

Communication Setup Using Firmware Version 3.0.00512

Table of Contents

Section	Page	Section	Page
Introduction		Device Management	13
Qualified Persons	2	Interfaces	20
Read this Instruction Sheet	2	Wi-Fi	23
Retain this Instruction Sheet.	2	Security	
Proper Application	2	Backup and Restore	28
Special Warranty Provisions.	3	User Accounts	29
Safety Information		Certificate Management	31
Understanding Safety-Alert Messages.	4	Web Access Configuration	32
Following Safety Instructions	4	VPN.	34
Replacement Instructions and Labels	4	Syslog.	46
Safety Precautions	5	Security—Advanced	
Wi-Fi Administration		Password Complexity	50
Connecting to the 6800 Series Control	6	User Role Configuration	51
Login	8	Firewall	54
General Status	10	Diagnostics	65
Security Status	13		

These instructions are for the R3 Communication Module running the 3.0.00512 software version.



Qualified Persons

WARNING

Only qualified persons who are knowledgeable in the installation, operation, and maintenance of overhead and underground electric distribution equipment, along with all associated hazards, may install, operate, and maintain the equipment covered by this publication. A qualified person is someone who is trained and competent in:

- The skills and techniques necessary to distinguish exposed live parts from nonlive parts of electrical equipment
- The skills and techniques necessary to determine the proper approach distances corresponding to the voltages to which the qualified person will be exposed
- The proper use of special precautionary techniques, personal protective equipment, insulated and shielding materials, and insulated tools for working on or near exposed energized parts of electrical equipment

These instructions are intended only for such qualified persons. They are not intended to be a substitute for adequate training and experience in safety procedures for this type of equipment.

Read this Instruction Sheet

NOTICE

Thoroughly and carefully read this instruction sheet and all materials included in the product's S&C Instruction Handbook before installing or operating the 6800 Series control. Become familiar with the Safety Information and Safety Precautions on pages 4 and 5. The latest version of this publication is available online in PDF format at sandc.com/en/support/product-literature/.

Retain this Instruction Sheet

This instruction sheet is a permanent part of the 6800 Series control. Designate a location where users can easily retrieve and refer to this publication.

Proper Application

WARNING

The equipment in this publication is only intended for a specific application. The application must be within the ratings furnished for the equipment. See S&C Specification Bulletin 1045-31.

Special Warranty Provisions

The standard warranty contained in S&C's standard conditions of sale, as set forth in Price Sheets 150 and 181, applies to the 6800 Series Automatic Switch Control, except the first paragraph of the said warranty is replaced by the following:

(1) General: The seller warrants to the immediate purchaser or end user for a period of 10 years from the date of shipment that the equipment delivered will be of the kind and quality specified in the contract description and will be free of defects of workmanship and material. Should any failure to conform to this warranty appear under proper and normal use within 10 years after the date of shipment, the seller agrees, upon prompt notification thereof and confirmation that the equipment has been stored, installed, operated, inspected, and maintained in accordance with the recommendations of the seller and standard industry practice, to correct the nonconformity either by repairing any damaged or defective parts of the equipment or (at the seller's option) by shipment of necessary replacement parts. The seller's warranty does not apply to any equipment that has been disassembled, repaired, or altered by anyone other than the seller. This limited warranty is granted only to the immediate purchaser or, if the equipment is purchased by a third party for installation in third-party equipment, the end user of the equipment. The seller's duty to perform under any warranty may be delayed, at the seller's sole option, until the seller has been paid in full for all goods purchased by the immediate purchaser. No such delay shall extend the warranty period.

Replacement parts provided by the seller or repairs performed by the seller under the warranty for the original equipment will be covered by the above special warranty provision for its duration. Replacement parts purchased separately will be covered by the above special warranty provision.

For equipment/services packages, the seller warrants for a period of one year after commissioning that the 6800 Series Automatic Switch Control will provide automatic fault isolation and system reconfiguration per agreed-upon service levels. The remedy shall be additional system analysis and reconfiguration of the IntelliTeam SG Automatic Restoration System until the desired result is achieved.

Warranty of the 6800 Series Automatic Switch Control is contingent upon the installation, configuration, and use of the control or software in accordance with S&C's applicable instruction sheets.

This warranty does not apply to major components not manufactured by S&C, such as batteries and communication devices. However, S&C will assign to the immediate purchaser or end user all manufacturer's warranties that apply to such major components.

Warranty of equipment/services packages is contingent upon receipt of adequate information on the user's distribution system, sufficiently detailed to prepare a technical analysis. The seller is not liable if an act of nature or parties beyond S&C's control negatively impact performance of equipment/services packages; for example, new construction that impedes radio communication, or changes to the distribution system that impact protection systems, available fault currents, or system-loading characteristics.

Safety Information

Understanding Safety-Alert Messages

Several types of safety-alert messages may appear throughout this instruction sheet and on labels and tags attached to the 6800 Series Automatic Switch Control. Become familiar with these types of messages and the importance of these various signal words:

DANGER

“DANGER” identifies the most serious and immediate hazards that will result in serious personal injury or death if instructions, including recommended precautions, are not followed.

WARNING

“WARNING” identifies hazards or unsafe practices that can result in serious personal injury or death if instructions, including recommended precautions, are not followed.

CAUTION

“CAUTION” identifies hazards or unsafe practices that can result in minor personal injury if instructions, including recommended precautions, are not followed.

