The 3e-520 series device uses the Lightweight Directory Access Protocol (LDAP) to authenticate username and password against an Active Directory Server.

The 3e-520 series uses LDAP over TLS protocol (LDAPS) for a secure connection to the remote server and verifies the server identity via a trusted root CA. The LDAP server's trust anchor must be loaded into the 'Certificate Store' as shown in Section 2.3.9. Additionally, an IPsec tunnel can be setup to further secure the connection between the 3e-520 series devices and the Active Directory server.

2.8.1 Remote A&A Setup

To reach the 3e-520 series 'Remote Authentication & Authorization Setup' page click on the 'Remote A&A Setup' menu under the Admin User Management sub-heading on the left panel of web GUI. (See Figure 72) Click the 'enable' option on the 'Remote Authentication & Authorization Feature' section. Next, under the 'LDAP Server Configuration' section, enter the LDAP server URI (hostname or IP address), and optional port number if LDAP server is running on non-standard port. e.g. ldaps://openldap.ultra-3eti.com:999

If an IPsec tunnel connection to the LDAP server is required, click on the 'IPsec Tunnel' checkbox. Select an IPsec tunnel profile from the drop-down window if a profile had been created (See Section 0 **Error! R eference source not found.**). Also, if required, check the 'Specify IPsec ID' checkbox and enter the ID in the next field down.

Next, enter User Search Format, the search format consists of the Fully Qualified DN as a flexible regular expression. The 3e-520 series device binds to the LDAP server using this distinguished name after substituting the '*' character with the username provided on the login screen. For example,

"uid=*,ou=people,dc=ultra-3eti,dc=com"

The 3e-520 series device would replace the "*" in this search string with the username input from web GUI login page to construct a bind DN.

"uid=john,ou=people,dc=ultra-3eti,dc=com"

LDAP server will return "*Invalid Credential*" if the username and password combination does not match any record on server. Or it will return the group membership that user belongs to.

e.g. *memberOf: cn=3e-local,ou=Group,dc=ultra-3eti,dc=com*

Click **Apply** to save your selections.

Figure 72: Admin User Management – Remote A&A Setup

2.8.2 Remote A&A User Groups

As discussed in Section 1.4.1 'User Roles', any of three roles can be assigned to Remote A&A users: '3e-local', '3e-CryptoOfficer', and '3e-administrator'. Users/roles created at the centralized management server are independent of users created locally at the 3e-520 series device.

Three role groups can be created at the centralized management server, users can then be assigned to the appropriate group. Table below describes User Groups/Roles and shows a list of major privileges.

Table 15: User Group Role & Privilege in LDAP Server

LDAP Group	Privilege				Note
	Local User Database Manipulation	LDAP Server Setting	Encrypt Algorithm/Key, etc. Security Related Setting	Other	
3e-local	Y	Y	Y	Y	Small number of users, e.g., device owners.
3e-CryptoOfficer	N	N	Y	Y	Most device maintainers fall in this group.
3e-administrator	N	N	N	Y	Users no "need-to-know" security related setting

2.8.3 LDAP Server Configuration

An Active Directory / LDAP server can be configured to the remote management of user authentication. To set up the Active Directory / LDAP server, you need to create three (3) user groups in Active Directory:

- 3e-local,
- 3e-CryptoOfficer, and
- 3e-administrator.

The remote user will be associated with one of these three (3) groups in the 'memberOf' attribute. The 3e-520 series device would authenticate the remote user's username & password against the LDAP server by querying the 'memberOf' attribute of the user. The group info ('memberOf' attribute) of the user will be returned from the LDAP server to the 3e-520 series device to grant the privilege of the user for remote management access.

2.9 Two-Factor Authentication

2.9.1 Two-Factor Authentication Overview

The remote management of 3e-520 series devices can be configured with Two-Factor authentication by utilizing CAC (Common Access Card) authentication and Remote LDAP Server authentication. The first factor authentication uses CAC certificate and pin authentication via trusted chain CAs and OCSP responder server. The second factor is to use CAC username & password to authenticate via LDAPS to the remote LDPS server.

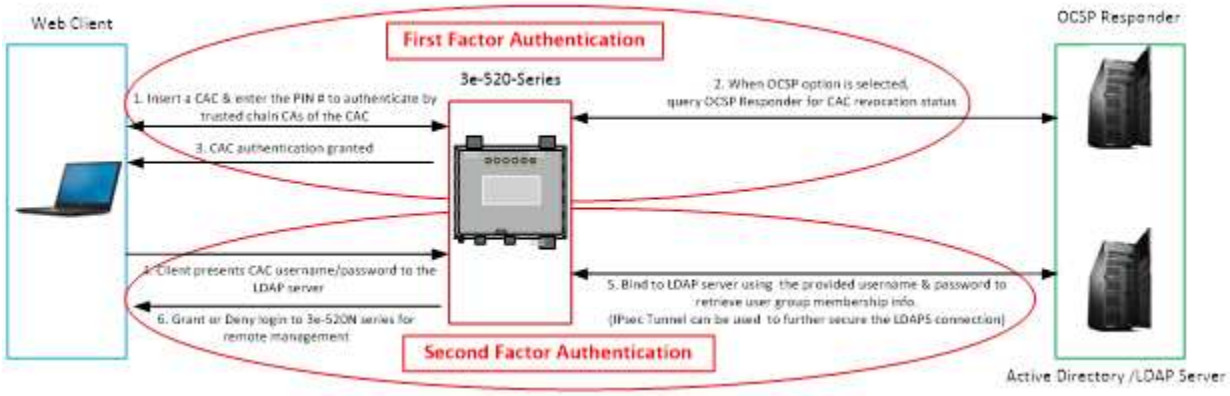


Figure 73: Two-Factor Authentication Overview

User with a valid CAC is authenticated to gain access to the 3e-520 series device web management interface. The 3e-520 series device optionally uses the Online Certificate Status Protocol (OCSP) to query OCSP Responder for CAC revocation status. Only if OCSP responder replies with a "good" certificate status would 3e-520 series device allow the authentication process to continue.

The following components are required to implement and operate a PKI network providing Two-Factor authentication of 3e-520 series device, see Figure 73 for the components that make up a PKI network.

2.9.1.1 Web Client

To Access Web GUI remotely with CAC authentication, the following requirements should be configured in the Web Client and 3e-520 series device.

- Only Windows Internet Explorer / Edge Web Browser supports CAC authentication.
- ActiveCard software and SmartCard reader driver are installed in the Web Client.
- The SmartCard service is enabled and running (from Windows Services).
- The Certificate Propagation service is enabled & running (from Windows Services).

2.9.1.2 OCSP Responder

If "Enforce OCSP check" is enabled on 3e-520 series device, an OCSP responder is required to be installed and setup in the network. Software such as Tumbleweed Validation Authority running on Windows Server platform can be configured as an OCSP responder. DoD CA-23 certificate and any corresponding CRL can be loaded to the OCSP Responder from a local file. Current DoD certificates and CRLs can be obtained from https://crl.chamb.disa.mil/.

2.9.2 First-Factor Authentication—CAC and OCSP

Before enabling Two-Factor Authentication, the Remote A&A needs to be enabled first. You also need to upload the certificate trust chain CAs (intermediate CA and Root CA) of the CAC to the Certificate Store of the 3e-520 series device. If the OCSP Responder is used, you need to upload the OCSP Signer Certificate to the device's Certificate Store as well.

To reach the 3e-520 series 'Two-Factor Authentication Setup' page click the '**Two-Factor Auth**' under the **User Management** sub-heading on the left panel of web GUI. See Figure 74: **Admin User Management – Two-Factor Authentication** below. Click the 'enable' option on the 'Two-Factor Authentication' Section. Next, under the 'CAC OCSP Responder Configuration' Section, select either Enforce or Skip OCSP Check. If Enforce OCSP Check is selected, select either Nonce is been used or not. Then Enter Primary URL and/or Secondary URL of the OCSP Server. Select a previous uploaded OCSP Responder Certificate from the list then click on Apply.

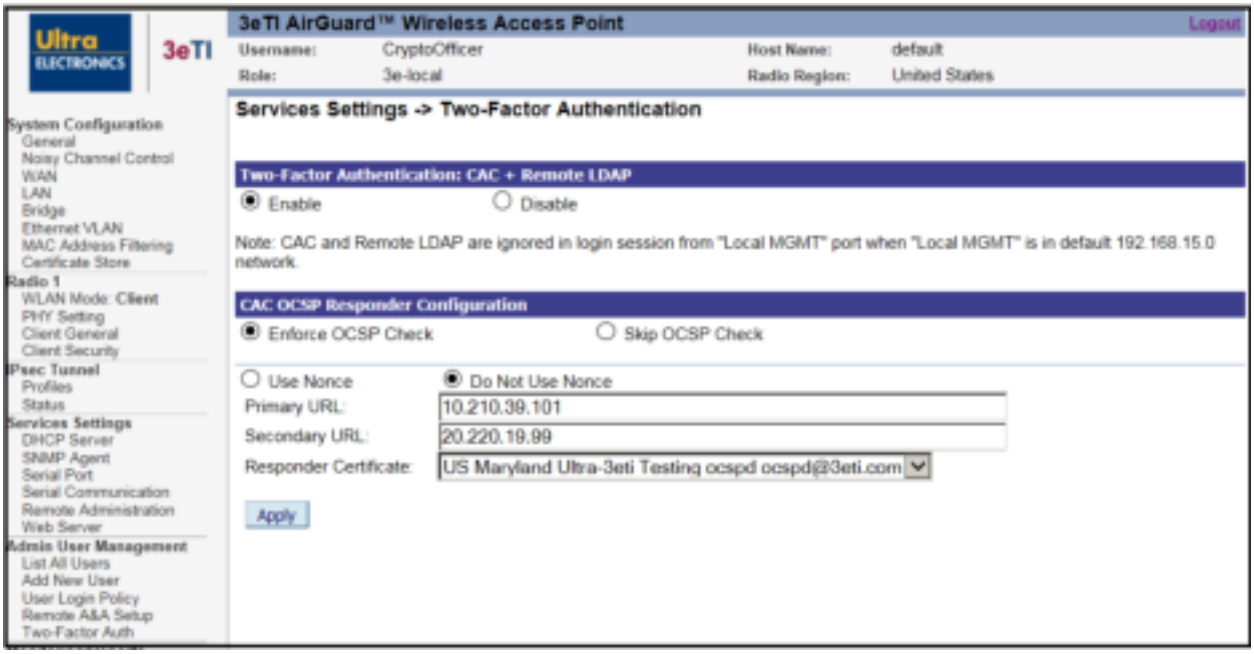


Figure 74: Admin User Management – Two-Factor Authentication

2.9.3 Second-Factor Authentication—LDAP Server

After the CAC authentication is granted, the username in the CN attribute of the CAC certificate along with its password will be sent to the LDAP server for authentication. If the authentication succeeds, the user group membership is retrieved from the LDAP server and used as privilege information for the remote

management. An IPsec tunnel can be used to further secure the LDAPS connection. Please refer to Section 2.8 Remote Authentication and Authorization for more detail.

Note: Two-Factor Authentication configuration change will take effect after device reboot.

2.10 Monitoring/Reports

This section gives you a variety of lists and status reports. Most of these are self-explanatory.

2.10.1 System Status

The **Monitoring/Reports - System Status** screen (Figure 75) displays the status of the unit, system status information include:

- System Uptime,
- Total Usable Memory size,
- Free Memory,
- Current Processes,
- Door Status (Open/Close status is detected by serial port connection),
- CPU Info,
- WAN Ethernet MAC address,
- LAN Ethernet MAC address,
- Radio 1 & 2 MAC address, and
- Routing Table.

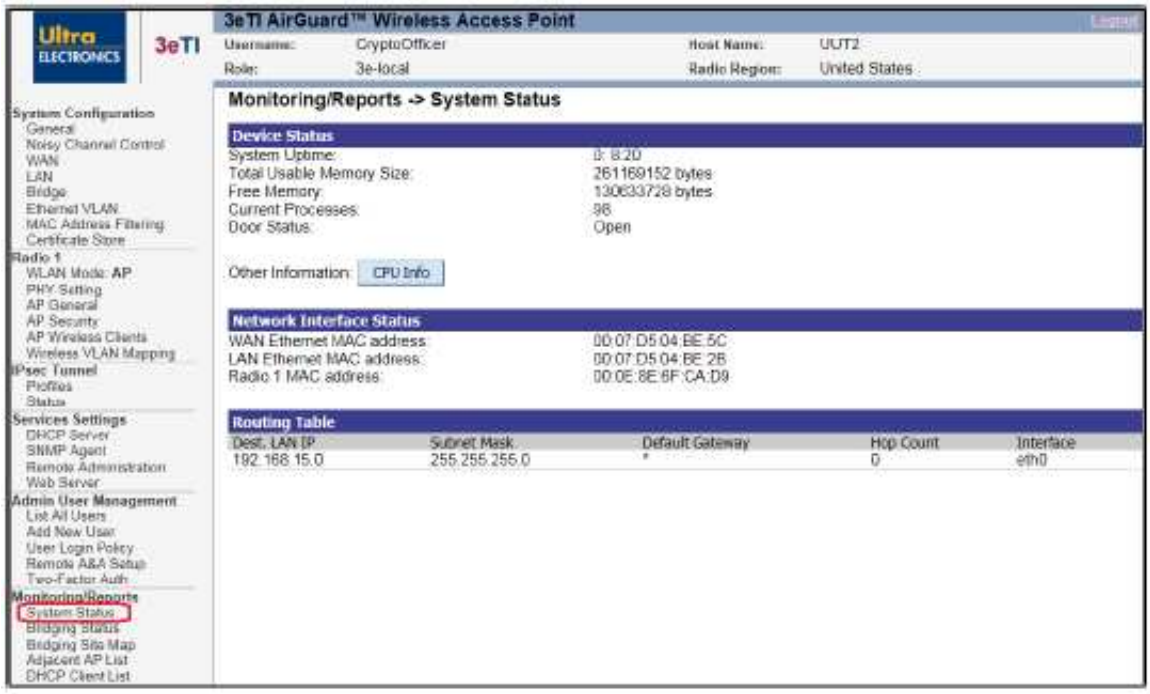


Figure 75: Monitoring/Reports — System Status

2.10.2 Bridge Status

The **Monitoring/Reports - Bridge Status** screen (Figure 76) displays the Spanning Tree Protocol (STP) status for each port, as well as associated **Bridge Information** for the device.

Ethernet Link STP Status: This is for the Uplink Ethernet port of the device. This screen displays current STP parameters for this port.

Bridge Information: This screen displays current STP parameters for the bridge link.

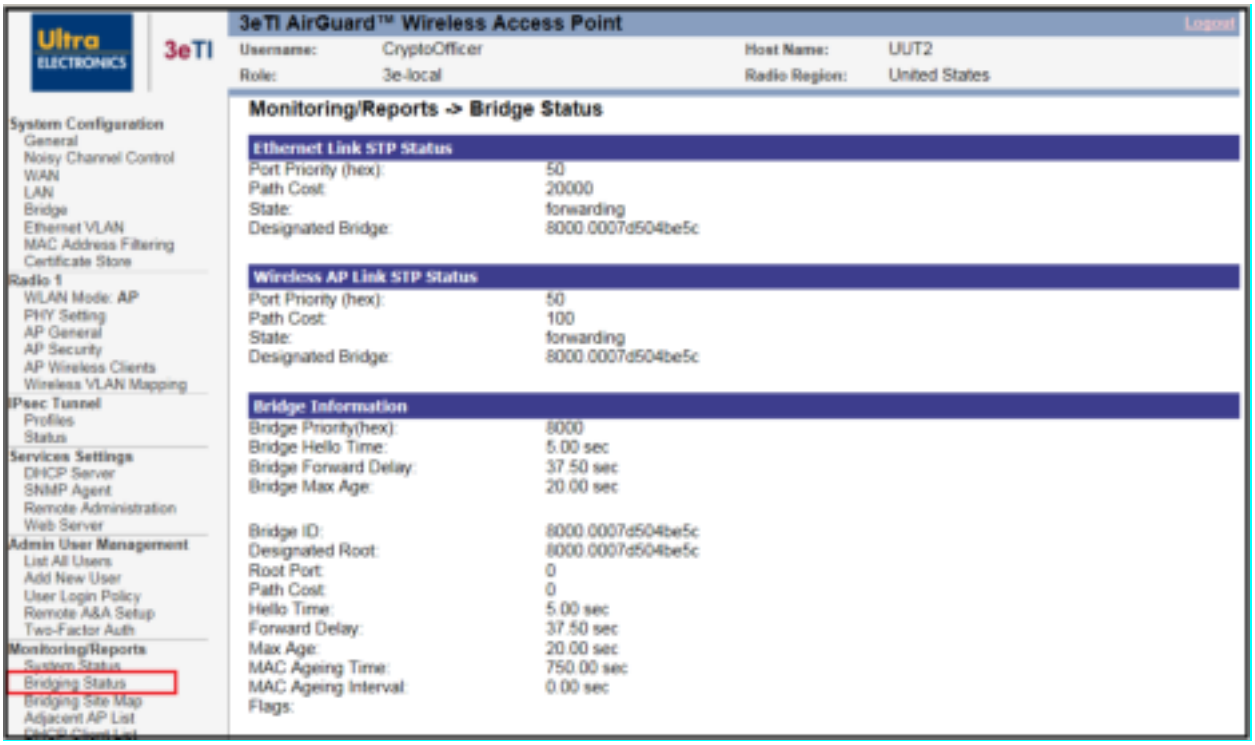


Figure 76: Monitoring/Reports — Bridge Status

2.10.3 Bridge Site Map

The **Monitoring/Reports – Bridging Site Map** screen (Figure 77) shows the spanning tree network topology of both wired and wireless nodes connected to the network. The root STP node is always on top and the nodes of the hierarchy are displayed below it. Wired links are double dotted lines and wireless links are single dotted lines.

NOTE: This map does not update dynamically. You must press the **Update** button to refresh the map.

Figure 77: Monitoring Reports — Bridging Site Map

2.10.4 Adjacent AP List

The **Monitoring/Reports – Adjacent AP List** screen (Figure 78) shows all the APs on the network. These APs are detected by the device's radio(s). The list of APs is only within the band that can be seen from a particular channel. For example, if the AP is on channel 1, it will display APs on channels 1-3.

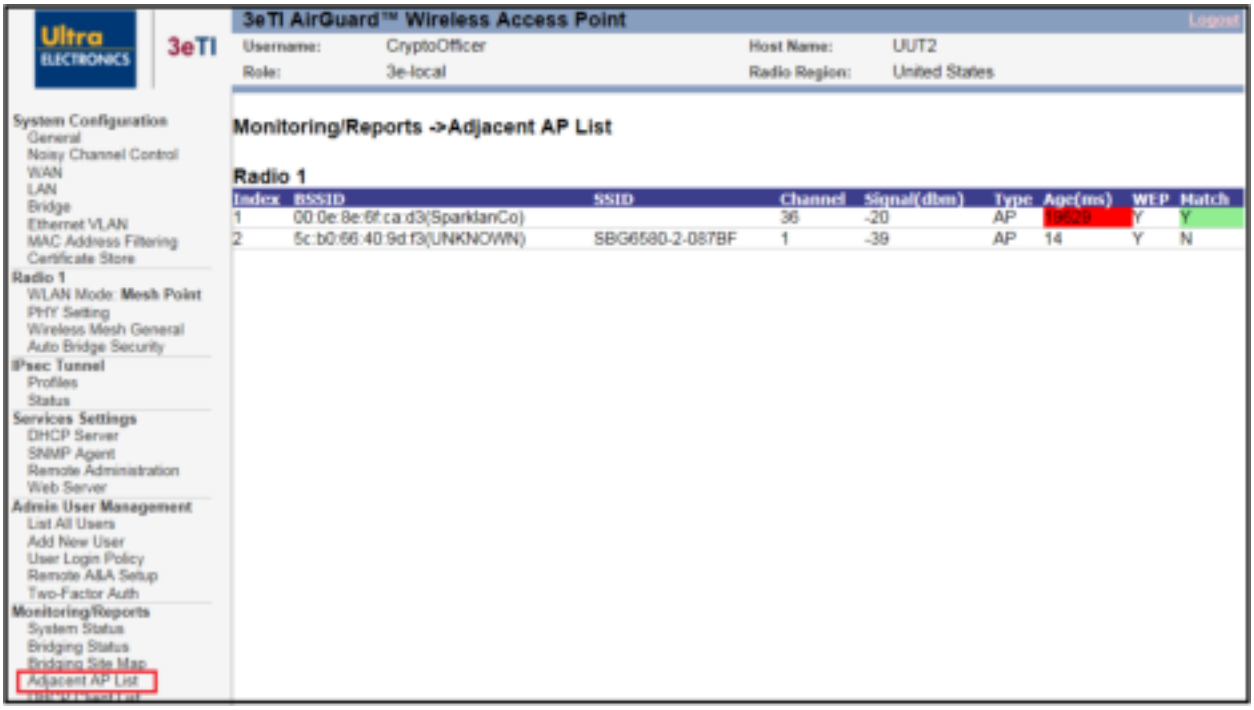


Figure 78: Monitoring/Reports — Adjacent AP List

2.10.5 DHCP Client List

The **Monitoring/Reports - DHCP Client List** screen (Figure 79) displays all clients currently connected to the unit via the DHCP server, including their reference **Index**, **Hostname**, **IP Address**, and **MAC Address**. It also indicates an **Expired at Date** for the client, based on the displayed DHCP server lease period.