NOTICE

“NOTICE” identifies important procedures or requirements that can result in product or property damage if instructions are not followed.

Following Safety Instructions

If any portion of this instruction sheet is unclear and assistance is needed, contact the nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C’s website sandc.com, or call the S&C Global Support and Monitoring Center at 1-888-762-1100.

NOTICE

Read this instruction sheet thoroughly and carefully before installing a 6800 Series Automatic Switch Control.



Replacement Instructions and Labels

If additional copies of this instruction sheet are needed, contact the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

It is important that any missing, damaged, or faded labels on the equipment be replaced immediately. Replacement labels are available by contacting the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

⚠ DANGER



The 6800 Series Automatic Switch Control line voltage input range is 93 to 276 Vac. Failure to observe the precautions below will result in serious personal injury or death.

Some of these precautions may differ from your company's operating procedures and rules. Where a discrepancy exists, follow your company's operating procedures and rules.

- | | |
|--|---|
| <ol style="list-style-type: none"> 1. QUALIFIED PERSONS. Access to the 6800 Series Automatic Switch Control must be restricted only to qualified persons. See the "Qualified Persons" section on page 2. 2. SAFETY PROCEDURES. Always follow safe operating procedures and rules. 3. PERSONAL PROTECTIVE EQUIPMENT. Always use suitable protective equipment, such as rubber gloves, rubber mats, hard hats, safety glasses, and flash clothing, in accordance with safe operating procedures and rules. | <ol style="list-style-type: none"> 4. SAFETY LABELS. Do not remove or obscure any of the "DANGER," "WARNING," "CAUTION," or "NOTICE" labels. 5. MAINTAINING PROPER CLEARANCE. Always maintain proper clearance from energized components. |
|--|---|

Connecting to the 6800 Series Control

Follow these steps to open the *Wi-Fi Configuration* screens:

STEP 1. In the Windows® 10 **Start** menu select *Start>Programs>S&C Electric>LinkStart>LinkStart V4*. The *Wi-Fi Connection Management* screen will open. See Figure 1.

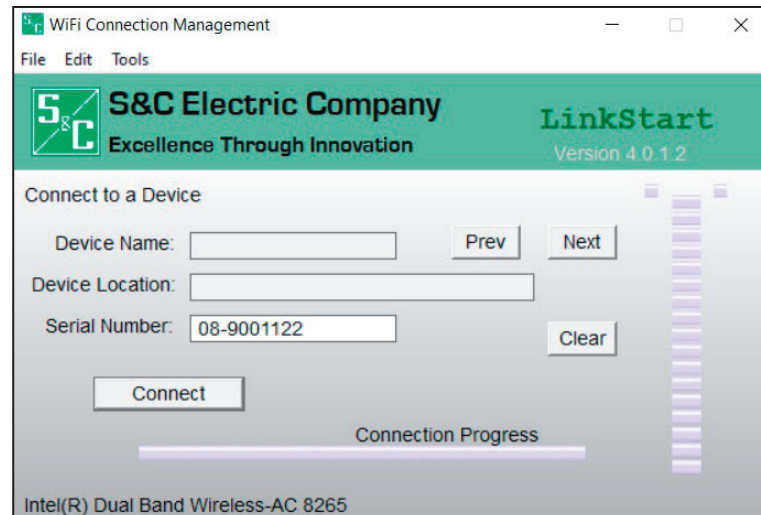


Figure 1. The LinkStart *Main* screen.

STEP 2. Enter the serial number of the 6800 Series control and click on the **Connect** button. See Figure 1. The **Connect** button changes to the **Cancel** button, and connection progress is shown on the connection status bar.

STEP 3. If the Enter Passphrase dialog box opens, enter the configured WPA2-PSK passphrase and click on the **OK** button to continue. See Figure 2 and the “WPA2-PSK Manual Setting” section on page 24 for additional details on WPA2-PSK Manual passphrase configuration.

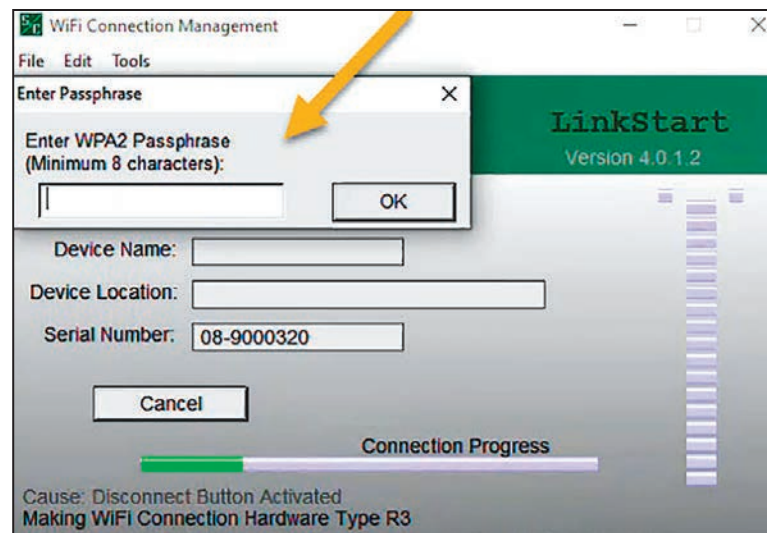


Figure 2. The Enter Passphrase dialog box.

When connection is established, the status bar indicates “Connection Successful” and displays a solid green bar. The vertical bar graph indicates signal strength of the Wi-Fi connection. See Figure 3.

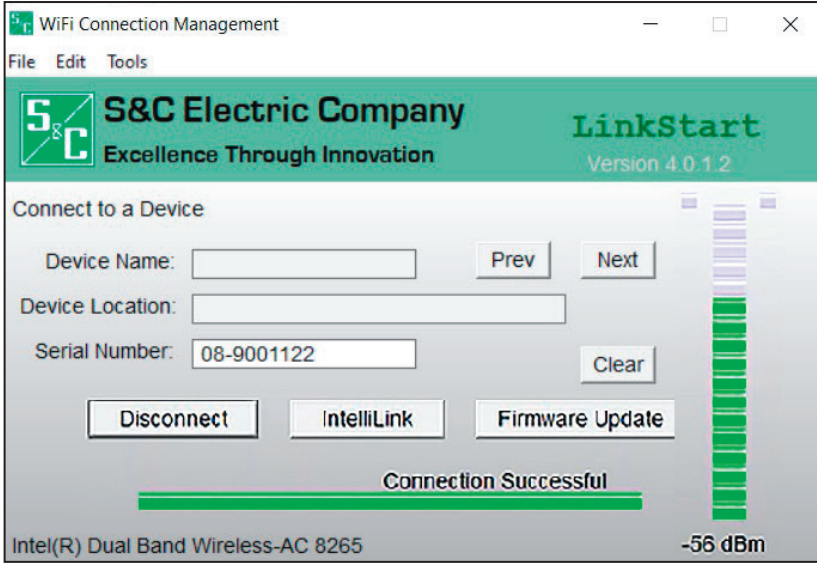


Figure 3. Successful connection to the 6800 Series control.

STEP 4. Open the **Tools** menu and click on the **Wi-Fi Administration** option. See Figure 4. The *Login* screen will open. See Figure 5 on page 8.

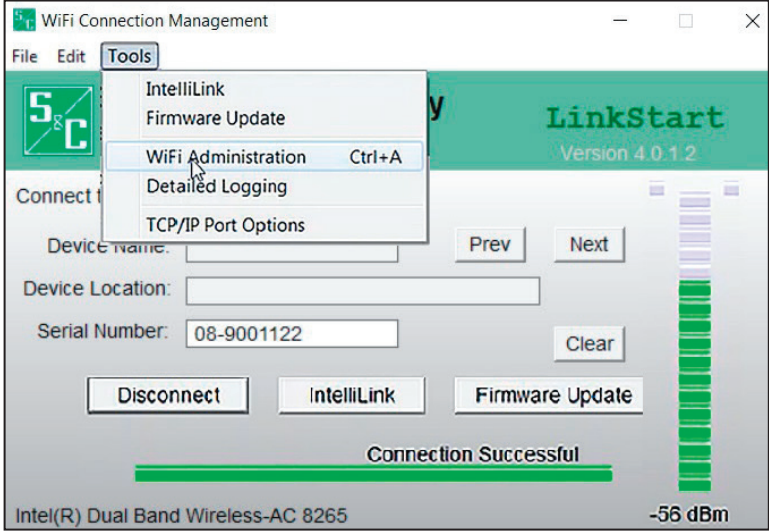


Figure 4. The Wi-Fi Administration entry on the Tools menu.

Login

The *Login* screen opens with username and password entry fields. See Figure 5. These screens are displayed in the Internet browser on the computer. The supported browser versions include Google Chrome and Microsoft Edge. The IP address is displayed at the top of the screen and is supplied by the R3 Communication Module.

Enter the appropriate username and password and click on the **Login** button. Authentication status is displayed.

The default administrator username and password can be requested from S&C by calling the Global Support and Monitoring Center at 888-762-1100 or by contacting S&C through the S&C Customer Portal at sandc.com/en/support/sc-customer-portal/.



Figure 5. The *Login* screen.

NOTICE

At the initial login with the default username and password, the user will be redirected to the *My User Account* screen. The default username and password must be changed before proceeding. This step cannot be skipped because the user will be unable to navigate to any other page until the password is changed.

The password entry must be at least eight characters in length and contain at least one uppercase letter, one lowercase, one number, and one special character. The admin or any user with a security admin role can modify password complexity. When entries are complete, click on the **Save** button to save the new password.

To change the default username and password for other user accounts, select the **User Accounts** tab from the **Security** menu. Click on the icon in the top right corner of the screen. Click on the **My User Account** link in the field that appears when hovering over the icon. See Figure 6 on page 9.