The DHCP Client list constantly collects entries. To remove entries from the list, check mark the **Revoke Entry** selection and click **Remove** to confirm the action.

Figure 79: Monitoring/Reports — DHCP Client List

2.11 Logs

2.11.1 System Log

The **Logs – System Log** screen (Figure 80) displays System Facility Messages with a Date-Time stamp. These are messages documenting functions performed internal to the system, based on the system's configured functionality. The system log records all the general system activity, operation and alerts information during the device running. For example, the system log records the device boots up, software version, management access and self-test record, etc. Generally, the administrator would only use this information if trained as, or working with, a field engineer or if gathering information to be provided to technical support.

The System Log (syslog) continues to accumulate listings until it reaches its 256KB size limit. The log rotates by overwriting the first 1/3. For security reasons, the system log cannot be cleared.

If you choose to **Export** the syslog, it can be opened or saved as an HTML document.

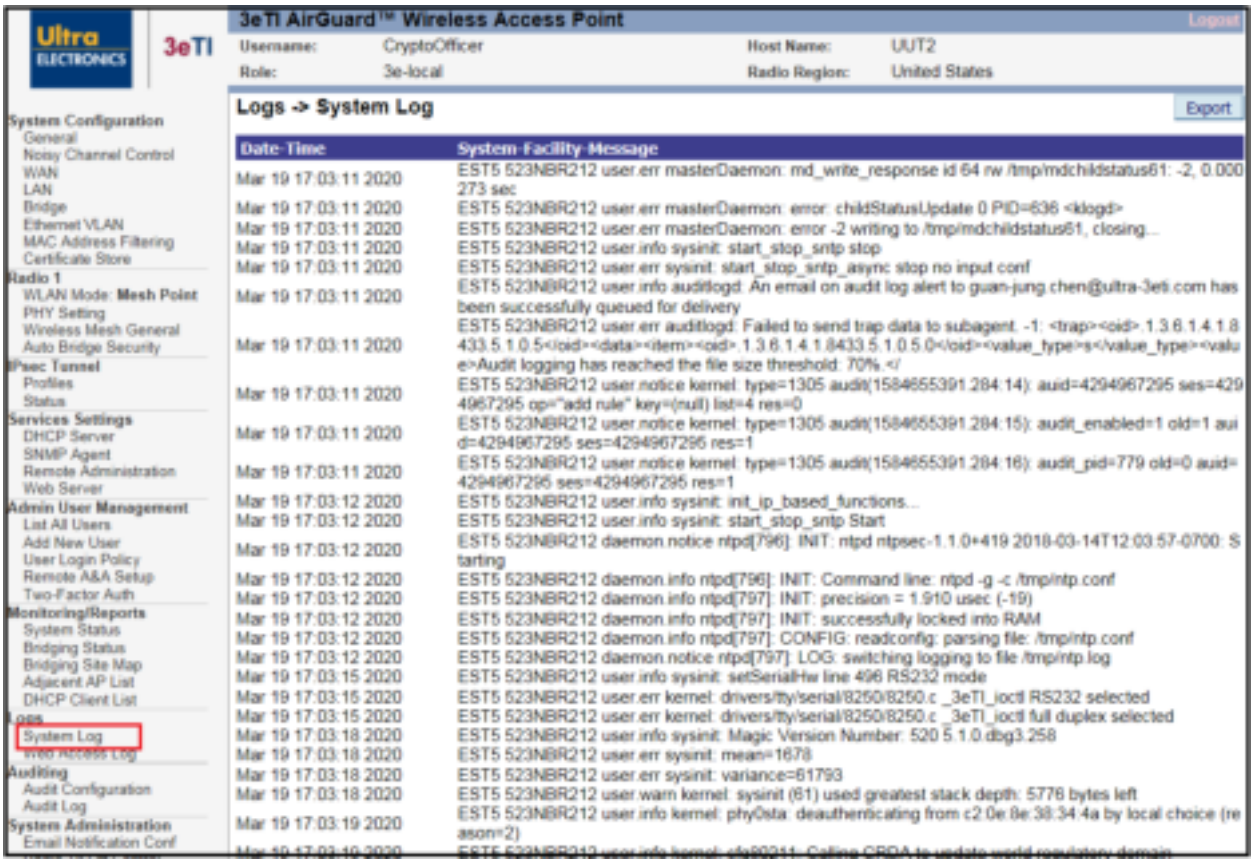


Figure 80: Logs – System Log

2.11.2 Web Access Log

The **Logs – Web Access Log** screen (Figure 81) displays System Facility Messages with a Date-Time stamp for any actions involving web access. All configuration operation access via web GUI will be logged. For example, web access log records when you set encryption mode, change operating mode, etc., using the web browser. It establishes a running record regarding what actions were performed and by whom.

The Web Access Log (Weblog) will continue to accumulate listings until it reaches its 10KB size limit. The log rotates by overwriting the first 1/2. For security reasons, the Weblog cannot be cleared.

To remind the administrator that the log will be overwritten soon, this device will send a notification email when the Weblog size reaches 50%. The device also provides a configurable "Weblog alert point" and "Weblog alert email" address. When the Weblog grows over the Weblog alert point, an email is automatically sent to the configured Weblog alert email address. Note that an email will be sent only once at the alert point before the Weblog rotates and begins overwriting data.

NOTE: The Weblog alert email address and email server need to be properly configured. Refer to Section 2.13.1 Email Notification Configuration for more information on server configuration.

If you choose to Export the weblog, it can be opened or saved as an HTML document.

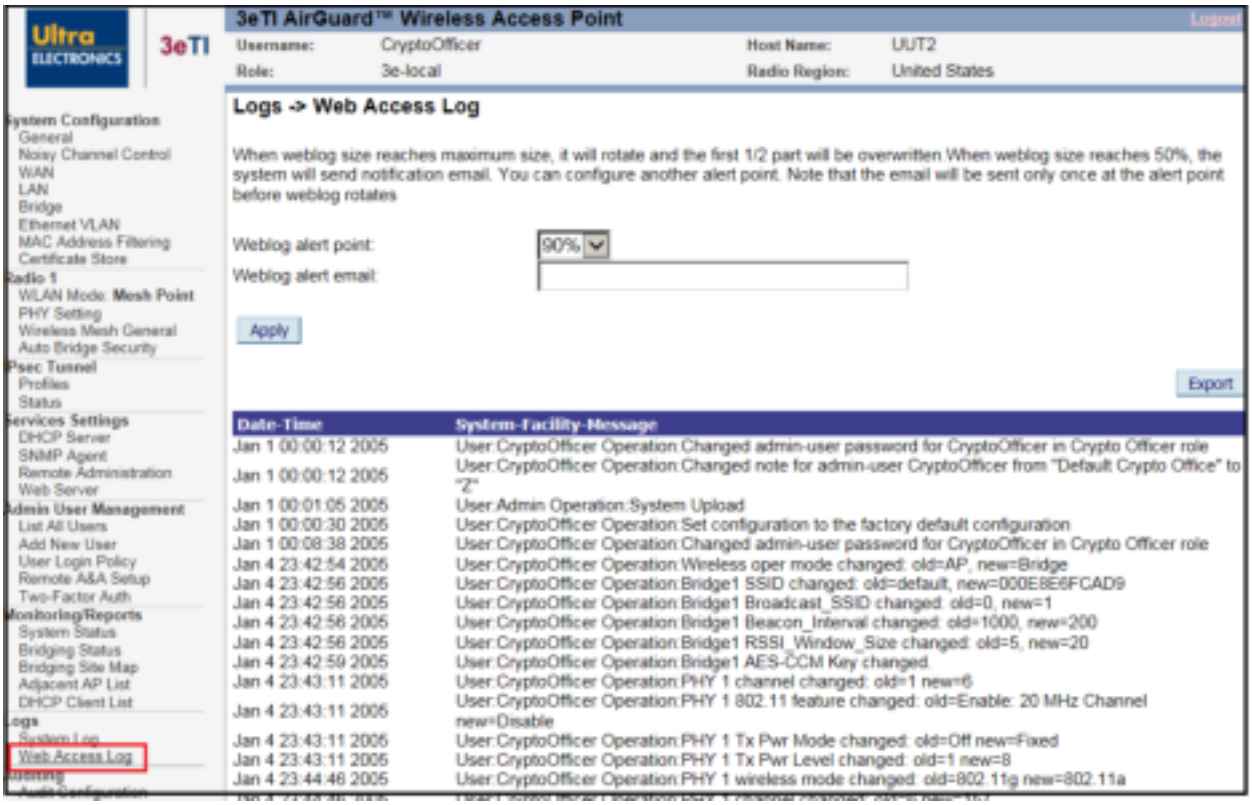


Figure 81: Logs – Web Access Log

2.12 Auditing

The unit collects audit data and provides an interface for authorized administrators to review generated audit records. It generates records for two separate classes of events: authentication/access to the system, and actions taken directly on the system. All audit records include the date/time of the event, the identity associated with the event (such as the service, computer or user), the success/failure of the event and a definition of the event (by code or explanation).

Every start and stop of the audit service are noted in the audit record. For audit events resulting from actions of identified users, the unit associates each auditable event with the identity of the user that caused the event. The unit includes or excludes auditable events from the set of audited events based on object identity, user identity, subject identity, host identity, and event type.

The Auditing screens contain auditing functions for the system. The screens and functions are detailed in the following subsections.

2.12.1 Audit Configuration

The **Auditing – Configuration** screen (Figure 82) is used to configure the auditing settings. You can enable or disable the auditing function on this screen. You can select which audit event types you wish to log. Table 16 lists event types and descriptions. The figure below describes the attributes for audit log selection, the user can also specify audit logs for a particular administrator by inputting the user ID in the text box.

NOTE: Many of these event notifications cannot be disabled for security reasons. They are displayed for reference only.

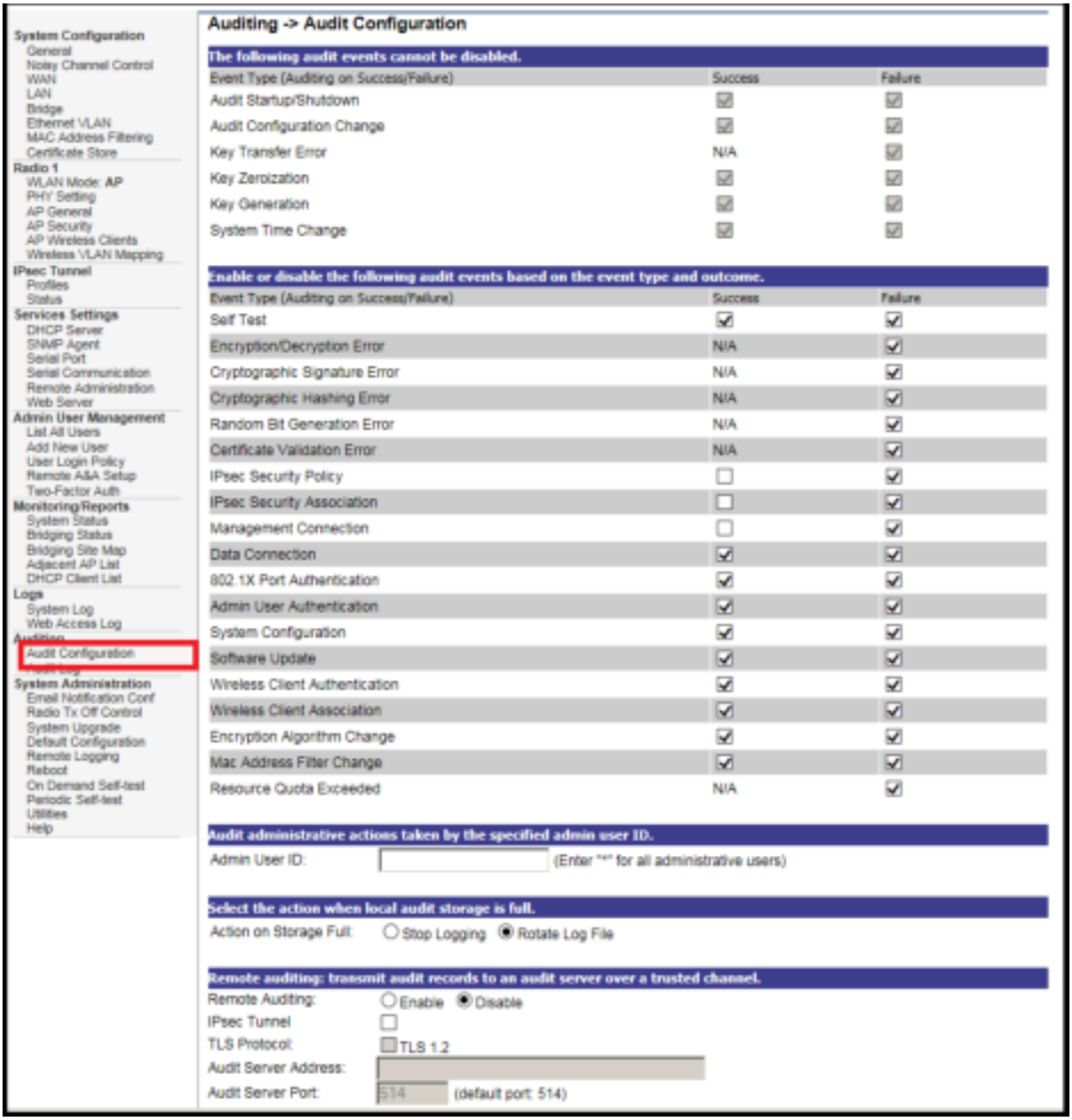


Figure 82: Auditing – Configuration

Table 16: Auditing – Configuration Event Types and Description	
Event Type	**Description**
Audit Startup Shutdown	Audit record generated when the audit service is started or stopped. This record cannot be disabled.
Audit Configuration Change	Any modification to the audit log configuration (enable/disable, recorded event types, etc.) will trigger the creation of an audit record. Cannot be disabled.
Key Transfer Error	Any error detected during the dynamic key exchange, either to the station or the authentication server. Cannot be disabled.
Key Zeroized	The keys are zeroized including: 1. Transitioning from static key to DKE (and vice versa) 2. Transitioning to bypass mode Individual log messages appear from the application and driver since keys are held in both locations. Cannot be disabled.
Key Generation	These events are logged anytime a newly generated key is introduced in AP either via web GUI or internally. Cannot be disabled.
System Time Changed	Whenever the time is changed via the GUI or at bootup if the time is within two minutes of 11/30/1999, 0hr, 0min. Cannot be disabled.
Self-test	Self-test Results. Default is to log success and failure.
Encryption Decryption Error	Failure of encryption or decryption. Default is to log failure.
Cryptographic Signature Error	Failure or cryptographic signature. Default is to log failure.
Random Bit Generation Error	Failure of randomization process. Default is to log failure.
Certificate Validation Error	Failure of certificate validation. Default is to log failure.
IPsec Security Policy	Success or failure of a packet crossing the IPsec Security Boundary. Default is to log failure only.
IPsec Security Association	IPsec Security Association success or failure. Default is to log success and failure.
Management Connection	Managed WEB TLS connection to the device. Default is to log success and failure.
Data Connection	No events are generated for wireless device.
802.1X Port Authentication	Wireless client authentication. Default is to log success and failure.
Admin User Authentication	Administrative user authentication, logout and lockout. Default is to log success and failure.
System Configuration	System configuration changes through the WEB management interface. Default is to log success and failure.
Software Update	System firmware updates. Default is to log success and failure.
Wireless Client Authentication	A station's authentication request is audit logged on success or failure. Default is to log both success and failure.
Wireless Client Association	A station an attempt to associate. Default is to log success and failure
Encryption Algorithm Changed	The encryption algorithm is changed, including bypass mode. Default is to log success and failure.
MAC Filter Changed	The MAC address filter is changed including adding/deleting, enable/disable, and changing filter type. Default is to log success and failure
Resource Quota Exceeded	Wireless client denied association due to resource limitation. Default is to log client denial.

2.12.1.1 Audit Records Limited by Admin User ID

In addition to limiting audit records by event type, the device can further limit records based on administrative user ID. To limit audit logging to only events associated with an administrative user, add the username to the 'Admin User ID' attribute.

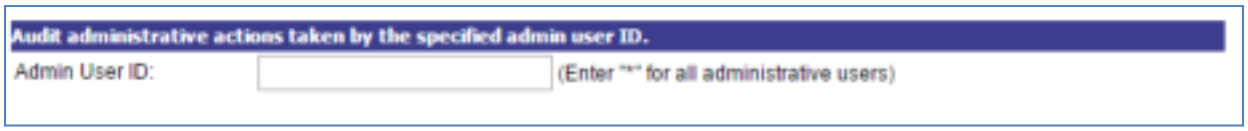


Figure 83: Audit Records Limited By User ID

2.12.1.2 Audit Record Local Storage Action

Audit log records are stored locally on the device in 256K of persistent memory. Once this memory is full, new audit record will rotate out the oldest records and the old records will be lost. Alternatively, the audit service can be configured to stop logging when the local storage is full. The default behavior is to rotate the audit log.

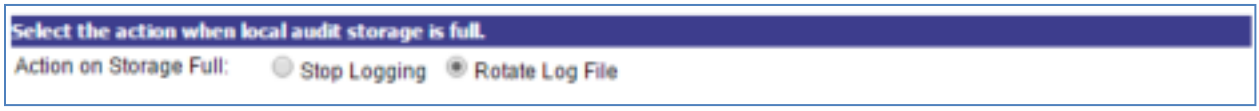


Figure 84: Audit Record Local Storage Action

2.12.1.3 Remote Audit Log Configuration Details

The remote logging feature is similar to remote sys logging except it optionally provides a TLS session over which to communicate. This feature will work with syslog servers supporting TLS 1.2. When remote audit logging is enabled, all audit log records will be stored locally, and duplicate records will be sent to the remote audit log server.

Note: Only the user with 3e-Local or 3e-CryptoOfficer role may change the audit log configuration.

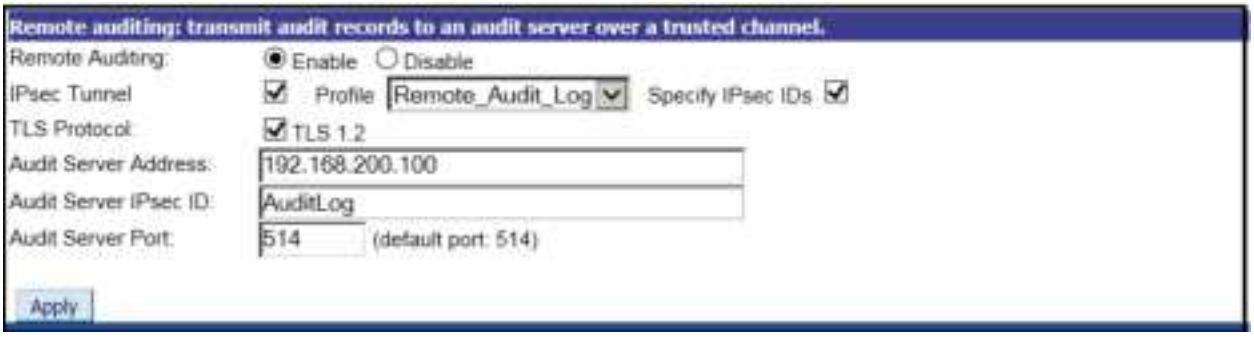


Figure 85: Remote Audit Logging with IPsec Tunnel

Remote Auditing: Enable or disable the remote logging of audit events.

IPsec Tunnel: When checked will further protect the remote audit log records by sending them within an IPsec tunnel. Check the box and select an IPsec Tunnel Profile. An IPsec Tunnel Profile must be configured before IPsec can be used to protect the audit log packets. See Section 0 in order to configure an IPsec Tunnel Profile. For Common Criteria compliance, the user must select this option to use IPsec tunnel to connect with audit log server. If the "Profile" drop-down list is empty, the user shall go to the IPsec

configuration screen to create a "Profile", in which the user will specify the peer IP address, certificates used for peer authentication and ESP encryption options. To view the IPsec tunnel status, user should refer to Section 2.5.2. In case of IPsec tunnel connection failure, the user can see the IPsec status and the device will continue to try establishing the tunnel will save the log to local storage. Once the tunnel is reestablished, the device will try to sync its local audit log with the remote server.

During the authentication phase of the IPsec protocol, the 3e-520 series (Initiator) will specify to which of the remote audit server's (Responder's) identities it wants to communicate with. Most remote audit servers will have one IPsec identity bound to the server's IP address. By default, the 3e-520 series will talk to this identity. There are instances where a remote audit server may host multiple IPsec identities. In this case, the desired identity can be specified by checking the "Specify IPsec IDs" check box and supplying an IPsec identity. If PKI certificate-based authentication is configured for the IPsec tunnel, the "IPsec IDs" field will match with the peer certificate's entire DN or A SAN:DNS name.

TLS Protocol: When the protocol is left un-checked, the audit log records will be transmitted over a TCP socket. By checking the TLS 1.2 protocol, that socket will be authenticated and encrypted using the TLS 1.2 protocol. The device will negotiate with the configured Audit Server for a secured TLS protocol.

Audit Server Address: User-entered string giving the remote server's address. String entry must be either a standard IPv4/v6 address or a valid domain name (see RFC 2181 for more details). Enclose IPv6 addresses in square brackets.

Audit Server Port: User-entered number string for the port number from which the remote logging server is accepting TLS sessions.

2.12.2 Audit Log

The **Auditing – Log** screen (Figure 86) provides a listing of all the audit records. Audit Log records all security related activities and events which are configured in the Audit Configuration setting (see Section 2.12.1).

The Audit Log (Audit-log) will continue to accumulate listings until it reaches its 256KB size limit. The log rotates by overwriting the first 1/3. For security reasons, the Audit-log cannot be cleared.

To remind the administrator that the log will be overwritten soon, this device will send a notification email when the Audit-log size reaches 50%. The device also provides a configurable "Audit-log alert point" and "Audit-log alert email" address. When the Audit-log grows over the Audit-log alert point, an email is automatically sent to the configured Audit-log alert email address. Note that an email will be sent only once at the alert point before the Audit-log rotates and begins overwriting data.

NOTE: The Audit-log alert email address and email server need to be properly configured. Refer to Section 2.13.1, Email Notification Configuration, for more information on server configuration.

If you choose to Export the Audit-log, it can be opened or saved as an HTML document.

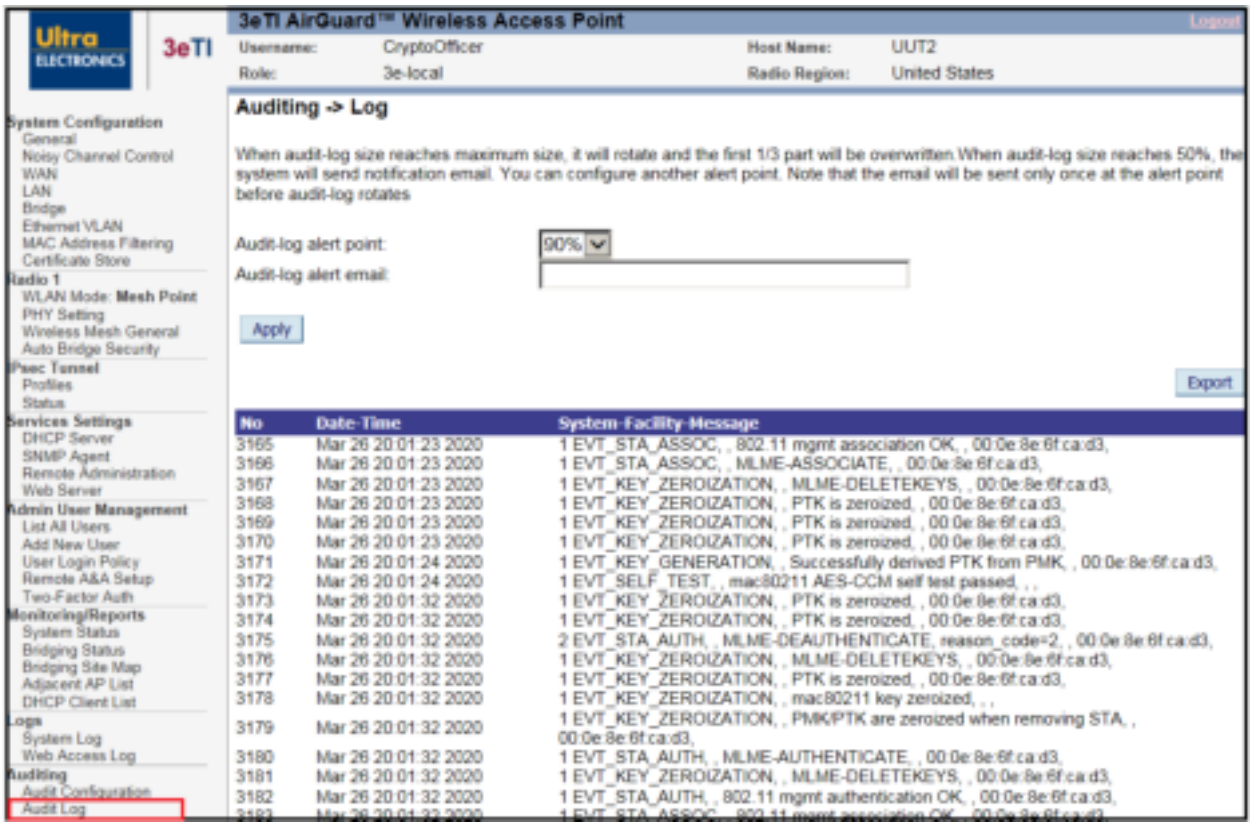


Figure 86: Auditing – Log

2.13 System Administration

The **System Administration** screens contain administrative functions. The screens and functions are detailed in the following section.

2.13.1 Email Notification Configuration

All system notification emails need to be set up using the **System Administration – Email Notification Configuration** screen (Figure 87). Your email server must support SMTP protocol.

If you email server does not require authentication to send email, then leave the username/password fields blank. If your email server does not support TLS 1.2 then disable TLS 1.2. You may also test your email setup using the test feature on this screen.

NOTE: Check your connection to the mail server. Emails sent from the 3e-520 series product family may be queued for a short period if the connection fails temporarily, but it will give up if the connection continues to fail.

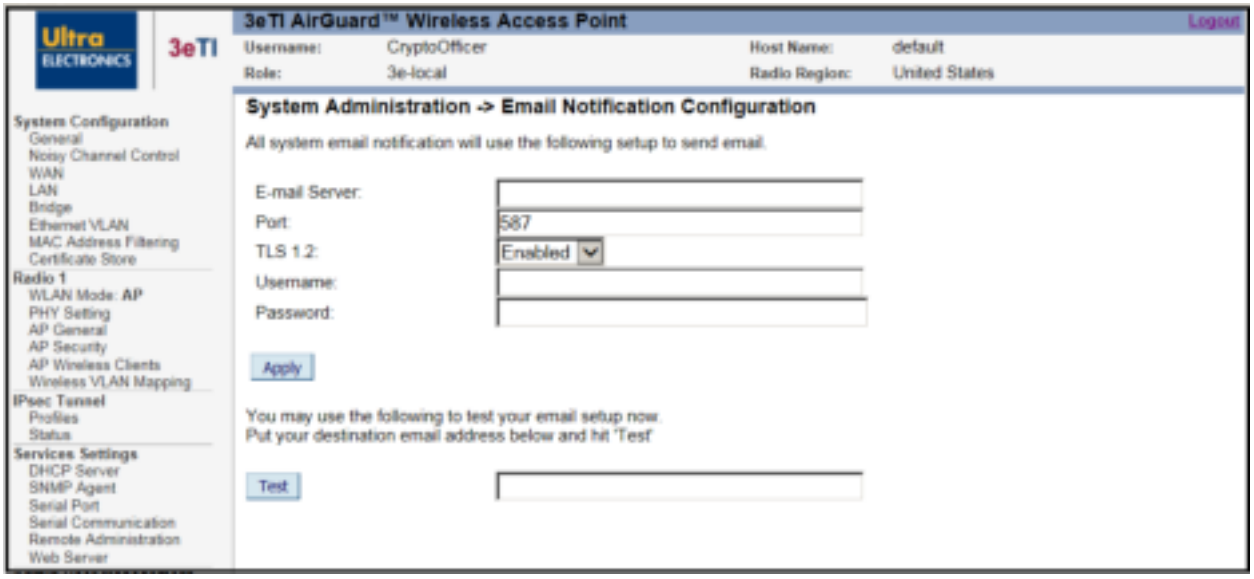


Figure 87: System Administration – Email Notification Configuration

To test the email function, the email address needs to be filled in. Afterwards click on the **Test** button and a pop-up window such as the one shown in Figure 88 will indicate the result of email test.

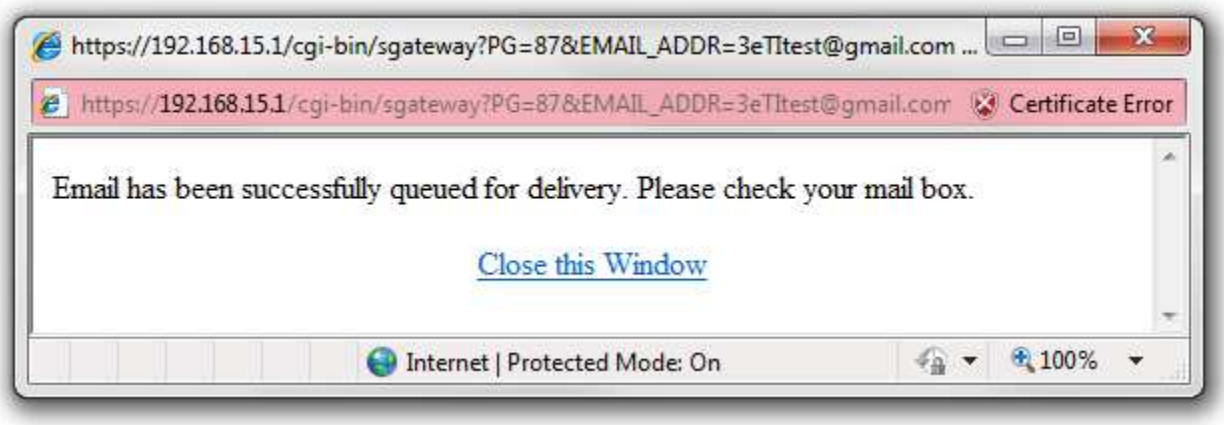


Figure 88: Email Test Result

2.13.2 Radio TX Off Control

The radios can be programmed to turn off and turn on during a specified time in the future as shown in Figure 89. This is typically executed via a management system like WiFiProtect Manager.

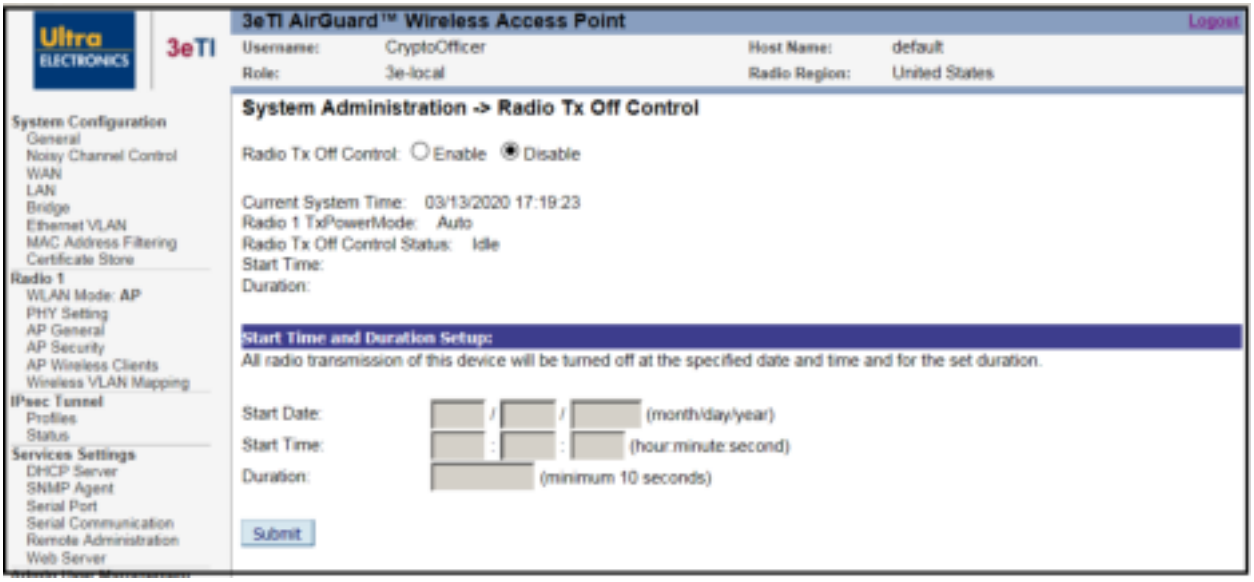


Figure 89: System Administration – Radio TX Off Control

2.13.3 System Upgrade

The **System Administration – System Upgrade** screen (Figure 90) gives you the ability to upload updates to the device's firmware as they become available. When a new upgrade file becomes available, you can perform a firmware upgrade from the Firmware Upgrade window. Normally, the user will first get email notification from 3eTI's product support team. If the user desires to download the new firmware release, a secure download link together with temporary username/password will be provided to the user. The user can download the firmware into local storage, then follows instruction in the section below to tell the device's web UI the local of the firmware.

There is also a configuration file transfer option which allows the system configuration file from one AP to be transferred to another AP, in order to minimize the administration of the APs. Only configuration parameters that can be shared between APs are downloaded in the configuration file. WAN IP address and hostname are not transferred in the configuration file.

Only the user with 3e-Local or 3e-CryptoOfficer role can access this function.

2.13.3.1 Firmware Upgrade

The CryptoOfficer can update the device's firmware. The device uses the public key to verify the digital signature. Upon successful verification, the device will load the new update upon reboot. The update will be rejected if the verification fails.

On the **System Administration – System Upgrade** screen (Figure 90), the **Firmware Upgrade** tab is the default view.

Click on **Browse** and select the firmware file to be uploaded. The device will only accept firmware files that have been digitally signed by 3eTI Click on the **Upload Firmware** button.

Figure 90: System Administration — System Upgrade – Firmware Upgrade

2.13.3.2 Configuration Export/Import

On the **System Administration – System Upgrade** screen (Figure 91) click on the **Configuration Export/Import** tab to upload and download configuration files to APs connected to the network.

To upload a configuration file, select the file using the browse button and enter the passphrase for that file. The passphrase protects the file from unauthorized users. It prevents unauthorized users from applying the system configuration file to an unauthorized AP to gain access to the network. Before downloading the system configuration file to a local computer, the user must enter a passphrase to protect the file. Before the system configuration file can be uploaded onto another AP, the passphrase must be entered on the remote AP.

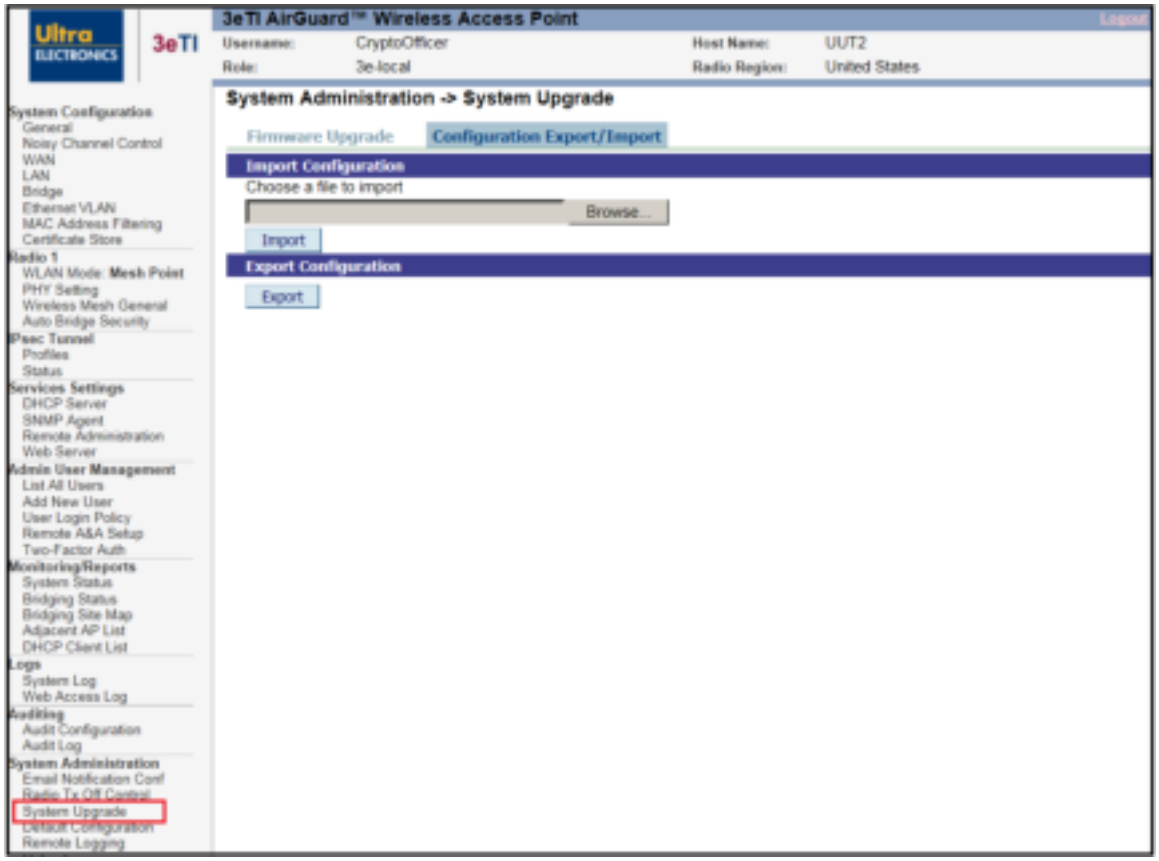


Figure 91: System Administration – System Upgrade – Configuration Export/Import

1) Notes and Tips:

a) When Exporting configuration files, keys are NOT downloaded.

b) When Importing configuration files to a device, if the device currently is configured to the same security options as those in the uploaded file, the keys are reused. Otherwise, the keys are zeroized and marked "key not set" from the web GUI.

e.g.: The current device has the 802.11i-PMK option on AP security. The configured files to be uploaded will use 802.11i-PMK for AP security. The existing 256bit PMK is reused. Otherwise, the AP security is marked "key not set".

c) In a VLAN scenario, VLAN ID (NOT the SSID) is the index to find a matching security option.

e.g.: Current device has 3 VLAN configured as follows:

i) VLAN ID = 1, SSID=area-1, security=802.11i pmk,

ii) VLAN ID = 2, SSID=area-2, security=802.11i-dot1x,

iii) VLAN ID = 3, SSID=area-3, security=static AES.

The configuration file to be uploaded has 4 VLAN configured as follows:

iv) VLAN ID = 1, SSID=test-1, security=802.11i pmk,

v) VLAN ID = 2, SSID=area-1, security=802.11i-dot1x,

vi) VLAN ID = 3, SSID=area-2, security=802.11i pmk,

vii) VLAN ID = 4, SSID=area-3, security=static AES.

The device will have 4 VLANs configured as follows:

viii) VLAN ID = 1, SSID=test-1, security=802.11i pmk (key set),

ix) VLAN ID = 2, SSID=area-1, security=802.11i-dot1x (key set),

x) VLAN ID = 3, SSID=area-2, security=802.11i pmk (key not set),

xi) VLAN ID = 4, SSID=area-3, security=static AES (key not set).

2.13.4 Default Configuration

The **System Administration – Default Configuration** screen (Figure 92) is used to reset the AP to its factory settings.

The **Restore** button is a fallback troubleshooting function that should only be used to reset to last saved general configuration.

The **Save** button can save the current general configuration to be restored in the future.

The **Reset** button can be used to reset and restore the configuration to the factory default settings.

Only the user with 3e-Local or 3e-CryptoOfficer role has access to the **Default Configuration** page.