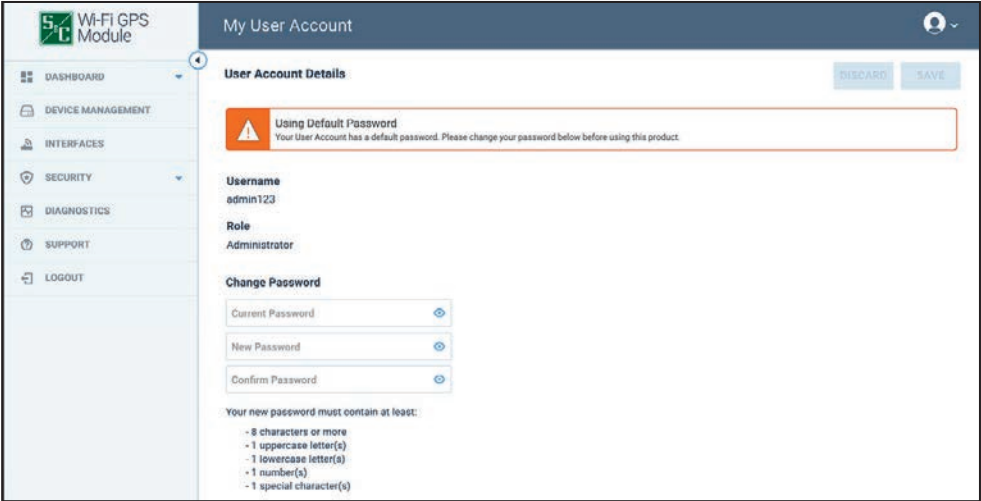


Figure 6. The My User Account screen.

Note: Cybersecurity features depend on whether a serial or Ethernet configuration is used between the R3 Communication Module and the S&C control. However, the Web user interface will remain the same no matter which configuration is used. See Table 1.

Table 1. Cybersecurity Feature Usability

Feature	Serial Configuration	Ethernet Configuration
Backup and Restore	Limited	Yes
User Accounts	Yes	Yes
Certificate Management	Limited	Yes
Web Access Configuration	No	Yes
VPN	No	Yes
Syslog	No	Yes
Password Complexity	Yes	Yes
User Role Configuration	Yes	Yes
Firewall	No	Yes

General Status

The *General Status* screen is informational and only displays data; no edits are allowed. Field edits are permitted in the respective menu sections where each field is defined. See Figure 7.

Note: The sample screens shown in this document do not display specific information such as the IP address. This information is user-specific.

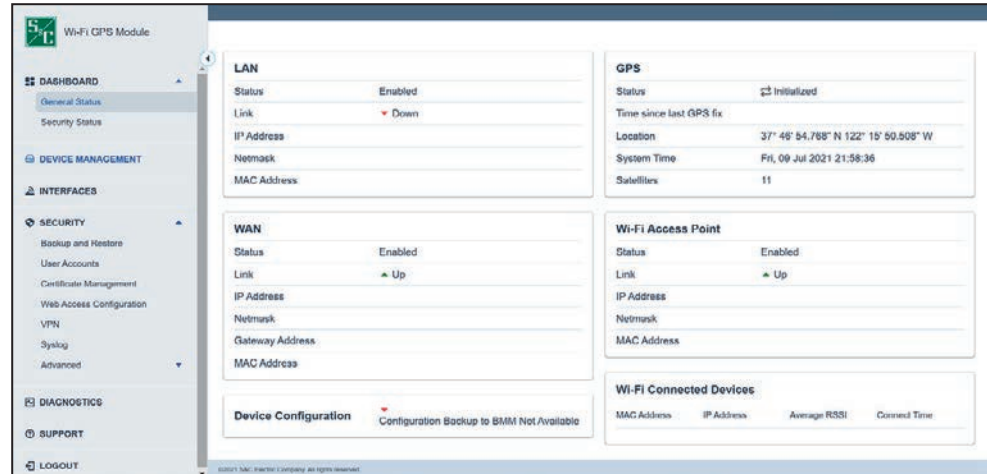


Figure 7. The *General Status* screen.

The *General Status* screen is comprised of the following data fields:

Host Name – This is the label assigned to the R3 Communications Module, defined in the “Device Management” section of the Web user interface.

Software Version – This displays the version of software installed on the R3 Communication Module.

Serial Number – This is a unique number assigned during manufacturing of the R3 Communication Module for identification and inventory purposes.

App Version – This is the S&C application version, including the build time.

Platform Version – This is the R3 Communications Module platform firmware version.

Configuration Version – This updates monotonically with each change to the device configuration (which includes **Interfaces** or **Device Management** settings).

Last Backup – This is the date/time of the last backup of the device configuration to the base memory module (BMM). This option is only available for the new IntelliRupter fault interrupter R3 control, not for the 6800 Series controls or the older IntelliRupter fault interrupter controls.

LAN

Table 2. Local Area Network (LAN) Descriptions

Field	Value/Format	Description
Status	Enabled Disabled	Status of the LAN interface
Link	Up Down	Link status of the LAN connection
IP address	000.000.000.000 format	Static IP address of the LAN interface
Netmask	000.000.000.000 format	Netmask of the LAN, defining the range of allowable IP addresses on the LAN
MAC address	00:00:00:00:00:00 format	MAC address of the LAN interface

WAN

Table 3. Wide Area Network (WAN) Descriptions

Field	Value/Format	Description
Status	Enabled Disabled	Status of the WAN interface
Link	Up Down	Link status of the WAN connection
IP address	000.000.000.000 format	Static IP address of the WAN interface
Netmask	000.000.000.000 format	Netmask of the WAN, defining the range of allowable IP addresses on the WAN
Gateway address	000.000.000.000 format	Default Gateway IP address for the WAN

Device Configuration

Table 4. Device Configuration Descriptions

Value/Format	Explanation
Synced	Settings are synced between the communication module and the base memory module
Not synced	Settings are different between the communication module and the base memory module
Configuration backup to BMM not available	Option not available on 6800 Series control or older IntelliRupter fault interrupter controls