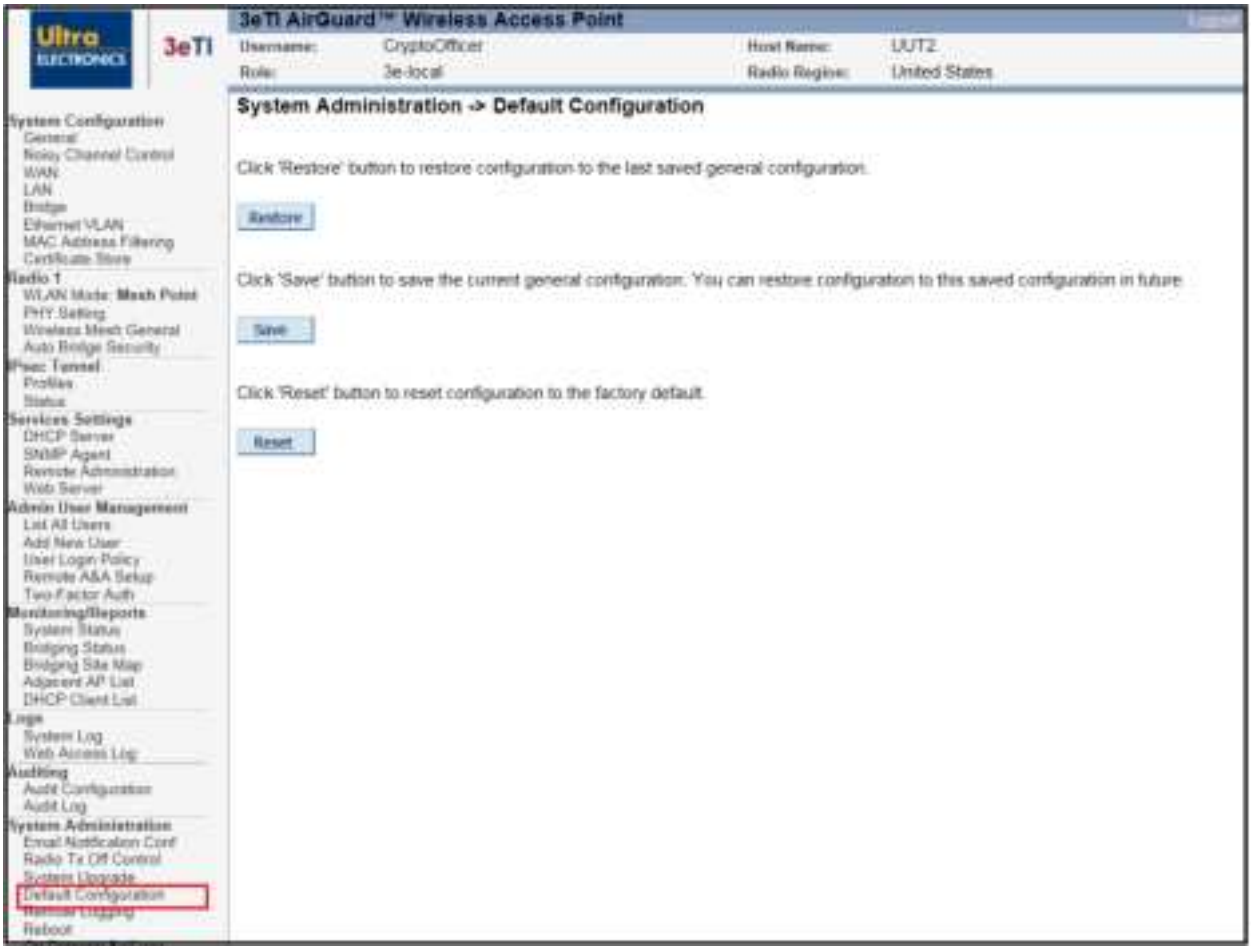


Figure 92: System Administration — Factory Default

2.13.5 Remote Logging

The **System Administration – Remote Logging** screen (Figure 93) allows you to forward the ***syslog*** data from each machine to a central remote logging server. In the unit, this function uses the ***syslogd*** daemon. If you enable Remote Logging, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.

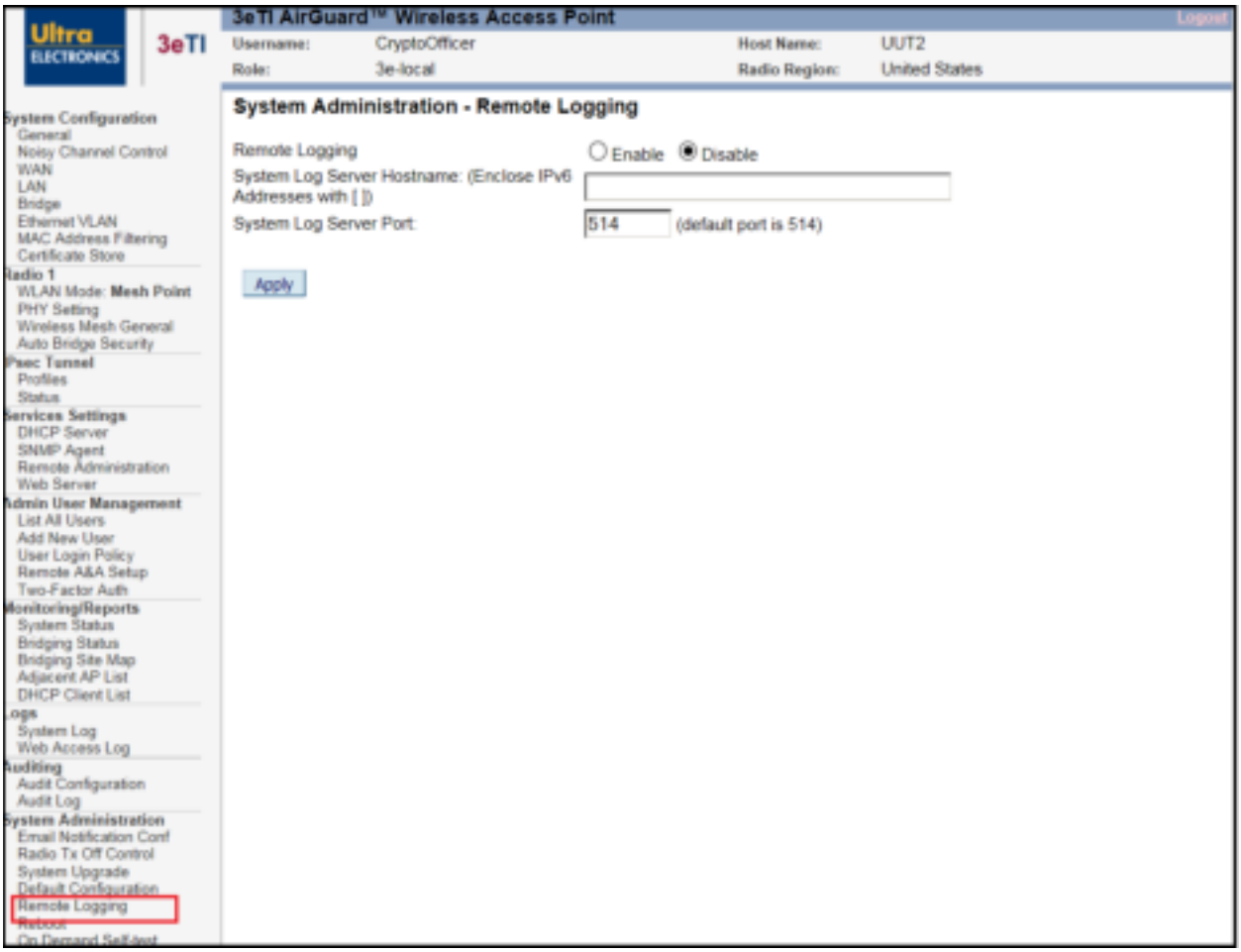


Figure 93: System Administration — Remote Logging

2.13.6 Reboot

The **System Administration – Reboot** screen (Figure 94) allows you to reboot the unit without changing any preset functionality.

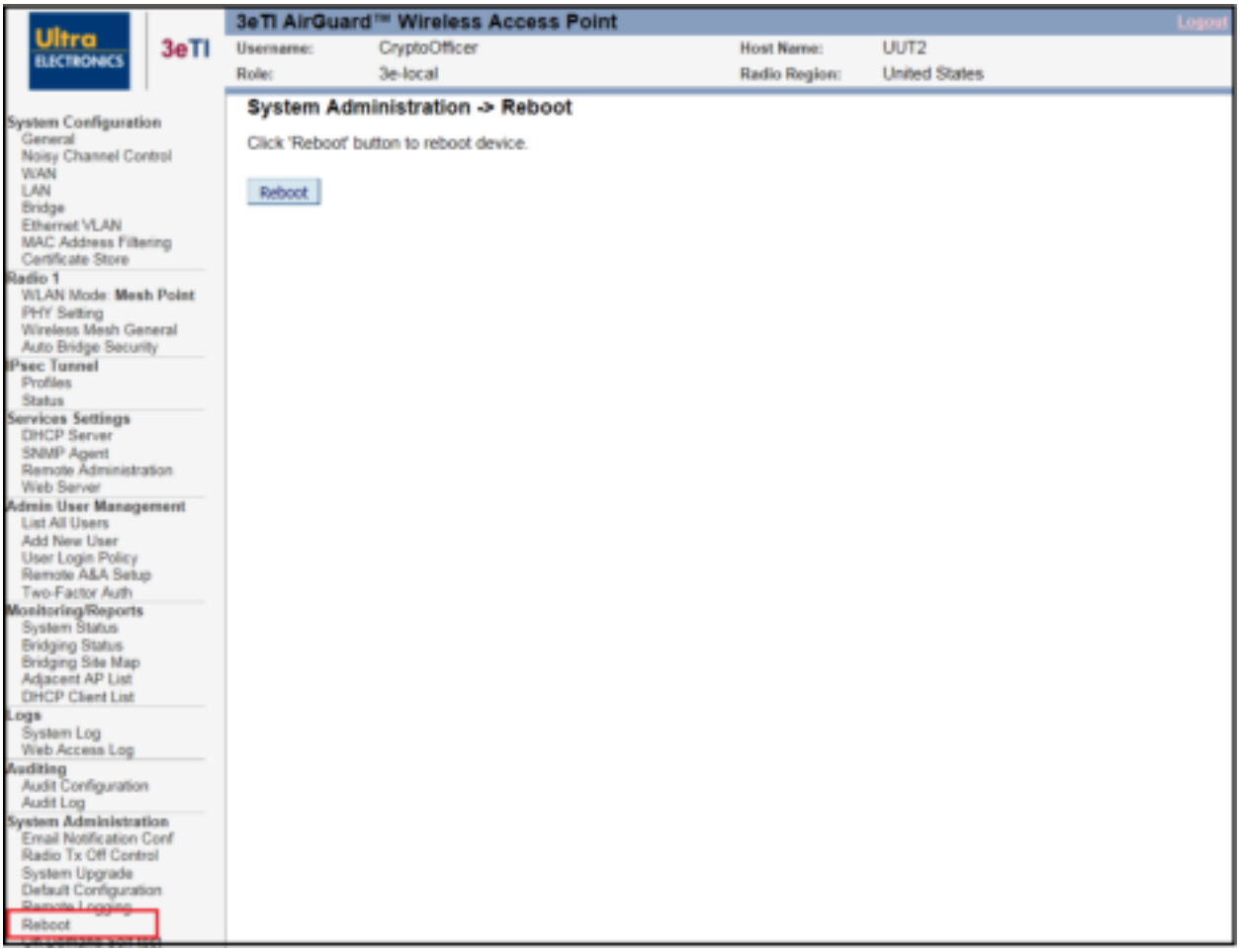


Figure 94: System Administration — Reboot

2.13.7 Self-Test

Self-tests are run to verify the correctness of cryptographic related functions. The 3e-520 series performs the following types of tests:

- Know Answer Tests for all supported encryption algorithms,
- Know Answer Tests for all supported hashing algorithms,
- Know Answer Tests for all supported HMAC algorithms,
- DRBG Tests,
- Sign/Verify Tests,
- Key Derivation Tests,
- Key Distribution Tests,
- Firmware and Bootloader Integrity Tests.

Test results are written to the system log. The platform should not pass secure data while self-tests are executing therefore network interfaces are disabled during self-tests. The platform is halted if any self-test fails. There are many possible factors can lead to a self-test error. For example, faulty hardware components in the noise/entropy generator could lead to DRBG and key generation failures. User can attempt the reboot the device in case of single self-test failure. If the device shows consistent self-test failures as indicated by the LED status, the user shall return the device to 3eTI for service.

These tests are run during power up, on demand or periodically. All of the above tests are executed automatically when the platform is powered up. Links to initiate on-demand or periodic self-tests are available on the platform's web page under "System Administration" if the user is logged in as a Crypto Officer.

2.13.7.1 On Demand Self-test

Selecting the **On Demand Self-test** link (Figure 95) and clicking on **Start Test** executes each self-test except the firmware and bootloader integrity checks. A web page will be displayed indicating if the tests passed.

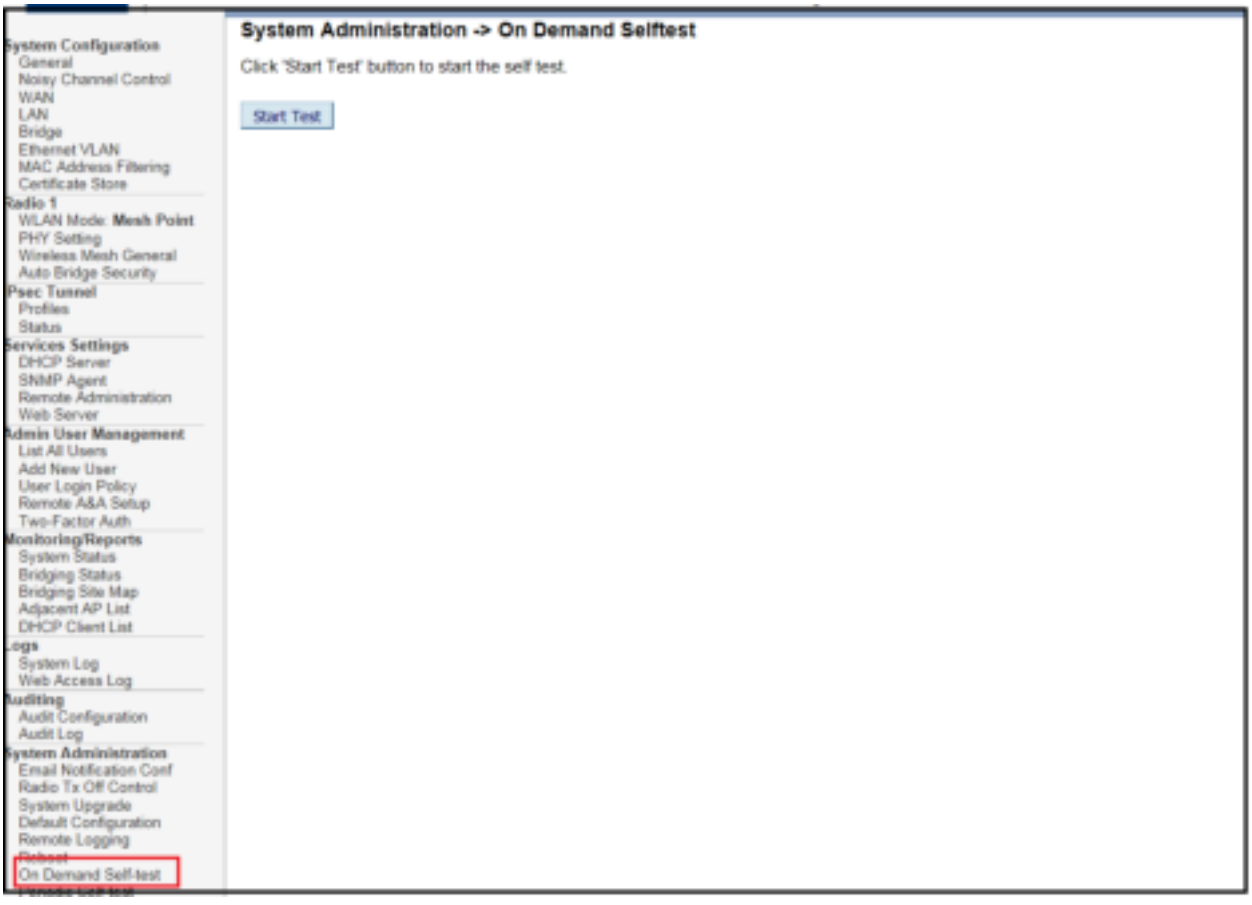


Figure 95: System Administration — On Demand Self-test

2.13.7.2 Periodic Self-test

Selecting the **Periodic Self-test** link (Figure 96) allows the user to enable/disable periodic tests. One test iteration executes each self-test except the firmware and bootloader integrity checks. The **Periodic Test Interval** is the time between test iterations

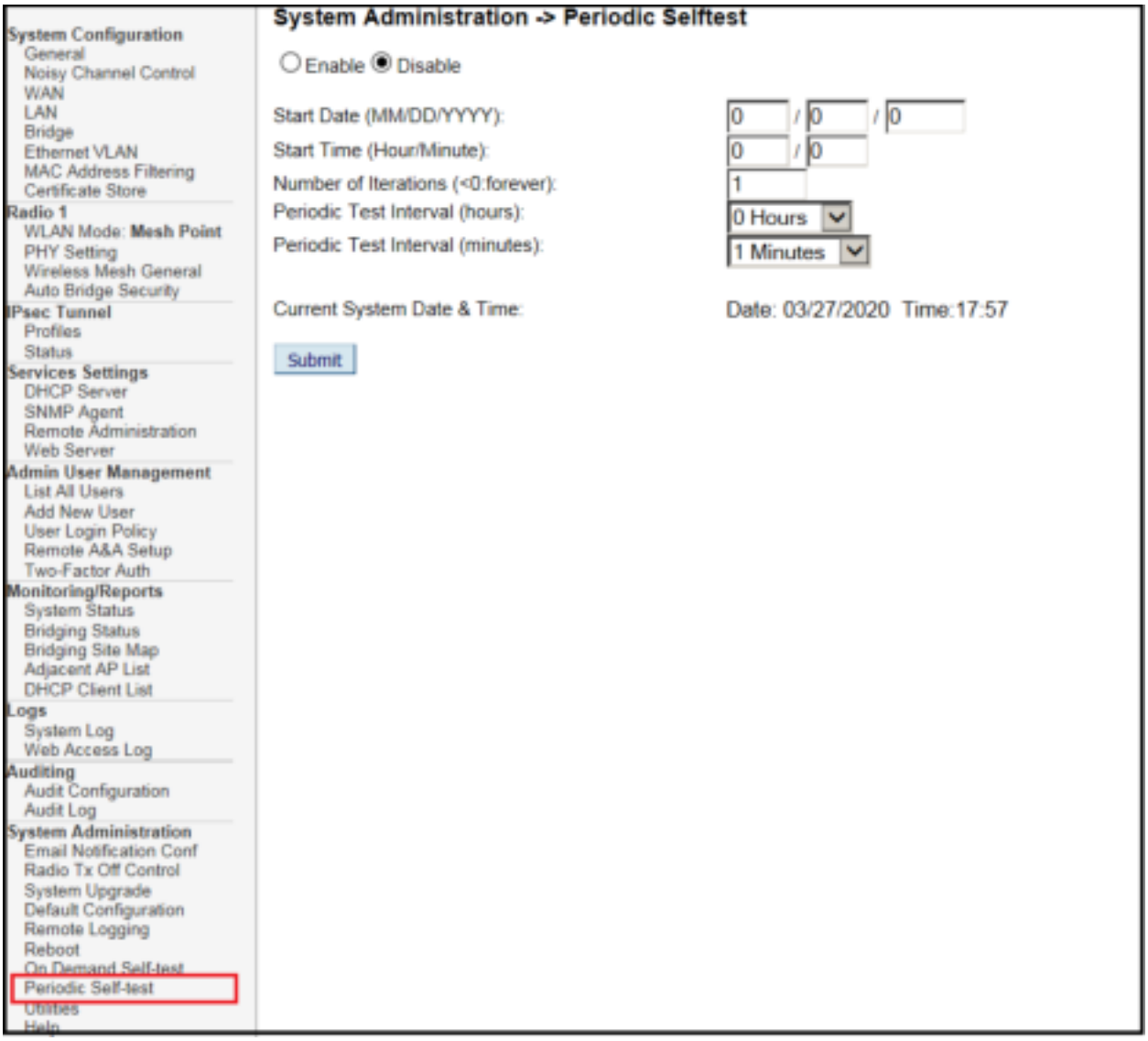


Figure 96: System Administration — Periodic Self-Test

Since network interfaces are disabled during self-tests, a message highlighted in red is displayed on the common banner informing the user that periodic self-tests are enabled.

NOTE: If the Number of Iterations is set to be negative, the self-test will run forever. Test processes will be logged in **Auditing – Log.** When **Periodic Test Interval** is set to a short period, such as 1 minute, log events will fill up the audit log very quickly and generate an email alert as configured.

2.13.8 Utilities

The **System Administration – Utilities** screen (Figure 97) gives you ready access to two useful utilities: Ping and Traceroute. Simply enter the IP Address or hostname you wish to ping or traceroute and click either the **Ping** or **Traceroute** button, as appropriate.

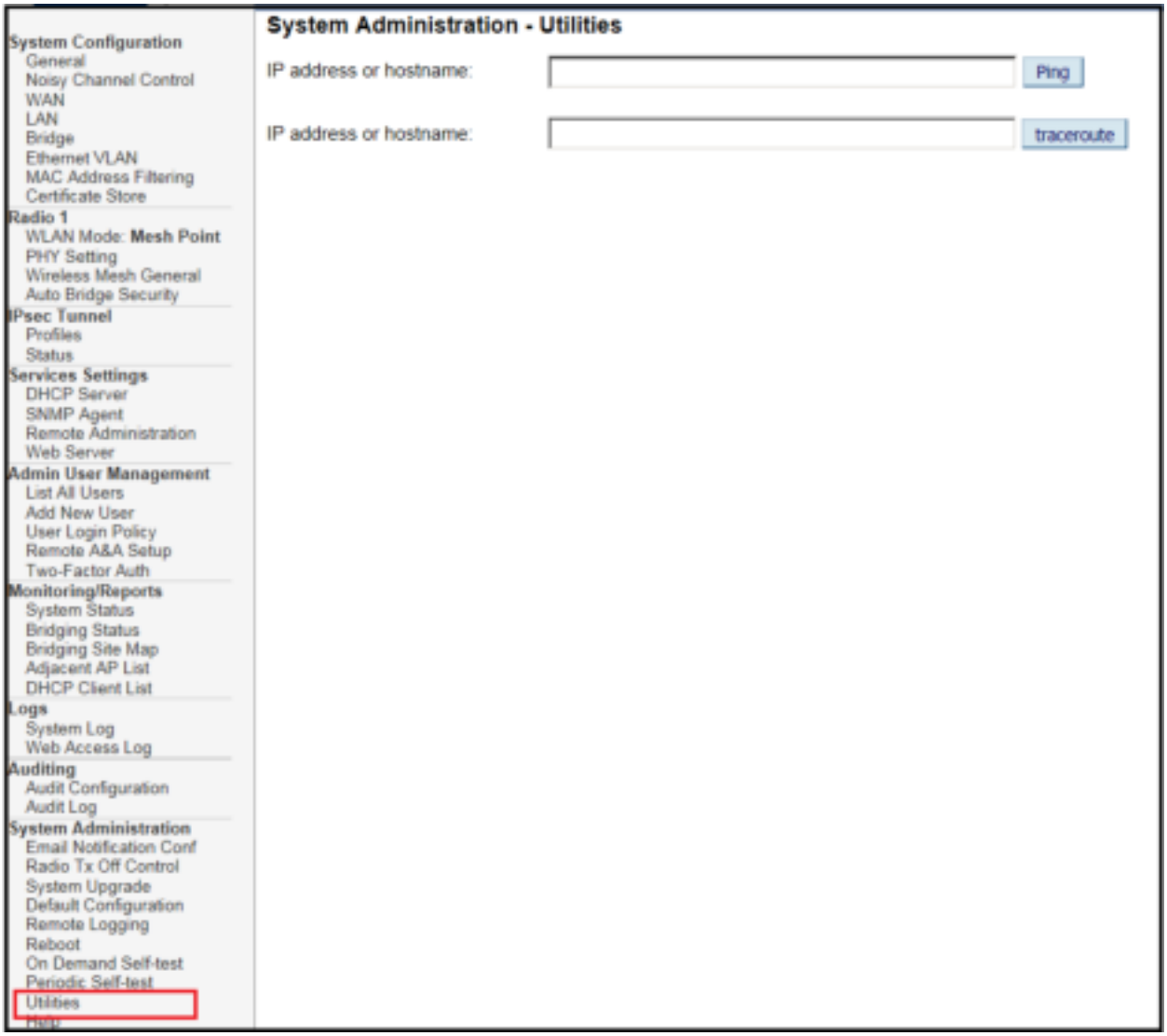


Figure 97: System Administration — Utilities

2.13.9 Help

The **System Administration – Help** screen (Figure 98) displays detailed hardware and software version information when you click on **Help**.

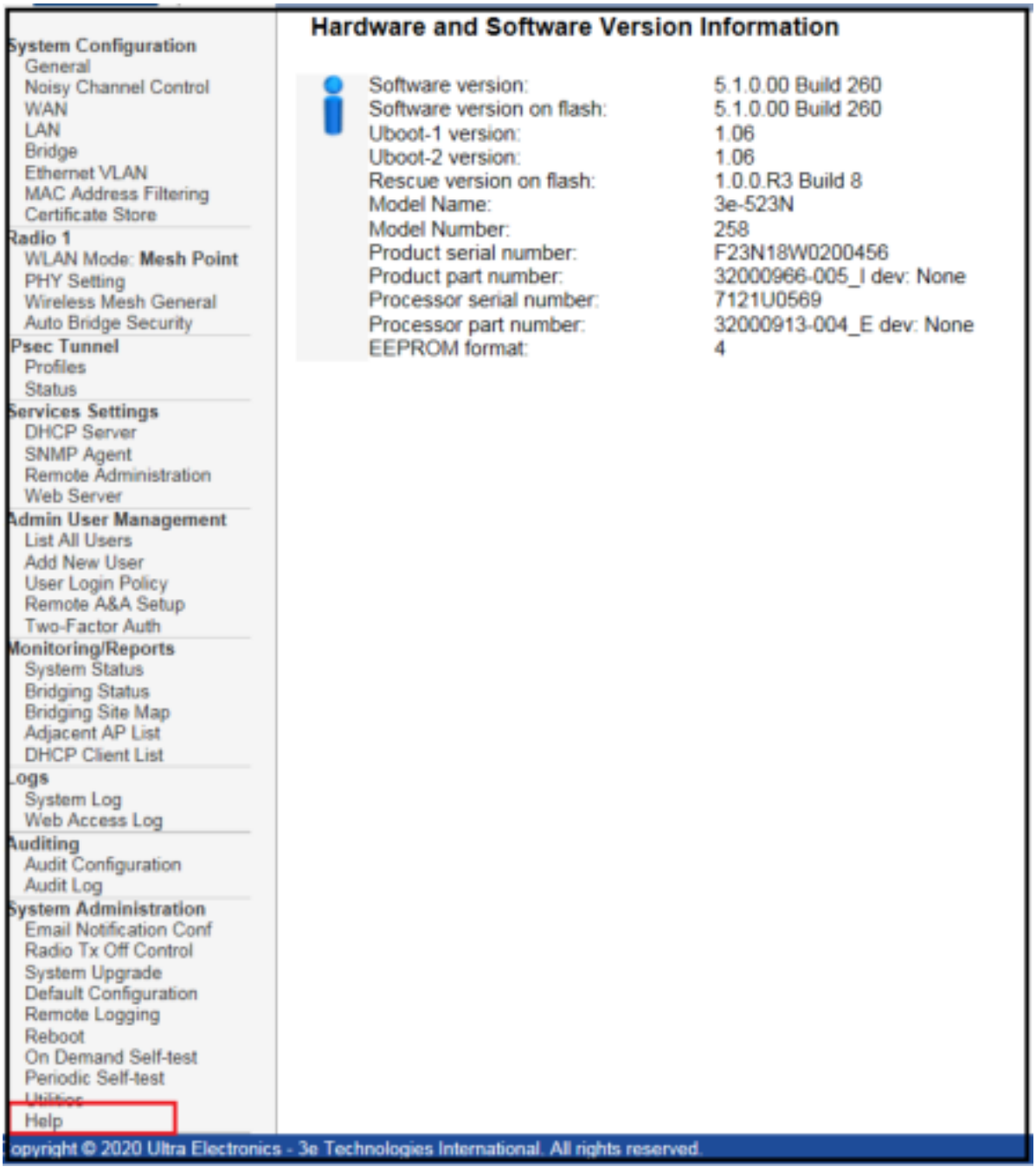


Figure 98: System Administration — Help: Hardware and Software Version Information

3. 3e-523N Hardware Installation

3.1 Preparation for Use

This section describes installation of the 3e–523N unit; see the following sections for 3e-525N series information. The 3e–523N requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation.

NOTE: The 3e–523N is designed for indoor use but can be deployed outdoors within a suitable enclosure. Contact 3eTI for details.

The 3e–523N package includes the following items:

- The 3e–523N unit,
- Power cable adapter,
- Quick Start Guide.

The available 3e–523N accessories are shown in Table 17.

Table 17: 3e-523N Accessories

Model Name	Description	Comments
3e-A523WA1	3e-523N Wiring Accessory	Serial I/O Interface Board with 20 cm cable and DIN Rail mounting hardware
3e-ANT-2303	3e-523N Antenna Set	Three RP-SMA Antennas
3e- A523PP1	3e-523N Power Pigtail	Cable with custom connector for providing existing 5-12 VDC power to 3e-523N
3e-A523DPK	3e-523N DIN-Rail Mounted Power Kit	DIN Rail mounted 120/240 VAC –> 9 VDC power supply and cable w/custom connector for 3e-523N
3e-A523DMNT	3e-523N Desktop Power Kit	Desktop 120/240 VAC –> 12 VDC power supply and cable w/custom connector for 3e-523N
3e-CBL-CAT6-2	2 Meter CAT6 Interconnection Cable	GigaBit capable Ethernet cable - 2 Meter Length
3e-CBL-CAT6-5	5 Meter CAT6 Interconnection Cable	GigaBit capable Ethernet cable - 5 Meter Length

3.1.1 Installation Instructions

It is intended that the user not open the unit. Any maintenance required is limited to the external enclosure surface, cable connections, and to the management software only.

WARNING: To comply with FCC RF exposure compliance requirements, the antennas used with the 3e-523N product family must be installed with a minimum separation distance of 20 cm, 35 cm for any approved directional antenna, from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

3.2 Device Installation

3.2.1 DIN Rail Mounting

The 3e-523N includes a standard locking DIN Rail mount as shown in Figure 99.

Figure 99: 3e-523N DIN Rail Mounting

3.2.2 Rear Mounting

The DIN Rail mount can be remoted to allow the 3e-523N directly mounts to a panel or other flat surface, using metal screws to attach the unit at four mounting holes as shown in Figure 100 and Figure 102. Note that these screws cannot penetrate more than 0.25 inches into the enclosure. This provides easy access to the front panel connectors and grounding screw.

Figure 100: 3e-523N Rear Mounting

3.2.3 Base Mounting

The 3e-523N can be mounted directly to a panel or other flat surface on its side, using metal screws to attach the unit at four mounting holes as shown in Figure 101 and Figure 102. However, this may obscure the label that provides important product information as shown below. Note that these screws cannot penetrate more than 0.25 inches into the enclosure.

Figure 101: 3e-523N Base Mounting

3.2.4 3e-523 Mounting Dimensions

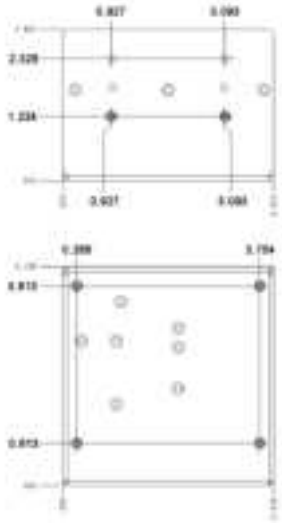


Figure 102: 3e-523N Mounting Dimensions

3.3 Accessory Kit Installation

Table 17: 3e-523N Accessories describes the Ethernet, power, ground, and serial I/O connections associated with these kits. Detailed installation instructions are provided with each accessory kit. Please contact 3eTI Product Support for additional information.

4. 3e-525N Hardware Installation

4.1 Installation Preparation

The 3e-525N product family requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming.

FCC Regulations require that the 3e-525N product family be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution.

3e-525N product operates with PoE which requires the use of a separate power injector that "injects" DC current into the Ethernet cable. These PoE devices should comply with the 802.3at or 802.3af specifications. Standard versions of the 3e-525N product family draw a maximum 14 Watts of power.

The 3e-525N product family package includes the following items:

- The 3e-525N unit,
- 3e-CPLR-1 weatherproof coupler (Qty 1),
- Quick Start Guide.

The available 3e-525N accessories are shown in Table 18.

Table 18: 3e-525N Accessories

Part Number	Description	Comments
3e-ANT-N	Single N-type Antenna	
3e-ANTMNT3N	3e-525N Triple Cable Mount	Mounting Bracket with 3 type-N Adapters without antenna cables
3e-ANT-DOME-1	Indoor (Ceiling-Mount) Dome Antenna	
3e-ANT-DOME-2	Outdoor Dome Antenna	
3e-CPLR-1	Bayonet Coupler	Coupler to waterproof connectors
3e-CONN-A1	AUX Cable Connector	Auxiliary connector for the 3e-525N
3e-POE-GB1	Gigabit POE Injector	
3e-CBL-CAT6-1	1 Meter CAT6 Interconnection Cable	GigaBit-Capable Ethernet Cable - 1 Meter Length – RJ45 Connectors on Both Ends
3e-CBL-CAT6-2	2 Meter CAT6 Interconnection Cable	GigaBit-Capable Ethernet Cable - 2 Meter Length – RJ45 Connectors on Both Ends
3e-CBL-CAT6-3	3 Meter CAT6 Interconnection Cable	GigaBit-Capable Ethernet Cable - 3 Meter Length – RJ45 Connectors on Both Ends
3e-OPK-N	Outdoor Protection Kit	Kit for the 3e-525N Family
3e-PMK-005	Pole Mount Kit	

The 3e–525N product family can be mounted outdoors on a high post to achieve the best bridge result. If mounted outdoors, the outdoor protection kit must be used to prevent lightning damage.

WARNING: To comply with FCC RF exposure compliance requirements, the antennas used with the 3e-525N family products must be installed with a minimum separation distance of 20 cm, 35 cm for any approved directional antenna, from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and / or connectors provided with the device or available from the manufacturer/ distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

4.2 Installation Instructions

The 3e–525N product family is intended to be installed as part of a complete wireless design solution.

This section deals only with the 3e–525N product family and its accessories. The purpose of this section is the description of the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Preliminary setup information provided below is intended for information and instruction of the wireless LAN system administration personnel.

It is intended that the user not open the unit. Any maintenance required is limited to the external enclosure surface, cable connections and to the management software (as described in previous sections) only. A failed unit should be returned to the manufacturer for maintenance.

4.2.1 3e-525N Ethernet Cable Assembly

The 3e-CPLR-1 is a weather-proof coupling accessory for connecting the standard RJ-45 cables to the I/O plate of the 3e-525N family products. Assembly requires no tools and this accessory can be attached to any standard Ethernet (RJ-45) cable assembly.

First, unpack parts from the assembly kit. Feed the Ethernet cable through the nut, sealing ring, and threaded sleeve. Place the two pieces of the locking ring over the RJ-45 connector, making sure these two pieces fully mate (you will hear an audible click). Pull the RJ-45 up to the edge of the threaded sleeve. Ensure the RJ-45 connector is oriented for Code A installation shows below. Tighten the housing and nut onto the threaded sleeve. (Figure 103).

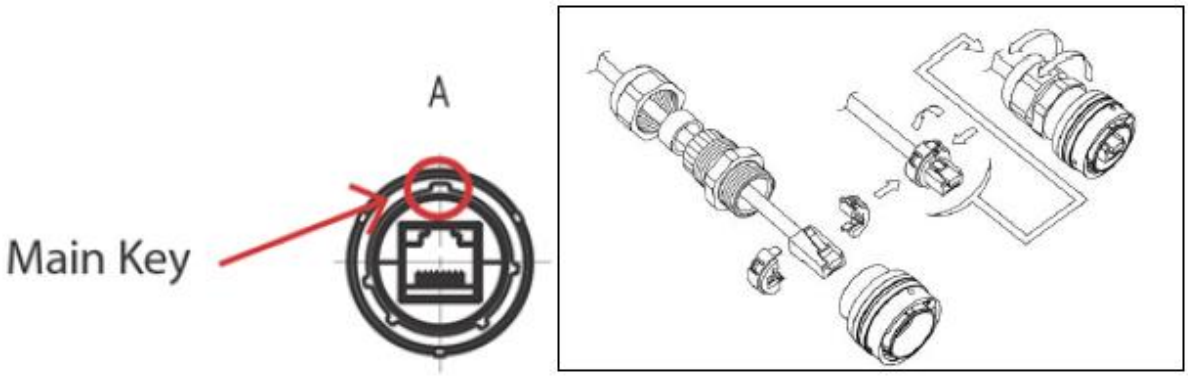


Figure 103: 3e-525N Ethernet Cable Assembly

4.2.2 Pole Mounting

To mount the unit outdoors, you should choose a suitable post to mount the unit high in the air. You can purchase a pole mounting kit from 3eTI. Use the U-ring, screws and nuts to attach the mounting plate to the post. Next attach the unit to the mounting plate with screws.

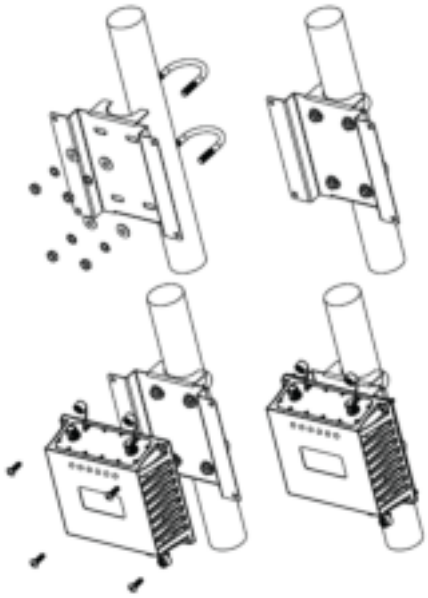


Figure 104: 3e-525N Pole Mount Installation

NOTE: Pole Mount Kit is designed for a Pole of Ø 2.5".

5. 3e-523E-900 Hardware Installation

5.1 Installation Preparation

The 3e-523E-900 radio-communications product requires physical mounting and installation on site, following a prescribed placement design to ensure optimum operation and roaming. By design, the 3e-523E-900 will only transmit and receive the intended direct-sequence spread spectrum modulated 900MHz through the use of automatic keying and code deciphering. Reference FCC ID QVT-523N-900, which is unique to this specific model.

FCC Regulations require that the 3e-523E-900 product be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution. The product uses an industry standard N-type RF output port on the exterior of the product. Installation is rated for commercial and military environments only (non-residential).

5.1.1 Specifications

ELECTRICAL SPECIFICATIONS:

Operating Voltage:	110/220VAC, 50/60Hz
Power Requirements:	15 Watts, max
External Interfaces:	Ethernet, 10/100/1000, standard RJ-45 interface N-type female jack antenna connector
Radio Transmission:	902-928 MHz band

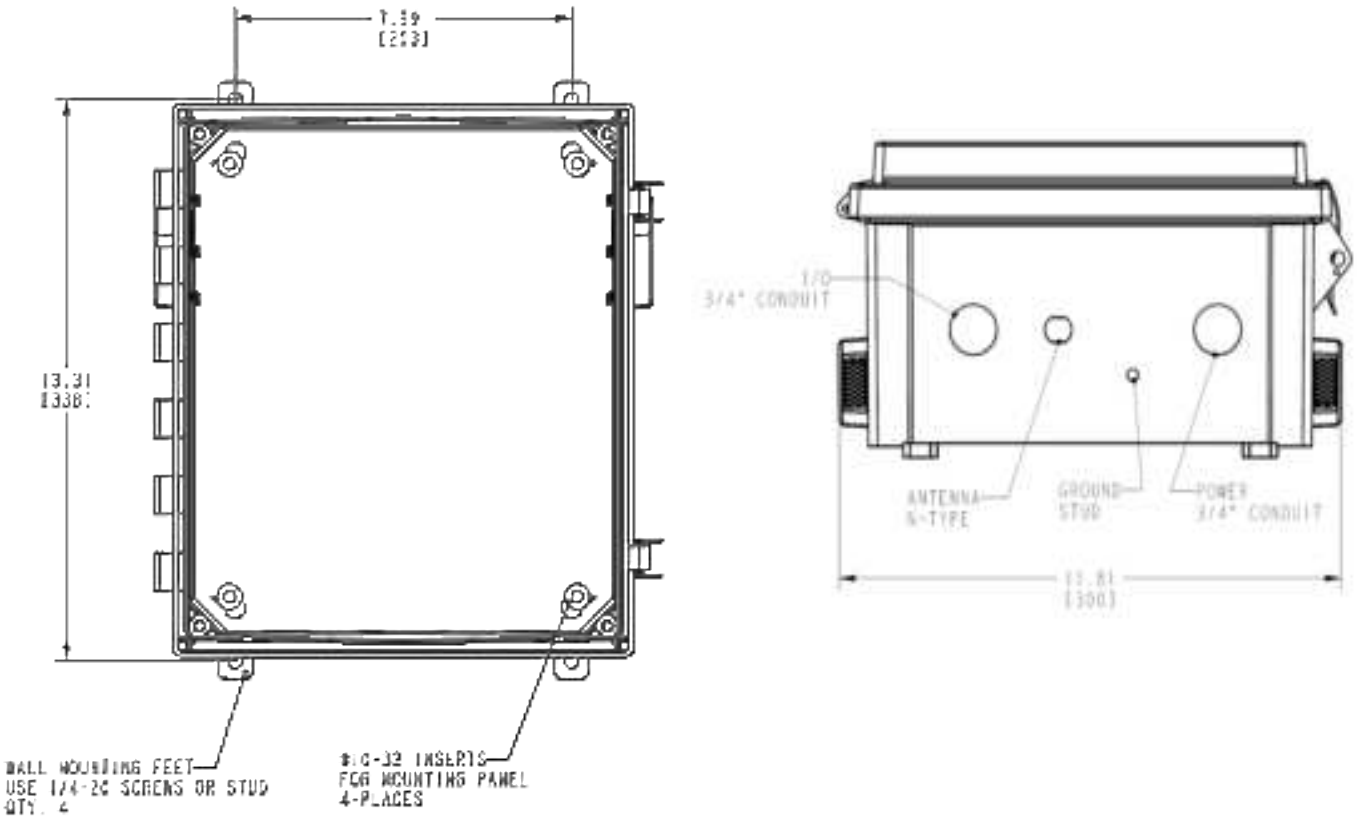
ENVIRONMENTAL SPECIFICATIONS:

Operating Temperature:	-40 to +50°C External Ambient (-40 to +122 °F)
Storage Temperature:	-40 to +70°C (-40 to +158 °F)
Relative Humidity:	90%, non-condensing

MECHANICAL / MOUNTING SPECIFICATIONS:

Enclosure:	Polycarbonate, polyurethane gasket, stainless steel hardware
Weight :	8.8 lbs
Features:	Pad-lockable, outdoor deployment (weatherproof)
Dimensions:	12.08" W x 13.57" H x 6.95" D

5.1.2 Mounting Pattern



5.1.3 Installation Instructions

! WARNING !