GPS

Table 5. Global Positioning System (GPS) Descriptions

Field	Value/Format	Description
Status	Initialized Up Down	Status of the GPS interface as it searches for location
Time since last GPS fix	Seconds	Time elapsed since the R3 last acquired a GPS location + time fix from its satellite info
Location	Latitude/Longitude	The latitude and longitude of the R3 control as derived from GPS data
System time	Day; Date: Day Month Year; Time: 00:00:00	The local time of the device as derived from GPS or network data
Satellites	Number (count)	The total number of satellites in view as derived from the GPS data

Wi-Fi Access Point

Table 6. Wi-Fi Access Point Descriptions

Field	Value/Format	Description
Status	Enabled Disabled	Status of the Wi-Fi access point interface
Link	Up Down	Link status of the Wi-Fi access point connection
IP address	000.000.000.000 format	Static IP address of the Wi-Fi access point interface
Netmask	000.000.000.000 format	Netmask of the Wi-Fi access point, defining the range of allowable IP addresses on the Wi-Fi access point
MAC address	00:00:00:00:00:00 format	MAC address of the Wi-Fi access point interface

Wi-Fi Connected Devices

Table 7. Wi-Fi Connected Device Descriptions

Field	Value/Format	Description
MAC address	00:00:00:00:00:00 format	MAC address of the client device connected to the R3 module's Wi-Fi access point
IP address	000.000.000.000 format	IP address of the client device connected to the R3 module's Wi-Fi access point
Average RSSI	Negative number	Moving average recorded signal strength of the client device connected to the R3 module's Wi-Fi access point
Connect time	Days:Hours:Minutes:Seconds	Connection duration of the client device connected to the R3 module's Wi-Fi access point

Security Status

The *Security Status* screen is informational and only displays data; no edits are allowed. See Figure 8. Field edits are permitted in the respective menu sections where each field is defined.

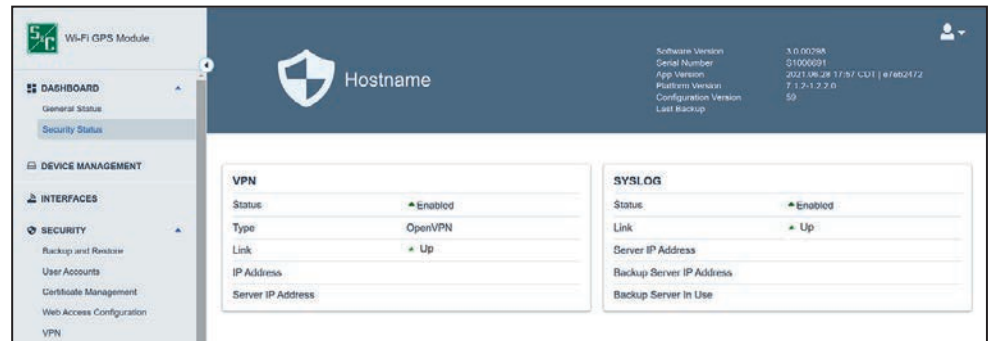


Figure 8. The *Security Status* screen.

Device Management

Click on the Device Management entry in the left menu to open the *Device Management* screen. The device configuration can be viewed, edited, or modified. See Figure 9.

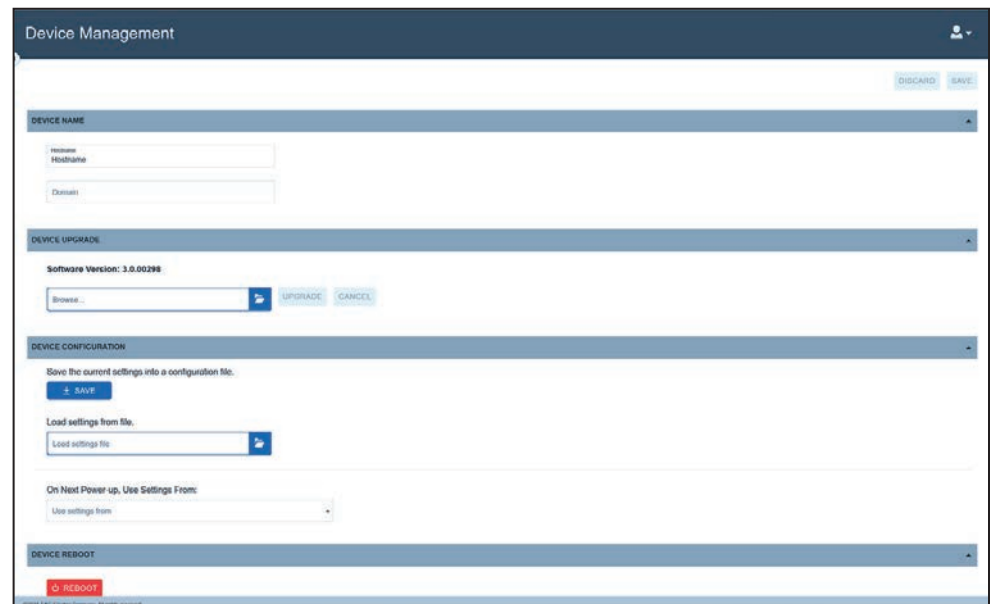


Figure 9. The System Name and Firmware Upgrade panels on the *Device Management* screen.

The *Device Management* screen contains the Device Name, Device Upgrade, Device Configuration, and Device Reboot panels.