Do not attempt to install any outdoor equipment during hazardous conditions such as a thunderstorm, where lightning could strike the equipment or installer. Failure to follow this warning could result in injury or death.

Mounting feet (and screws) are supplied with the unit, attached inside of the cover. Installer must attach these to the enclosure prior to mounting.

Drill holes per mounting pattern drawing and fasten with ¼" screws or bolts (provided by the installer), as appropriate for the installation.

AC power cabling and cable gland (or conduit and hub) are to be provided by the installer as appropriate. Two cutouts provided, one for signal wire, one for power wiring, each at 1.109" diameter. Both holes must have appropriate cable glands or conduit hubs added for weatherproof installation.

Figure 105: 3e-523E-900 Installation

External grounding wire is not provided with the unit. Protection for the user and unit require a safety ground wire attached to the threaded stud at the bottom of the unit to a secure earth bonded surface. The length of this grounding wire should be kept to a minimum, Ultra-3eTI recommends less than 3 feet.

NOTE: The installer is required to ensure that the connection to a proper earth ground is made by properly certified and authorized personnel and must conform to all applicable codes and regulations. The materials required to connect to a proper ground are defined by local conditions and must be procured locally to ensure the correct safety environment is achieved. The cable used to connect to a proper ground must be AWG 10 or heavier. This cable should be kept as short as possible.

5.1.4 RF Connections

RF lightning arrester, and antenna are not provided with the unit.

- The installer should provide a suitable lightning arrestor that can attach directly to the N-female RF port at the bottom of the unit. Ground the lightning arrestor to the same earth bonded ground attachment as used for the unit.
- The installer should provide a suitable antenna, maximum +6dBi gain omni-directional dipole or directional Yagi style, to meet the RF coverage needs per application.
- A 25-foot length of LMR-240 cable is provided with the unit to connect the user-provided antenna to the unit. Ensure this cable is routed and tied down to avoid undue mechanical stress on the lightning arrestor attached to the unit.

5.1.5 RF Safety Information

FCC: To comply with FCC RF exposure compliance requirements, the antennas used with the 3e-523E-900 product must be installed with a minimum separation distance of 20 cm from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and / or connectors provided with the device or available from the manufacturer / distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance to the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Appendix A. Common Criteria

A.1 Overview

Common Criteria for Information Technology Security Evaluation is an international standard for computer security certification. The 520 series claims compliance with CPP_ND_V20 and PP_WLAN_AS_EP_V1.0.

This appendix provides details of how to administer the Device to be compliant with the requirements specified in the protection profiles. In this User Guide, CryptoOfficer is equivalent to the Security Administrator in the Security Target document while Administrator is equivalent to the Non-Security Administrator role in the Security Target. The operational environment has to satisfy the conditions listed in the table below.

Table 19: Operational Environment Objective

Operational Environment Objective from Security Target		User Guidance Reference	Applicable User Role(s)
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	*N/A*	*None*
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	*Add this in the Section 3 Configuration Management section of the user guide. (Add some wording to reflect this in the user guide.*	*None*
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	*Add this in the Section 3 Configuration Management section of the user guide. Add some wording to reflect this in the user guide.*	*None*

A.2 Common Criteria Compliant Steps

User shall follow the steps detailed below from A.3 to A.9 to put the device into Common Criteria Compliant mode of operation.

A.3 Identifying Secure Delivery of the Device

See 3eTI "Delivery Procedure" document.

A.4 Running Compliant Firmware

The following organizational assumption shall be met to operate the device in Common Criteria compliant mode.

Table 20: Device Organizational Assumption

Operational Function	Description
Banners	The device will display a customizable banner prior to the login process.
General Purpose	Only those services that are necessary for the operation, administration and support of the device are required.
Security	The physical security for the device is provided by the environment.
Admin	The security administrators should follow and apply the guidance in a safe manner.
TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

The device must be running firmware version 5.1 in order to be compliant with the CPP_ND_V20 and PP_WLAN_AS_EP_V10. The device comes delivered with the appropriate firmware for compliance. The following procedure describes how to verify the firmware is version 5.1. Please note that the device's cryptographic engine always runs in NIST FIPS mode; there is no configuration necessary.

- Supply power to the device via a DC power supply or via POE (see Section 0 or 1.2.2.2).
- Configure the Ethernet interface on the PC with a static IP address (of 192.168.15.100 and netmask 255.255.255.0).
- Connect the interface on the PC to the Designated Management Interface on the device (see Section 1.2.1 and Section 1.2.2 for details).
- Open a supported browser on the PC and navigate to https://192.168.15.1. Log into the device with user name 'CryptoOfficer'. The default password for the CryptoOfficer user is 'CryptoFIPS'. The device will require you to change the password.
- Verify firmware 5.1 is installed by checking the 'Software version' on the 'Help' screen described in Section 2.13.9.

Software version 5.1.0.0 Build 260 for 3e-523N:

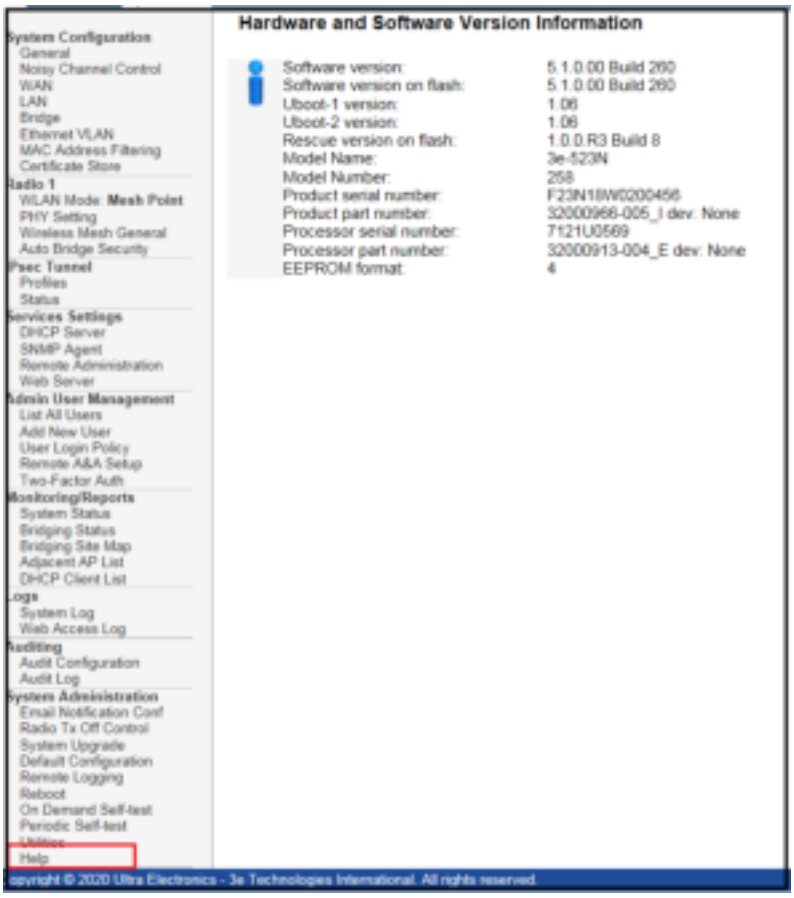


Figure 106: Software Version

The following requirements are satisfied by running the device with firmware image version 5.1.

Table 21: Firmware Requirements

PPWLAN Requirement	Description
FCS_CKM.1 (1) - Cryptographic Key Generation (symmetric Keys for WPA2 Connections.	The firmware provides symmetric key generation using a FIPS approved cryptographic engine
FCS_CKM.1(2) - Cryptographic Key Generation (for asymmetric keys)	The firmware provides asymmetric key generation using a FIPS approved cryptographic engine
FCS_CKM_EXT.4 - Extended: Cryptographic Key Zeroization	The firmware zeroizes all key material when not in use. No further configuration is necessary.
FCS_COP.1 (1) - Cryptographic Operation (for data encryption/decryption)	The firmware uses a FIPS approved cryptographic engine.
FCS_COP.1 (2) - Cryptographic Operation (for cryptographic signature)	
FCS_COP.1 (3) - Cryptographic Operation (for cryptographic hashing)	
FCS_COP.1 (4) - Cryptographic Operation (for keyed-hash message authentication)	
FCS_COP.1 (5) - Cryptographic Operation (WPA2 Data Encryption/Decryption)	

PPWLAN Requirement	Description
FCS_TLS_EXT.1 - Extended: TLS	The firmware provides a WEB interface that supports TLS version 1.1 or 1.2 with ciphers AES-CBC-128 or AES-CBC-256. The cipher suite is auto-negotiated on each web request and requires no further configuration. The following cipher suites are supported by the device: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268, • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268, • TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268, TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268, • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246, • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
FCS_HTTPS_EXT.1 - Extended: HTTPS	The firmware provides a WEB interface that is based on the TCP/IP and HTTPS protocols. The WEB interface does not support unsecure HTTP requests.
FCS_RBG_EXT.1 - Extended: Cryptographic Operation (Random Bit Generation)	The firmware produces random numbers for all cryptographic functions using a FIPS approved generator.
FPT_TUD_EXT.1 - Extended: Trusted Update	The device verifies all uploaded firmware is digitally signed by 3eTI before it is written to flash (see Section 2.13.3.1 Firmware Upgrade for details). The current version of TOE firmware is displayed by viewing the Help screen in Section 2.13.9.
FPT_TST_EXT.1 - Extended: TSF Testing	The device automatically runs a self-test during initial start-up. Results of the test are logged in the Audit Log. No further configuration is necessary.
FPT_FLS.1 - Fail Secure	In the case of a power on test failure, the system will halt and will be left in a secure state with network interfaces disabled. See Section 2.13.7 for self-test details.
FTP_TRP.1 - Trusted Path	The WEB interface is the trusted path between the device and remote administrators. No further configuration is necessary.

A.5 Adding Administrative Users

Users that are allowed to make changes to the device are termed "Authorized Administrators". An Authorized Administrator has either read or read/write privileges over key operational components of the device based on their configured role. Each user is assigned one of two supported roles: 'Crypto Officer' or 'Administrator' (see Section 1.4.1 for a detailed description of the 'Crypto Officer' and 'Administrator' roles).

Add administrative users to the device and set login policies in order to comply with the PPWLAN.

- Log into the WEB GUI over the Designated Management Interface by pointing your browsing to https://192.168.15.1 and logging in as the default user (CryptoOfficer).
- Create user accounts by following the guidance in Section 2.7.2 Add New User. Set each user's "Maximum Bad Password Attempt" and Password Lockout Period" attributes to lock the user out for a period of time after successive bad password attempts. Please note that "Password Lockout Period" will keep the user locked out from device access for that specified time period. The default lockout period is 10 minutes and is configurable from 0-90 minutes. In order to ensure that remote administrator authentication failures do not lead to a situation where no administrator access is available, an administrator account with local access should be configured with a lockout period of "0" minutes. When the 'Password Lockout Period' value is set to 0, the administrator won't be locked

out even after the login threshold is reached. Note that the 'Password Lockout Period' should not otherwise be set to 0.

- Enable the "Password Aging" attribute for each use and set the "Maximum Password Age" to force the user to change his password on a regular basis.
- Set the 'Minimum Password Length' to 15 characters in the User Login Policy page by following the guidance in Section 2.7.3. Set the 'Login Session Timeout' to a value between 3 and 60 minutes.
- Add a login banner as described in Section 2.3.2.

The following requirements are satisfied once administrative users have been added and the login policy has been set.

Table 22: Administration and Login Policy Requirements

PPWLAN Requirement	Description
FIA_AFL.1 - Authentication Failure Handling	See Section 2.7 for details on how to add users and set their "Maximum Bad Password Attempt" and "Password Lockout Period" attributes.
FIA_PMG_EXT.1 - Extended: Password Management	See Section 2.7 for details on how to set passwords and password length requirements. Passwords shall be able to be composed of any combination upper and lower case letters, numbers, and the following special characters: '!', '@', '#', '$', '%', '^', '&', '*', '(', ')'
FIA_UIA_EXT.1 - Extended: User Identification and Authentication	The device responds to ICMP echo requests and displays a login banner before initiating the authentication process. See Section 2.3.2 for details on setting the login banner.
FIA_UAU.7 - Protected Authentication Feedback	The device only provides obscured feedback while the authentication is in progress.
FIA_UAU_EXT.5 - Extended: Password-based Authentication Mechanism	The device provides a local password based authentication mechanism. See Section 2.7 for details on creating administrative users.
FIA_UAU.6 - Re-authenticating	The device requires a user to reenter his or her current password when changing that password. See Section 2.7.1 for detail on changing a user's password.
FMT_MTD.1 - Management of TSF Data (for general TSF data)	The device limits the management of the Security Functions to authorized administrators. The WEB GUI, through which the device is managed, prevents the reading of password-based authentication data, pre-shared keys, symmetric keys or private keys.
FMT_SMF.1 - Specification of Management Functions	The device provides management functionality through the WEB interface.
FMT_SMR.1 - Restrictions on Security Roles	The device maintains user roles and assigns local users to those roles. Access to security functions is limited by the roles. See Section 1.4 for details on security roles.
FTA_SSL.3 - TSF-initiated Termination	WEB interface sessions are terminated when inactive for a configurable amount of time. See Section 2.7.3 for detail on 'Login Session Timeouts'.
FTA_SSL.4 - User-initiated Termination	The device's WEB interface provides a 'Log Out' button on every web page.
FTA_SSL_EXT.1 - Extended: TSF-initiated Session Locking	WEB interface sessions are terminated when inactive for a configurable amount of time. See Section 2.7.3 for detail on 'Login Session Timeouts'.
FTA_TAB.1 - Default TOE Access Banners	A login banner is displayed before establishing a WEB interface session. See Section 2.3.2 for details on setting the login banner.
FMT_MOF.1 - Management of Security Functions Behavior	Management of security functions is limited to authorized administrators through the WEB interface. See Section 1.4 for details on security roles.

A.6 Configuring System Time

The device requires a reliable time source for proper operation. The device is equipped with a real-time clock that is used as the local time source. Additionally, the device can be configured to synchronize its real-time clock with an external NTP time source. The real-time clock must be accurately set and synchronized with an external time source through an IPsec tunnel in order to operate in a Common Criteria environment.

1) Add an IPsec Tunnel Profile to the device by following the guidance in Section 0. Ensure that the Cipher Suite selected is **NOT** "Suite B GMAC 128" or "Suite B GMAC 256". These Cipher Suites do not provide confidentiality and are not compliant with the PPWLAN.
   a) The IPsec tunnel SA re-key timer shall be configured to the range within 24 hours (1440 minutes, refer to Section 0),
   b) The IPsec tunnel child SA re-key timer shall be configured to the range within 8 hours (480 minutes, refer to Section 0).
2) Configure the System Time to synchronize with an external NTP time source by following the guidance in Section 2.3.2. Check the IPsec Tunnel check box and select the IPsec profile configured above.

The following requirements are satisfied once the time has been accurately set.

Table 23: Time Stamp Requirements

NDPP Requirement	Description
FPT_STM.1 - Reliable Time Stamps	The device provides reliable timestamps using a local real time clock optionally synchronized with an external source. See Section 2.3.2 for setting the system time.

A.7 Configuring Access Point Mode

The device supports multiple modes of wireless communication, including Access Point, Mesh Access Point, Mesh Point and Client mode. In order to operate in a Common Criteria environment, the device must be configured in Access Point mode.

- Follow the guidance in Section 2.4.2 and place the device in Wireless Access Point mode.
- Complete the PHY settings in Section 2.4.3.
- Complete the Access Point General Settings in Section 2.4.4. By default the device does not allow management sessions from wireless clients. Update the "Management from Client" attribute on the AP General page if wireless clients need access to the WEB interface.
- Complete the Wireless VLAN Mapping configuration by making sure the "Wireless VLAN" attribute is disabled in Section 2.4.4.4.

In a Common Criteria environment, the Access point must use 802.1x when authenticating wireless clients. Additionally communications with the Authentication Server (RADIUS) must be protected using IPsec Tunnels.

1) Add an IPsec Tunnel Profile to the device by following the guidance in Section 0. Ensure that the Cipher Suite selected is **NOT** "Suite B GMAC 128" or "Suite B GMAC 256". These Cipher Suites do not provide confidentiality.

   a) The IPsec tunnel SA rekey timer shall be configured to the range within 24 hours (1440 minutes, refer to Section 0),

   b) The IPsec tunnel child SA rekey timer shall be configured to the range within 8 hours (480 minutes, refer to Section 0).

2) Complete the Access Point Security Settings in Section 2.4.4.2. Select 802.1x as the authentication method. Check the IPsec Tunnel checkbox and select the IPsec Tunnel profile added in the step above. Configure the 'Radius Server Type' to be IETF and fill in the RADIUS server address and shared secret.

The following PPWLAN requirements are satisfied once the device is configured in Access Point mode as described above.

Table 24: Access Point Security Requirements

NDPP Requirement	Description
FIA_8021X_EXT.1 - Extended: 802.1X Port Access Entity (Authenticator) Authentication.	The device performs the 802.1x authenticator role and does not provide wireless clients access until a successful authentication exchange is completed. Communication between the device and the RADIUS server conforms to RFC 2865 and 3579. See Section 2.4.4.2 for Access Point Security settings.
FCS_IPSEC_EXT.1 - Extended: Internet Protocol Security (IPsec) Communications	The device tunnels RADIUS traffic using IPsec ESP protocol. IKEv2 is used for authentication and key exchange. NAT traversal is supported. See Section 0 for building IPsec Tunnel Profiles.
FIA_PSK_EXT.1 - Extended: Pre-Shared Key Composition	The device can use Pre-Shared keys for IPsec authentication. The keys can be entered as text or a bit string. See Section 0 for building IPsec Tunnel Profiles.
FIA_X509_EXT.1 - Extended: X509 Certificates	The device supports X509v3 certificates used in IPsec and TLS authentication. The device protects certificates from unauthorized deletions and modification through limiting access to authorized entities using the WEB interface. See Section 0 for building IPsec Tunnel Profiles. See Section 2.6.6 for configuring the WEB Server Certificate
FTP_ITC.1 - Inter-TSF trusted channel	All communication between the device and the Authentication Server , NTP server and remote log server is through one or more IPsec tunnels. See Section 0 and Section 2.4.4.2 for configuration details.
FCS_CKM.2 (1) - Cryptographic Key Distribution (PMK)	All RADIUS based key distribution is done through an IPsec tunnel and does not expose the cryptographic keys.
FCS_CKM.2 (2) - Cryptographic Key Distribution (GTK)	All RADIUS based key distribution is done through an IPsec tunnel and does not expose the cryptographic keys.

A.8 Configuring Wireless Client Session Establishment

The device can deny establishment of wireless clients based on MAC address, time, day and per radio interface.

- Follow the guidance in Section 1.3.3 "MAC Address Filtering" to limit wireless client access.

The following PPWLAN requirements are satisfied.

Table 25: Access Point Session Establishment

NDPP Requirement	Description
FTA_TSE.1 - TOE Session Establishment	The device is able to deny establishment of a wireless client session based on MAC address, time or day.

The "MAC Address Filtering" is per wireless interface based, so that a wireless client can be added to the "deny list" on one interface while be on the "allowed list" on the other interface. To make this happen, first follow Section 2.4 to configure each radio into "Access Point" mode, then follow Section 1.3.4 to configure the "MAC Address Filtering" for each radio

A.9 Configuring Audit Event Loggin

The device generates audit log records for the following security related events:

- All use of the identification and authentication mechanism.
- Any attempt at unlocking an interactive session.
- The termination of a remote session by the session-locking mechanism.
- The termination of an interactive session.
- Changes in system time.
- Initiation or Failure of a firmware update.
- Initiation, Termination or Failure of a trusted channel.

Each audit log record is stored locally on the device and can be viewed by an authorized administrator with a 3e-local role (see Section 2.12.2 for viewing audit log records). In addition to storing records locally, the device must be configured to transmit audit log records to a remote auditing server over a trusted channel using an IPsec tunnel. Since the volume of audit log records can become excessive, an authorized administrator with a 'Crypto Officer' role can choose not to log categories of audit events—IPsec Security Policy success audit records, for example, can be muted and not logged.

Audit log records are stored locally on the device in 256K of persistent memory. Once this memory is full, new audit record will rotate out the oldest records and the old records will be lost.

In order to operate in a Common Criteria environment the following audit records must be enabled:

- 'Self-Test' Success and Failure audit records.
- 'Management Connection' Success and Failure audit records.
- 'Admin User Authentication' Success and Failure audit records.
- 'System Configuration' Success and Failure audit records.
- 'Software Update' Success and Failure audit records.

See Section 2.12.1 in order to verify the above audit records are enabled. Additionally, the device must be configured to transmit audit records to a remote auditing server through an IPsec tunnel.

1) Add an IPsec Tunnel Profile to the device by following the guidance in Section 0. Ensure that the Cipher Suite selected is **NOT** "Suite B GMAC 128" or "Suite B GMAC 256". These Cipher Suites do not provide confidentiality and are not compliant with the.

   a) The IPsec tunnel SA rekey timer shall be configured to the range within 24 hours (1440 minutes, refer to Section 0),

   b) The IPsec tunnel child SA rekey timer shall be configured to the range within 8 hours (480 minutes, refer to Section 0).

2) Enable the Remote Auditing and provide the 'Audit Server Address' and 'Audit Server Port' described in Section 2.12.1. Be sure to check the IPsec Tunnel check box and select the IPsec Tunnel profile add in the above step.

The following PPWLAN requirements are satisfied once the audit logging is configured.

Table 26: Audit Log Requirements

PPWLAN Requirement	Description
FAU_GEN.1 - Audit Data Generation	The device audit logs startup and shutdown of the audit function.
FAU_GEN.2 - User Identity Association	The user ID is included in all audit log records resulting from the action of administrative users.
FAU_SEL.1 - Selective Audit	See Section 2.12.1 for details on selecting auditable events.
FAU_STG.1 - Protected Audit Trail Storage (Local Storage)	The device stores the last 256KB of audit records and prevents their removal. No further configuration is necessary.
FAU_STG_EXT.1 - Extended: External Audit Trail Storage	See Section 2.12.1 for details on configuring a remote audit log server.
FAU_STG_EXT.3 - Action in Case of Loss of Audit Server Connectivity	The device stops passing packets and logs a communication error when Audit Server connectivity is lost. No further configuration is necessary.
FAU_STG_EXT.4 - Prevention of Audit Data Loss	See Section 2.12.1 for configuring the audit service to either stop logging or rotate the logs when the local audit trail is full.
FAU_SAR.1 - Audit Review	See Section 2.12.2 for details on reviewing audit records.
FAU_SAR.2 - Restricted Audit Review	Read access to audit records is limited to authorized administrators with the 'CryptoOfficer' role. See Section 1.4.1 for details on Management User Roles.

A.10 Understanding Audit Events

A.10.1 Audit Event Record Structure

The following is a sample Audit Event message:

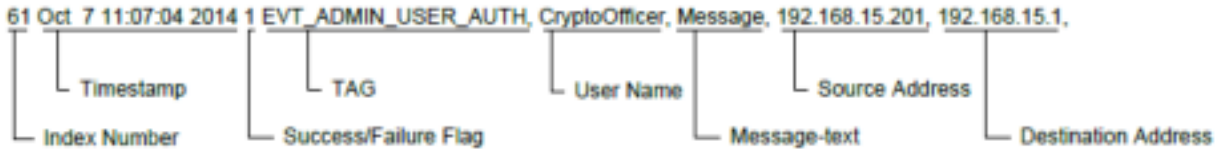


Table 27 describes the fields in an Audit Event message. If the Audit Event logging utility cannot determine the value for a particular field, a space character appears followed by the comma delimiter.

Table 27: Fields in Audit Event Message

Field	Description
Index Number	The Audit Event logging utility prepends each message with an index number that is incremented with every message. The index is set to '1' whenever the system is rebooted. The index wraps back around to '1' after its maximum value of '99999'.
Timestamp	Time when the message was generated in the form 'MMM DD HH:mm:SS YYYY' MMM - Abbreviated month name DD - Day of month as 1 or 2 characters HH - Hour (0-23) mm - Minute (0-59) SS - Second (0-60) YYYY - Year Time is in local time.
Success/Failure Flag	Flag indicating if the audit record was generated from a successful event or an event that failed. 1 - The event was successful 2 - The event failed
TAG	3eTI-enumerated message tag which uniquely identifies the message type.
User Name	Authorized administrator that initiated the event.
Message-text	Description of the event.
Source Address	Source IP or MAC address of the network packet that initiated the event.
Destination Address	Destination IP or MAC address of the network packet that initiated the event.

A.10.2 Audit Event: Audit Startup and Shutdown

The Audit Event logging utility is started automatically during the system bootup. The utility cannot be stopped other than by rebooting the system. When the device is restarted, the audit log contains the following information:

- 69 Sep 11 14:11:44 2017 1 EVT_AUDIT_START_STOP, , Audit Log is shutting down, , ,
- 1 Sep 11 14:13:12 2017 1 EVT_AUDIT_START_STOP, , Audit Log is enabled on startup, , ,

A.10.3 Audit Event: Audit Coverage Change

Audit log messages are generated when the audit configuration is changed. The following messages are generated as a result of successful audit configuration change through the WEB GUI:

- 307 Sep 11 15:01:05 2017 1 EVT_AUDIT_CONFIG_CHANGE, CryptoOfficer, Audit configuration has been updated, , ,
- 309 Sep 11 15:01:05 2017 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Updated audit configuration, , ,

The following messages are generated as a result of failed audit configuration change through the WEB GUI:

- 318 Sep 11 15:03:48 2017 2 EVT_AUDIT_CONFIG_CHANGE, CryptoOfficer, Invalid audit server address, , ,

- 319 Sep 11 15:03:48 2017 2 EVT_SYSTEM_CONFIG, CryptoOfficer, Failed to update audit configuration, , ,

A.10.4 Audit Event: Loss of Connectivity to Server

Audit log messages are generated when the link to the external audit server is not available. The following messages are generated as a result of losing connectivity to the audit server 192.168.205.9:

- 454 Sep 11 15:30:45 2017 2 EVT_MANAGEMENT_CONNECTION, , Connection Error: Audit data waiting to be sent out, , 192.168.205.9:11515,
- 612 Sep 11 15:41:11 2017 2 EVT_MANAGEMENT_CONNECTION, , Failed to initiate a TCP connection, , 192.168.205.9:11515,

A.10.5 Audit Event: Administrative Actions Event

The following are some examples of audit log messages recording administrative actions:

1) **User Login and Logout:**
   a) 344 Sep 11 15:16:35 2017 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.15.100 logged in successfully, , ,
   b) 352 Sep 11 15:17:34 2017 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.15.100 logged out, , ,
2) **Configure User:**
   a) 364 Sep 11 11:37:44 2017 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, Added admin-user TestUser1 role=Administrator, , ,
3) **Modify User Password:**
   a) 372 Sep 11 11:41:46 2017 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, Changed admin-user password for TestUser1 in Administrator role, , ,
4) **Configure AP 802.1x Security Method:**
   a) 432 Sep 11 12:03:33 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i sub-algorithm is changed from PSK Passphrase to 802.1x, , ,
   b) 436 Sep 11 12:03:33 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i Primary Radius Server IP changed: old=, new=192.168.205.9, , ,
   c) 437 Sep 11 12:03:33 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i Radius Shared Secret changed, , ,
   d) 438 Sep 11 12:03:33 2017 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Updated AP security configuration, , ,
5) **Configure AP PSK with Master Key:**
   a) 647 Sep 11 15:44:17 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i sub-algorithm is changed from 802.1x to PSK Master Key, , ,
   b) 648 Sep 11 15:44:17 2017 1 EVT_KEY_GENERATION, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

c) 649 Sep 11 15:44:17 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

d) 651 Sep 11 15:44:17 2017 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Updated AP security configuration, , ,

6) Configure AP PSK with Passphrase:

a) 654 Sep 11 15:45:15 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i sub-algorithm is changed from PSK Master Key to PSK Passphrase, , ,

b) 655 Sep 11 15:45:15 2017 1 EVT_KEY_GENERATION, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

c) 656 Sep 11 15:45:15 2017 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

d) 657 Sep 11 15:45:15 2017 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Updated AP security configuration, , ,

7) Login banner change:

a) 7 Apr 12 18:48:18 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Terms & Condition changed: old={This is first banner message second line} new={This is second banner message second line third line}, ,

8) Configure session inactivity and timeout:

a) 10 May 13 09:52:05 2018 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, Login session timed out., , ,

9) Configure IPsec functions:

a) Add IPsec profile:

i) 14 May 13 09:53:23 2018 1 EVT_KEY_ZEROIZATION, , Zeroized IPsec Profile PSK, , ,

ii) 15 May 13 09:53:23 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, IPsec Profile first_profile added, , ,

iii) 16 May 13 09:53:23 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Add VPN profile has been successful, , ,

10) Update IPsec profile:

a) 18 May 13 09:54:36 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, IPsec Profile first_profile Updated, , ,

b) 19 May 13 09:54:36 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Update VPN profile has been successful, , ,

11) Use IPsec profile [NTP]:

a) 13 Apr 12 19:02:11 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, NTP server 1 IP changed, old= new=192.168.2.1, , ,

b) 14 Apr 12 19:02:11 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, NTP server 1 IPsec profile changed, old=, new=second_profile, , ,

12) Generating/import of, changing, or deleting of cryptographic keys WiFi PSK change:

a) 31 Apr 12 19:05:34 2018 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i sub-algorithm is changed from PSK Master Key to PSK Passphrase, , ,

b) 32 Apr 12 19:05:34 2018 1 EVT_KEY_GENERATION, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

c) 33 Apr 12 19:05:34 2018 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i PSK Master Key changed., , ,

d) 34 Apr 12 19:05:34 2018 1 EVT_ENCRYPT_ALG_CHANGED, CryptoOfficer, AP1 FIPS-802.11i Group Key Life Time changed from 600 to 900 (minutes), , ,

13) IPsec PSK change:

a) 40 Apr 12 19:07:29 2018 1 EVT_KEY_ZEROIZATION, CryptoOfficer, Zeroized IPsec Profile PSK, , ,

b) 41 Apr 12 19:07:29 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, IPsec Profile second_profile Updated, , ,

14) Import device certificate and private key:

a) 8 Apr 12 19:00:27 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Device Certificate [US Maryland Ultra-3eti Testing device1 device1@3eti.com] uploaded successfully., , ,

15) Delete device certificate and private key:

a) 73 Apr 12 19:13:26 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Deleted /csp/certs/device/cert/1.cert [US Maryland Ultra-3eti Testing device1 device1@3eti.com], , ,

A.10.6 Audit Event: Failure of Key Generation/Distribution

Audit log messages are generated when any failure of key generation/distribution occurs. The following message is generated as a result of GMK rekey failure:

- 6593 May 11 10:38:29 2015 2 EVT_KEY_GENERATION, , failed to get random data for GMK rekeying, , 00:0e:8e:4b:ba:3d,

The following is an example of an audit log message resulting from an ephemeral key generation failure occurring on the VPN connection to the audit server 192.168.205.9:

- 6023 May 11 13:10:36 2015 2 EVT_KEY_GENERATION, , audit1 VPN [192.168.205.9]: Ephemeral key generation failed, , ,

A.10.7 Audit Event: Failure of Encryption or Decryption

Audit log messages are generated when encryption or decryption of user data fails. The following is an example of an audit log message resulting from data decryption failure:

- 3544 May 10 13:11:30 2015 2 EVT_ENCRYPT_DECRYPT_ERR, , audit1 VPN [192.168.205.9]: Encryption / Decryption failed, , ,

A.10.8 Audit Event: Failure of Cryptographic Signature

Audit log messages are generated when cryptographic signing fails. The following is an example of an audit log message resulting from cryptographic signature failure:

- 3614 May 10 13:11:52 2015 2 EVT_CRYPTO_SIGNATURE_ERR, , audit1 VPN [192.168.205.9]: Cryptographic signature failed, , ,

A.10.9 Audit Event: Failure of Hashing Function

Audit log messages are generated when cryptographic hashing fails. The following is an example of an audit log message resulting from a hashing failure:

- 3621 May 10 13:12:02 2015 2 EVT_CRYPTO_HASHING_ERR, , audit1 VPN [192.168.205.9]: Cryptographic hashing function failed, , ,

A.10.10 Audit Event: Failure of WPA2 Encryption or Decryption

Audit log messages are generated when WPA2 encryption or decryption fails. The following is an example of an audit log message resulting from WPA2 decryption failure:

- 3744 May 10 13:18:30 2015 2 EVT_ENCRYPT_DECRYPT_ERR, , mac80211 CCMP Replay packet, 02:15:6d:84:f4:c4, 00:0e:8e:4b:ba:3d,

A.10.11 Audit Event: Failure to Establish a HTTPS/TLS Session

Audit log messages are generated when there is a failure in the TLS handshake—for example, the following message is generated when there is a TLS handshake failure:

- 70 Mar 18 11:58:41 2015 2 EVT_MANAGEMENT_CONNECTION, , TLS handshake failure - no matching cipher, 192.168.15.201, ,

Other failure reasons could include mismatching TLS versions, TLS authentication failure (if the TLS client refuse to trust the TOE's server certificate).

A.10.12 Audit Event: Establishment or Termination of a HTTPS/TLS Session

Audit log messages are generated each time a TLS session is established or terminated. The following message is generated when there is a new TLS session:

- 83 Mar 18 11:58:42 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS handshake success, 192.168.15.201, ,

The following message is generated when a TLS session is terminated:

- 86 Mar 18 11:58:44 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS session terminated, 192.168.15.201, ,

A.10.13 Audit Event: Failure of IPsec Security Association Establishment

Audit log messages are generated each time an IPsec Security Association fails to be established. The following is an example of an audit log message resulting from an IPsec Security Association failure:

- 3244 May 10 13:12:53 2015 2 EVT_IPSEC_SA, , audit1 VPN [192.168.205.9]: Traffic selector mismatch, , ,

The device verifies that the algorithm used in the ESP SA (IKEv2 CHILD_SA) is less than or equal to the algorithm of the parent IKE_SA. If during the negotiation there is no algorithm that fits this requirement, the device will send a NO_PROPOSAL_CHOSEN message and the CHILD_SA will not be established, with the following audit events generated:

- 150 Sep 12 11:14:39 2017 2 EVT_IPSEC_SA, , ntp11 VPN [192.168.205.9]: IPsec cryptographic algorithm mismatch, , ,

- 151 Sep 12 11:14:39 2017 2 EVT_IPSEC_SA, , ntp11 VPN [192.168.205.9]: SA removed due to NO_PROPOSAL_CHOSEN notification from peer, , ,

A.10.14 Audit Event: Establishment or Termination of an IPsec Security Association

Audit log messages are generated each time an IPsec Security Association is established or terminated. The following message is generated when there is a new IPsec Security Association:

- 217 Mar 26 14:30:25 2015 1 EVT_IPSEC_SA, , SAD-add src=192.168.254.254 dst=192.168.205.9 spi=3405309099(0xcaf8e4ab) res=1, ,

- 218 Mar 26 14:30:25 2015 1 EVT_IPSEC_SA, , SAD-add src=192.168.254.254 dst=192.168.205.9 spi=3470987138(0xcee30f82) res=1, ,,

The following message is generated when an IPsec Security Association is terminated:

- 222 Mar 26 14:36:30 2015 1 EVT_IPSEC_SA, , SAD-delete src=192.168.254.254 dst=192.168.205.9 spi=3405309099(0xcaf8e4ab) res=1, ,

- 223 Mar 26 14:36:30 2015 1 EVT_IPSEC_SA, , SAD-delete src=192.168.254.254 dst=192.168.205.9 spi=3470987138(0xcee30f82) res=1, ,

A.10.15 Audit Event: Failure of Random Bit Generation

Audit log messages are generated when random bit generation fails. The following is an example of an audit log message resulting from random bit generation failure:

- 3534 May 10 13:15:01 2015 2 EVT_RBG_ERR, , audit1 VPN [192.168.205.9]: Random number generator failed, , ,

A.10.16 Audit Event: Authentication Failure Handling

Audit log messages are generated when the defined number of unsuccessful authentication attempts has been met. The following message is generated when the threshold of 3 login attempts with invalid password has reached:

- 145 May 12 15:00:38 2015 2 EVT_ADMIN_USER_AUTH, TestUser, User TestUser account locked (threshold of 3 login attempts with invalid password reached), , ,

A.10.17 Audit Event: Admin User Authentication

Audit log events are generated whenever an administrative user successfully or unsuccessfully attempts WEB interface access. Additionally, logout events are recorded when an administrative user successfully ends a WEB interface session by clicking the log-off button—for example, the following logs show a failed authentication attempt followed by a successful login and a logout:

- 39 Mar 18 11:49:59 2015 2 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.205.208 could not be authenticated, , ,
- 41 Mar 18 11:50:07 2015 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.205.208 logged in successfully, , ,
- 45 Mar 18 11:55:56 2015 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.205.208 logged out, , ,

A.10.18 Audit Event: 802.1X Authentication

Audit log messages are generated when 802.1X authentication request is accepted or rejected for a wireless client. The following messages show a successful authentication attempt (Access Accept) and a failed authentication attempt (Access Reject) for the wireless client 8c:70:5a:40:f0:a0:

- 8104 May 12 14:42:05 2015 1 EVT_STA_AUTH, , Access Accept from auth server, , 8c:70:5a:40:f0:a0,
- 8104 May 12 14:42:05 2015 2 EVT_STA_AUTH, , Access Reject from auth server, , 8c:70:5a:40:f0:a0,

The following message is an example of audit log message showing the device received a data frame from the not associated client 8c:70:5a:40:f0:a0:

- 8168 May 12 13:01:05 2015 2 EVT_KEY_TRANSFER_ERR, , IEEE 802.1x data frame from not associated STA, , 8c:70:5a:40:f0:a0,

A.10.19 Audit Event: Certificate Validation and Upload

Audit log messages are generated when the certificates fail to be validated—for example, the following messages are generated as a result of attempting to upload an invalid certificate through the WEB GUI:

- 7617 May 11 16:12:03 2015 2 EVT_CERT_VALIDATION_ERR, CryptoOfficer, Issuer certificate(s) upload failed: invalid or unsupported file format., , ,
- 7618 May 11 16:12:03 2015 2 EVT_SYSTEM_CONFIG, CryptoOfficer, Failed to upload Issuer certificate, , ,

The following message is generated a result of uploading an issuer certificate through the WEB GUI:

- 8239 May 12 15:36:55 2015 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Uploaded Issuer certificate, , ,

A.10.20 Audit Event: Failure of the TSF

Audit log messages are generated when any failure of the TSF is detected—for example, the following messages are generated as a result of RNG self-test failures:

- 7 May 11 10:01:07 2015 2 EVT_SELF_TEST, , Random Number Generator (openssl) self-test failed, , ,
- 30 May 11 10:01:08 2015 2 EVT_SELF_TEST, , The self-test failed, , ,

A.10.21 Audit Event: Changes to the System Time

Audit log messages are generated when the date or time on the device is changed—for example, the following messages are generated as a result of changing the date manually through the WEB GUI:

- 3544 Mar 18 13:00:36 2015 1 EVT_SYSTEM_CONFIG, CryptoOfficer, Updated general system configuration, , ,
- 3557 Mar 18 02:00:35 2015 1 EVT_TIME_CHANGE, , System time has been changed - old_timestamp: 1426701636 new_timestamp: 1426662035, 192.168.205.208, ,

Please note the numbers in the logs above are UNIX epoch. There are many stand-alone or online tools to convert epoch to human readable time stamps.

A.10.22 Audit Event: Self-Test

During device's power up process, the firmware runs algorithm known answer tests, the audit messages shown below indicate the test results. In case of any test failure, the system will halt and the module will not be operable. The status output LED GPIO pins will be set high to indicate the system halt condition. User can reboot the device in attempts to eliminate the self-failure, if continuous failure shows up, the device should be returned to Ultra-3eTI for repairs.