Device Name

Enter a user-defined name for the **Hostname** field and click on the **Save** button. The entry is limited to 50 characters. The **Hostname** field is displayed on the *General Status* screen at the top. The **Domain** field is optional and used to indicate specific information for the device. See Figure 9 on page 13.

Device Upgrade

The **Device Upgrade** panel is used to load new firmware onto the R3 Communication Module.

Follow these steps to perform a firmware upgrade:

- STEP 1.** Locate the firmware file (.img) for download to the computer. The firmware files are located in the S&C Customer Portal at sandc.com/en/support/sc-customer-portal/.
- STEP 2.** When the firmware file has been successfully downloaded to a PC, the firmware file will need to be uploaded to the R3 Communication Module. Click on the **Browse** button in the Device Upgrade panel. See Figure 10.



Figure 10. Upload the firmware file to the R3 Communication Module.

STEP 3. In the *Open* screen, navigate to and select the desired firmware file. Then, click on the **Open** button to begin the upload process. See Figure 11.

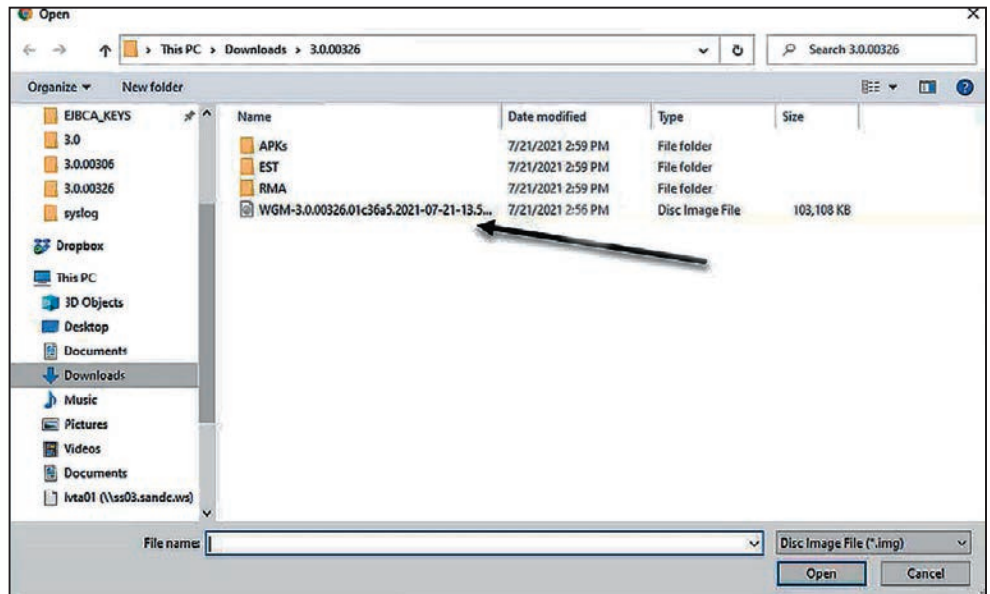


Figure 11. The Windows *Open* screen.

A dialog box will appear indicating “File Upload in Progress.” See Figure 12.

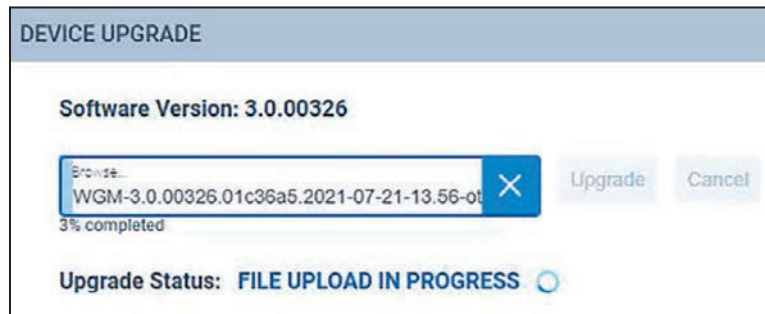


Figure 12. The upgrade status indicated on the Device Upgrade dialog box.

The Success dialog box appears to indicate the firmware was successfully downloaded. See Figure 13.

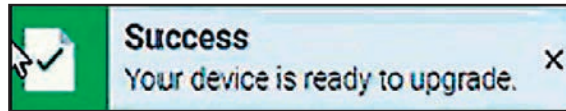


Figure 13. The Success dialog box.

STEP 4. The communication module verifies S&C Electric Company digitally signed the firmware. This step is automated. See Figure 14.

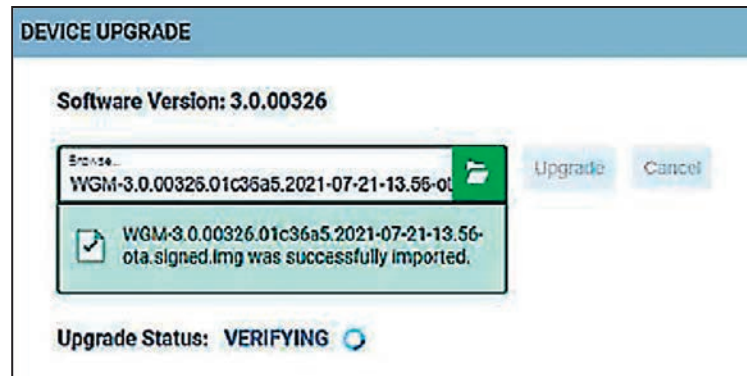


Figure 14. Verifying the digital signature.

STEP 5. When verification is complete, a notification appears in the top right corner of the screen. Click on the X button to dismiss the notification. In the Device Upgrade dialog box, the **Upgrade** button will indicate blue and the **Upgrade Status** field will indicate "Verified." See Figure 15.

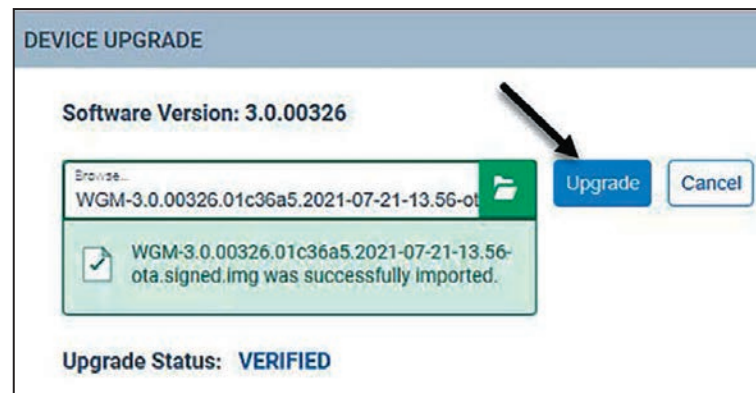


Figure 15. Upgrade status verified.

STEP 6. Click on the **Upgrade** button to initiate the **Upgrade** process. The dialog box will indicate “Device Upgrade in Progress.” See Figure 16.



Figure 16. Device upgrade in progress.

STEP 7. When the upgrade process completes, a notification appears indicating the R3 Communication Module will be unavailable while it reboots. The reboot will take several minutes to complete. See Figure 17.

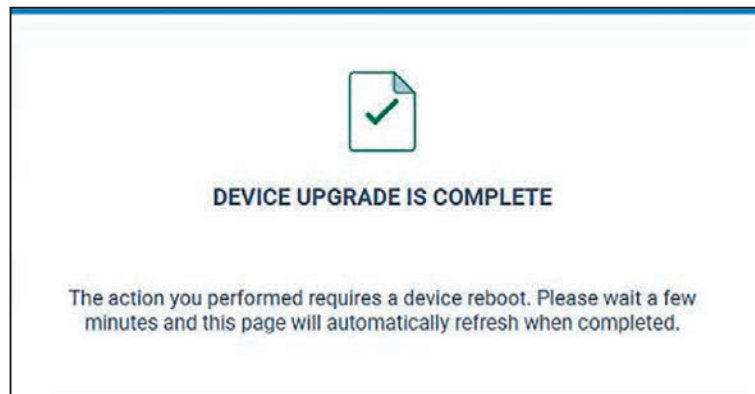


Figure 17. Device upgrade complete, reboot in progress.

STEP 8. The *Login* screen opens when the reboot is complete. Log in and confirm the new firmware has been installed successfully by checking the *General Status* screen.

Device Configuration

The Device Configuration panel allows a user to save the device settings, load a settings file to the device, and determine where to load settings from the next time the device powers up. There are three menu options: **Save**, **Load Settings from a File**, and **On Next Power-Up, Use Settings From**. (Not applicable for 6800 Series controls.)

The **Save** operation allows configuration settings assigned to the R3 Communication Module to be downloaded from the module and saved to a local computer or hard drive. The **Save** button writes the present settings to an XML file (.json extension) for export to a local hard drive or external memory device. The download process will begin when the **Save** button is selected in the Device Configuration panel. See Figure 18.

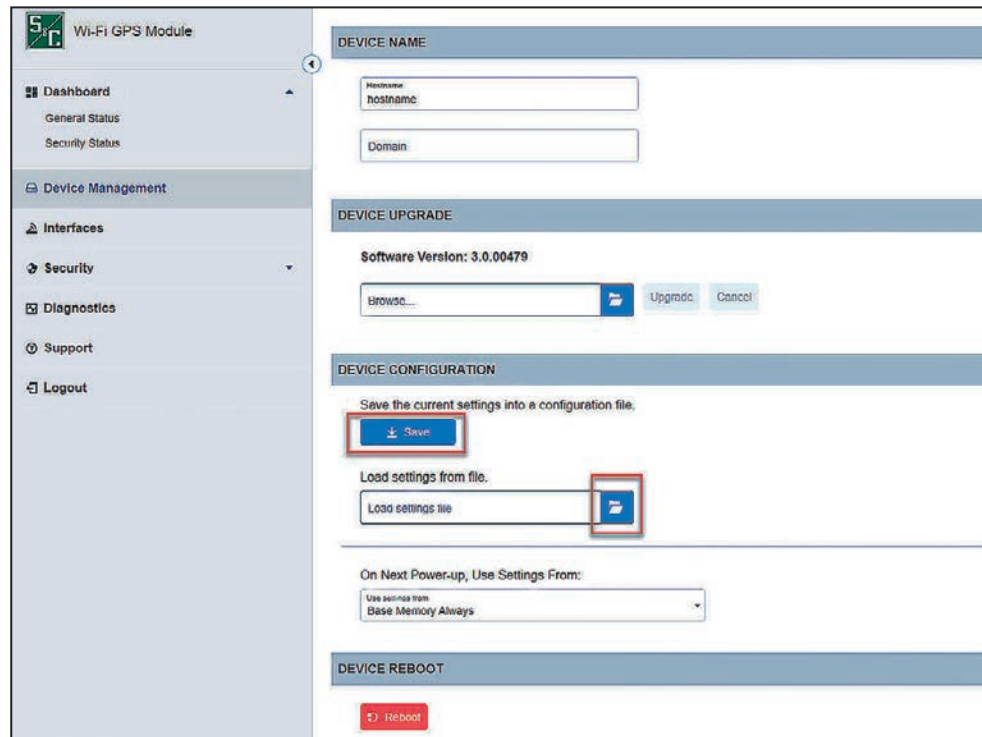


Figure 18. The Device Configuration panel of the *Device Management* screen.