Audit log messages are generated when the device's Security Functions self-test is completed. The self-test is run automatically on system boot up. The following messages are generated as each self-test function completes:

- 2 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , The system wide self-test has been triggered, , ,
- 3 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard ECB mode (openssl) self-test passed, , ,
- 4 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard CBC mode (openssl) self-test passed, , ,
- 5 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Secure Hash Algorithm 1 (openssl) self-test passed, , ,
- 6 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Secure Hash Algorithm 2 (openssl) self-test passed, , ,
- 7 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Random Number Generator (openssl) self-test passed, , ,

- 8 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Hashed Message Authentication Code (openssl) self-test passed, , ,
- 9 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , RSA Algorithm (openssl) self-test passed, , ,
- 10 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Triple DES (openssl) self-test passed, , ,
- 11 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , TLS-KDF Key Distribution Function (openssl) self-test passed, , ,
- 12 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , KAS (Key Agreement Scheme) (openssl) self-test passed, , ,
- 13 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard ECB mode (hardware kernel) self-test passed, , ,
- 14 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard CCM mode (hardware kernel) self-test passed, , ,
- 15 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard CBC mode (hardware kernel) self-test passed, , ,
- 16 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Advanced Encryption Standard CMAC mode (hardware kernel) self-test passed, , ,
- 17 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Secure Hash Algorithm 1 (hardware kernel) self-test passed, , ,
- 18 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Secure Hash Algorithm 2 (hardware kernel) self-test passed, , ,
- 19 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Hashed Message Authentication Code (hardware kernel) self-test passed, , ,
- 20 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Triple DES ECB (hardware kernel) self-test passed, , ,
- 21 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Triple DES CBC (hardware kernel) self-test passed, , ,
- 22 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , ECDSA Verification self-test passed, , ,
- 23 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Firmware Integrity Check self-test passed, , ,
- 24 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Bootloader Integrity Check self-test passed, , ,
- 25 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , Key Error Detection self-test passed, , ,
- 26 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , The self-test passed, , ,
- 27 Sep 11 14:13:13 2017 1 EVT_SELF_TEST, , power up test run, , ,

A.10.23 Audit Event: Successful or Failed System Updates

An audit log message is generated on initiation of system software updates—for example, the following messages are generated as a result of success firmware update:

- 77 Sep 12 15:10:49 2017 1 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update initiated, 192.168.15.100, ,
- 78 Sep 12 15:11:08 2017 1 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update has been successful, 192.168.15.100, ,

The following messages are generated as a result of failed firmware update due to ECDSA signature mismatch:

- 59 Sep 12 15:16:33 2017 1 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update initiated, 192.168.15.100, ,
- 61 Sep 12 15:16:40 2017 2 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update failure: ECDSA signature mismatch, 192.168.15.100, ,

The following messages are generated as a result of failed firmware update due to HMAC integrity check error:

- 85 Sep 12 15:20:32 2017 1 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update initiated, 192.168.15.100, ,
- 86 Sep 12 15:20:38 2017 2 EVT_SOFTWARE_UPDATE, CryptoOfficer, System software update failure: HMAC check error, 192.168.15.100, ,

A.10.24 Audit Event: Maximum Quota

Audit log messages are generated when the maximum quotas of system resources have been reached – for example, the following message is generated as a result of the maximum 64 wireless clients being exceeded:

- 324 Apr 29 15:48:28 2015 2 EVT_RESOURCE_QUOTA_EXCEED, , No more room for new STAs, 8c:70:5a:40:f0:a0, ,

A.10.25 Audit Event: Attempts at Unlocking an Interactive Session

Sessions are terminated, not locked, due to inactivity and, therefore, there is no unlocking audit record. The authorized administrative user is required to re-authenticate thereby creating a new session. At that time, a login audit record will be generated.

A.10.26 Audit Event: Termination of a Remote Session by the Session Locking Mechanism

The remote session will be terminated by the device when the inactivity time period exceeds the configured value. The session timeout value can be configured under the "User Login Policy" page, covered under Section 2.7.3.

Audit log messages are generated when remote sessions are terminated due to inactivity—for example, the following message is generated when a remote session is terminated due to inactivity:

- 32 Mar 18 15:07:09 2015 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, Login session timed out., , ,

A.10.27 Audit Event: Termination of an Interactive Session

Audit log messages are generated whenever an authenticated administrator logs off the device—for example, the following message is generated as a result of a log off:

- 37 Mar 18 15:08:00 2015 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, httpd - User CryptoOfficer from 192.168.205.208 logged out, , ,

A.10.28 Audit Event: Denial of a Session Establishment due to MAC Address Filtering

Audit log messages are generated when a wireless client's access is denied based on MAC address, time and day—for example, the following messages are generated as a result of MAC address filtering:

- 8321 May 12 16:07:35 2015 2 EVT_STA_AUTH, , 802.11 ACL is active: REJECT STA, 00:0e:8e:4b:ba:3d, ,
- 8322 May 12 16:07:35 2015 2 EVT_STA_AUTH, , 802.11 mgmt authentication failure, , 00:0e:8e:4b:ba:3d,

A.10.29 Audit Event: Initiation of a Trusted Channel

Audit log messages are generated when a trusted channel is initiated. Trusted channels include TLS/HTTPS sessions used in the WEB interface as well as TLS sessions for remote audit logging. The following is an example of an audit log message when a remote audit logging trusted channel is established:

- 70 May 11 15:12:25 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS Initiated, , 192.168.205.23:8889,

The following is an example of an audit log message when a WEB interface trusted channel is established:

- 131 May 11 15:20:57 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS Initiated, 192.168.205.208:23253, ,

A.10.30 Audit Event: Termination of a Trusted Channel

The following is an example of an audit log message when a remote audit logging trusted channel is terminated:

- 139 May 11 15:28:36 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS Terminated, , 192.168.205.23:8889,

The following is an example of an audit log message when a WEB interface trusted channel is terminated:

- 132 May 11 15:20:57 2015 1 EVT_MANAGEMENT_CONNECTION, , TLS Terminated, 192.168.205.208:23253, ,

A.10.31 Audit Event: Failure of Trusted Channel or Trusted Path Functions

The following is an example of an audit log message when a remote audit logging trusted channel fails:

- 143 May 11 15:29:34 2015 2 EVT_MANAGEMENT_CONNECTION, , Failed to initiate a TCP connection to the audit server, , 192.168.205.9:8889,

A.10.32 Audit Event: Trust Channel Connection Re-establishment

No recovery is needed as the TOE will automatically attempt to establish a new connection.

A.10.33 Audit Event: Load Certificates that Fail to Meet the NDcPP Requirements

The following are some examples of audit log messages when loading certificates that fail to meet the NDcPP requirements:

- 278 Sep 11 11:12:31 2017 2 EVT_CERT_VALIDATION_ERR, CryptoOfficer, CRL issuer does not have CRL-sign capability. CRL cannot be used!, , ,
- 335 Sep 11 11:26:50 2020 2 EVT_CERT_VALIDATION_ERR, CryptoOfficer, Certificate is expired. Make sure your system clock is accurate., , ,

A.10.34 Audit Event: Configure Session Inactivity and Time out

- 366 Sep 11 11:37:44 2017 1 EVT_ADMIN_USER_AUTH, CryptoOfficer, Changed admin-user TestUser1 role=Administrator lockout period=3, session timeout=9,,,

A.10.35 Audit Event: Detection of Modification of Channel Data for 802.11 and 802.1x

- 8168 May 12 13:01:05 2015 2 EVT_KEY_TRANSFER_ERR, , IEEE 802.1x data frame from not associated STA, , 8c:70:5a:40:f0:a0,

A.10.36 Audit Event: Configure/Change the Reference Identifier for Peer

- 10 Apr 13 19:37:59 2018 1 EVT_SYSTEM_CONFIG, CryptoOfficer, NTP server 1 IPsec server id changed, old=636N-L3, new=636N-L2, , ,

A.11 Key Zeroization

The device zeroizes keys when it no longer uses them. The user can choose to reboot (Section 2.13.6) the device thus zeroizes the keys in RAM or choose "Factory Default" (Section 2.13.4) which will zeroize all keys in RAM and FLASH.

A.12 User Space Processors

The following user space processes typically run on the device:

Table 28: The List of User Space Processes

Process Name	Process Description
udevd	The device/event managing daemon to the Linux kernel
rngd	This daemon checks and feeds random data from hardware device to kernel random device
masterDaemon	The master daemon that start, stop and monitor 3eTI applications

Process Name	Process Description
syslogd	The Linux system logging daemon
klogd	The Kernel Log Daemon
configDaemon	The system configuration daemon
rtocd	The Radio Transfer Off Control (rtoc) daemon for scheduling and maintaining radio silence
syscmdd	The system command scheduler daemon
miscHWD	The miscellaneous hardware daemon that controls hardware buttons and LED displays
self-testd	The daemon for performing on-demand or periodic self-test
mini_httpd	The HTTPS web server daemon
radard	The daemon to perform radar signal detection and dynamic frequency selection
radioPHYd	The daemon that monitors and controls radio PHY settings
xcManager	The XML-based system configuration manager daemon
hostapd	This daemon provides IEEE 802.11 access point management functionality and implements IEEE 802.1X Authenticator to enforce WLAN client authentication.
auditlogd	The user space security auditing daemon
starter	The IPsec starter daemon that starts and configures the keying daemon charon
charon	The IPsec keying daemon for establishing IKEv2 VPN connections
ntpd	The daemon that sets and maintains the system time in synchronization with time servers using the Network Time Protocol (NTP)

Note: All processes listed run at hardware privilege ring 1 and software privilege as root.

Appendix B. Term Reference Guide

B.1 Acronyms and Abbreviations

3DES	–	Triple Data Encryption Standard
3eTI	–	3e Technologies International
AC	–	Alternating Current
AES	–	Advanced Encryption Standard
AP	–	Access Point
AS	–	Authentication Server
AWB	–	Auto-forming Wireless Bridging
BSS	–	Basic Service Set
BSSID	–	Basic Service Set Identifier
CA	–	Certificate Authority
CAC	–	Common Access Card
CBC	–	Cipher Block Chaining
CCM	–	Counter with CBC-MAC
CCMP	–	Counter-mode/CBC-MAC Protocol
CMVP	–	Cryptographic Module Validation Program
CRL	–	Certificate Revocation List
CSV	–	Certified Server Validation
CTR	–	Counter Mode
CTS	–	Clear to Send
DES	–	Data Encryption Standard
DFS	–	Dynamic Frequency Selection
DHCP	–	Dynamic Host Configuration Protocol
DLC	–	Data Link Control
DNS	–	Domain Name System
DoD	–	Department of Defense
DS	–	Data Server
DSSS	–	Direct-Sequence Spread Spectrum
DTIM	–	Delivery Traffic Indication Message
EAL	–	Evaluation Assurance Level
EAP	–	Extensible Authentication Protocol
EAPoL	–	Extensible Authentication Protocol over LAN
ECB	–	Electronic Codebook
FHSS	–	Frequency-Hopping Spread Spectrum
FIPS	–	Federal Information Processing Standards
GHz	–	Gigahertz
GUI	–	Graphical User Interface
HTTPS	–	Hypertext Transfer Protocol Service
IANA	–	Internet Assigned Numbers Authority
MAC	–	Media Access Control
MAC	–	Message Authentication Code
Mbps	–	Megabits per second
MHz	–	Megahertz
MIB	–	Management Information Base
MIC	–	Message Integrity Check
MIMO	–	Multiple-input and Multiple-output
MP	–	Mobile Power
MSDU	–	MAC Service Data Unit
NIST	–	National Institute of Standards and Technology
NMS	–	Network Management Station
NTP	–	Network Time Protocol
OCSP	–	Online Certificate Status Protocol
OFDM	–	Orthogonal Frequency Division Multiplexing
OSI	–	Open Systems Interconnection
PC	–	Personal Computer
PDA	–	Personal Digital Assistant
PEM	–	Privacy Enhanced Mail
PHY	–	Physical Layer
PIN	–	Personal Identification Number
PKI	–	Public Key Infrastructure
PMK	–	Primary Master Key
PoE	–	Power-over-Ethernet
PSK	–	Pre-Shared Key
PTZ	–	Pan/Tilt/Zoom
Pwr	–	Power
RF	–	Radio Frequency
RFC	–	Request for Comments
RSN	–	Robust Security Network
RSSI	–	Received Signal Strength Indicator
RSTP	–	Rapid Spanning Tree Protocol
RTS	–	Request to Send
Rx	–	Reception
SHA	–	Secure Hash Algorithm
SNMP	–	Simple Network Management Protocol
SP	–	Service Pack
SS	–	Signal Strength
SSID	–	Service Set Identifier

ICMP	–	Internet Control Message Protocol
ID	–	Identifier
IE	–	Information Element
IEEE	–	Institute of Electrical and Electronics Engineers
IP	–	Internet Protocol
ISP	–	Internet Service Provider
LAN	–	Local Area Network
LED	–	Light Emitting Diode
LLC	–	Logical Link Control
SSL	–	Secure Socket Layer
STA	–	Station
STP	–	Spanning Tree Protocol
TCP	–	Transmission Control Protocol
TLS	–	Transport Layer Security
TU	–	Time Unit
Tx	–	Transmission
URL	–	Uniform Resource Locator
VDC	–	Volts Direct Current
VLAN	–	Virtual Local Area Network
VPK	–	Virtual Private Network
VPN	–	Virtual Private Network
WAN	–	Wide Area Network
WDS	–	Wireless Distribution System
Wi-Fi	–	Wireless Fidelity
WLAN	–	Wireless Local Area Network
WPA2	–	Wi-Fi Protected Access 2

B.2 Term Definitions

Term	Definition
Triple Data Encryption Standard (3DES)	3DES is a mode of the DES encryption algorithm that encrypts data three times.
802.11	802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997
802.11b (also referred to as 802.11 High Rate or Wi-Fi)	802.11b is an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
Access Point (AP)	An AP is a gateway set up to allow a group of LAN users access to another group or a main group. The AP does not use the DHCP server function and therefore accepts IP address assignments from the controlling network.
Advanced Encryption Standard (AES)	AES is a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing DES encryption. AES works at multiple network layers simultaneously.
Bridge	A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet or Token-Ring.
Dynamic Host Configuration Protocol (DHCP)	DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic

Term	Definition
	addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many Internet Service Providers (ISPs) use dynamic IP addressing for dial-up users.
Network Management Station (NMS)	NMS includes management software such as, HP Openview and IBM Netview.
Service Set Identifier (SSID)	A SSID is a Network ID unique to a network. Only clients and APs that share that the same SSID are able to communicate with each other. This string is case-sensitive. Wireless LANs offer several security options, but increasing the security also means increasing the time spent managing the system. Encryption is the key. The biggest threat is from intruders coming into the LAN. You set a seven-digit alphanumeric security code, called an SSID, in each wireless device and they thereafter operate as a group.
Wireless Local Area Network (WLAN)	A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

Appendix C. Serial I/O Interface Board

The Serial I/O Interface Board Cable is used to connect to the **SERIAL – I/O** connector on the 3e-523N as shown in Figure 107. The Serial I/O Termination connector provides secure termination for connections to serial I/O, LED status, and power as described in Table 29.

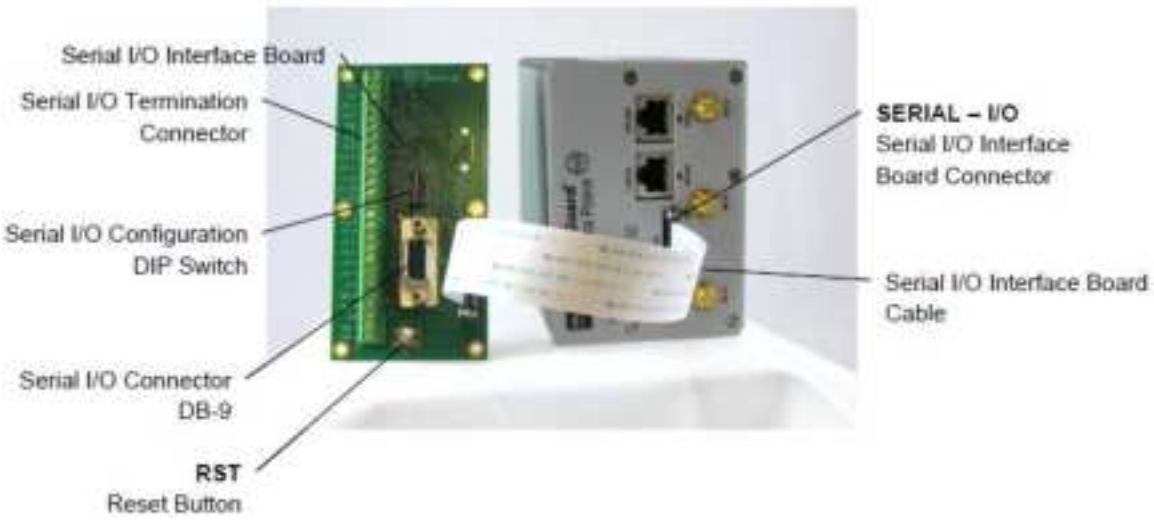


Figure 107: Serial I/O Interface Board

Table 29: Serial I/O Termination	
Terminal Block Label	**Connection Description**
IN 1 -	General Input[1]
IN 1 +	General Input[1]
OUT 1 +	General Output[2]
OUT 1 -	General Output[2]
PWR -	Ground (black wire for AMR)
IN 0 -	General Input[1] (green wire for AMR)
IN 0 +	General Input[1]
OUT 0 +	General Output[2]
OUT 0 -	General Output[2] (red wire for AMR)
RX-/TX	RS-485/422 receive (1/2 of pair), RS-232 Transmit (output from 3e-523N) Parallel to DB-9 pin 3
RX+/RTS	RS-485/422 receive (1/2 of pair), RS-232 RTS (input to 3e-523N) Parallel to DB-9 pin 7
TX+/CTS	RS-485/422 transmit (1/2 of pair), RS-232 CTS (output from 3e-523N) Parallel to DB-9 pin 8
TX-/RX	RS-485/422 transmit (1/2 of pair), RS-232 Receive (input to 3e-523N) Parallel to DB-9 pin 2
LED A -	Active low LED driver[3] (ties to LED Cathode, with 100 ohms limiting resistor)
LED B -	Active low LED driver[3]
LED C -	Active low LED driver[3]

Table 29: Serial I/O Termination	
Terminal Block Label	**Connection Description**
LED D -	Active low LED driver[3]
LED E -	Active low LED driver[3]
LED F -	Active low LED driver[3]
+3.3V	LED driver voltage source (ties to LED Anode terminal)
SMB CK	SM Bus Clock signal
SMB DT	SM Bus Data
GND	Circuit Ground
PWR -	Alternate power return (limited to 2A max)
PWR +	Alternate power source (limited to 2A max)

Notes:

1. Inputs limited to +13V maximum, signal drives an opto-coupler (LED side), internal circuits include current limiting resistor.
2. Outputs require source voltage and current limiting. Use up to +13V and minimum 1,000 ohm limiting resistor. Source voltage (from the 3e-523N device) can be switched in using positions 1 to 3 (switch to "ON" side) of "S1" DIP switch.
3. LED functionality currently reserved. LED A and LED B indicate Ethernet traffic, mirrors "WAN" indicator on the 3e-523N unit.

The Serial I/O Configuration DIP switch (Figure 108) allows you to configure the interface as described in Table 30.

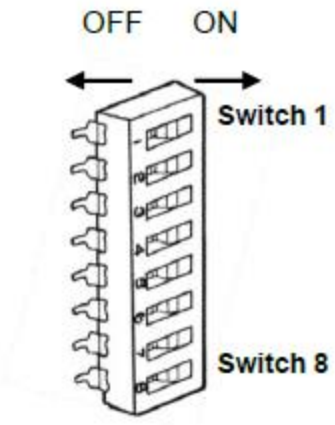


Figure 108: Serial I/O Configuration DIP Switch

Table 30: Serial I/O Configuration DIP Switch	
Switch	**Name**
1	"ON" Connects input power rail to source both "OUT 1 +" and "IN 1 +" terminals
2	"ON" Connects input power rail to source "IN 0 +" terminal
3	"ON" Connects input power rail to source "OUT 0 +" terminal
4	Set RS-485 slew rate to "low" (default, OFF position, is high slew rate)
5	Terminate RS-485 RX pair with 120-ohm load
6	Set to Half-Duplex RS-485 mode (must switch both 6 & 7 to "ON" position)
7	Set to Half-Duplex RS-485 mode (must switch both 6 & 7 to "ON" position)
8	Terminate RS-485 TX pair with 120-ohm load

The Serial I/O Connector provides an RS232 serial I/O port via a standard DB-9 connector as shown in Table 31.

Table 31: DB-9 Serial I/O Connector		
Pin	**Signal Name**	**Name**
1	CD	Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	System Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send
9	RI	Ring Indicator

Appendix D. 3e-523E-900 Specific Operation

D.1 3e-523E-900 Overview

The 3e-523E-900 system transmits WiFi protocols over the 900MHz ISM band instead of 2.4GHz or 5GHz bands at up to 1Watt RF power. Channel selection is limited to four selections, distributed across 902 to 928 MHz. The 900MHz signal is transmitted out of the 3e-523E-900 unit at the external RF port (bulkhead N-style antenna connection) through a supplied RF cable. Antenna selections are limited to +6dBi (or lower) omni-directional of dipole construction, or a +6dBi (or lower gain) directional Yagi style.

D.2 PHY Settings Specific to 3e-523E-900

In the 3e-523E-900, wireless mode is locked as 802.11b mode. Channels are limited to 5MHz channel bandwidth and distributed as shown below.

The PHY Setting screen, see Figure 41, allows the user to access only the available channels (802.11b mode, 5MHz bandwidth per channel). Transmit power settings for the 3e-523E-900 are limited to use Fixed mode only, and up to level 4 or 5 depending on the channel. The remaining options on this page are the same as the 3e-523N.

Table 32: 3e-523E-900 Frequency Channel Numbers

Wireless Mode	Channel No.	Fixed Power Level
802.11b	7 (906 MHz) 8 (911 MHz) 9 (916 MHz) 10 (921 MHz)	3, 4, or 5

Appendix E. Technical Support

E.1 Manufacturer's Statement

The 3e-523N and 3e-525N are provided with a warranty. It is not desired or expected that the user opens the device. If a malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.

If you are experiencing trouble with this unit, the point of contact is:

support@ultra-3eTI.com
1-800-449-3384, option 2
or visit our web site at www.ultra-3eti.com