The **Load** feature allows configuration settings from a previously stored XML file to be uploaded to the R3 Communication Module. The **Load Settings from File** option imports settings from when the device is power cycled. Clicking on the **Folder** icon in the Device Configuration panel invokes a series of dialog boxes allowing navigation on a PC to a saved configuration file. See Figure 18.

The **On Next Power Up, Use Settings From** feature is only available for the IntelliRupter® Fault Interrupter.

Device Reboot

The red **Reboot** button enables the user to restart the communication module. When selected, a dialog box appears for confirmation of the **Reboot** command. After the **Reboot** button is clicked, the Device Reboot in Progress dialog box appears. See Figure 19. The entire reboot process requires a few minutes to complete before communication to the R3 Communication Module is re-established. When the reboot is complete, the user interface will automatically load the *Login* screen.

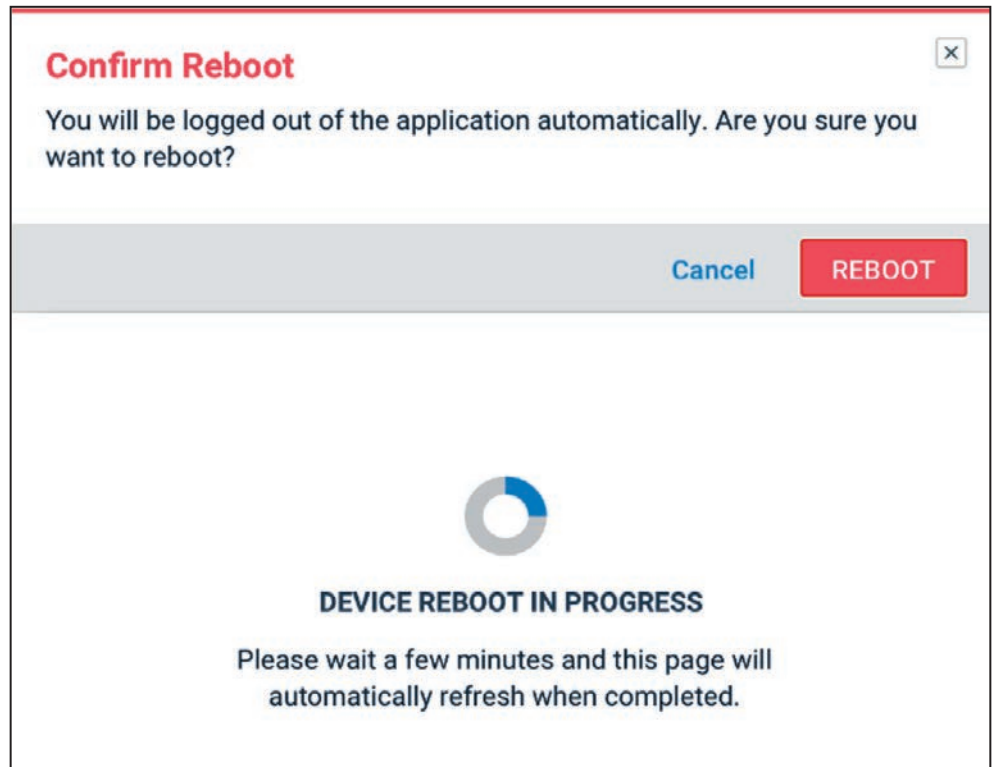


Figure 19. The Device Reboot dialog box.

Interfaces

The *Interfaces* screen is used to specify how the R3 Communication Module will communicate externally with other devices. The R3 Communication Module consists of three physical interfaces (Ethernet 1, Ethernet 2, and Serial 1) and one logical interface (Wi-Fi Access Point).

Ethernet 1 (To 6800 Faceplate)

Ethernet 1 is the interface associated with the R3 Communication Module local area network (LAN). Ethernet 1 is defined for devices connecting to physical Ethernet Port 1. Two toggle buttons are in the Ethernet 1 interface panel (**Enable Ethernet 1** and **Enable Ping**), and two data entry fields (**Static IP Address** and **Netmask**). See Figure 20.



Figure 20. The Ethernet 1 (to Control Module) panel.

NOTICE

The R3 Communication Module must be configured for Ethernet IP wiring. See S&C Instruction Sheet 1045-570 for more information.

The **Enable Ethernet 1** option is set to **On** position by default, as indicated in Figure 20, and can be disabled by toggling the **Enable Ethernet 1** button from **On** position to the **Off** position. Disabling Ethernet 1 results in loss of connectivity to any device physically connected to Ethernet port 1.

The **Enable Ping** option allows the user to send an ICMP ping to any device physically connected to Ethernet 1. The **Enable Ping** button is in the **On** position on Ethernet 1 by default. To disable ping on Ethernet 1, click on the **Enable Ping** toggle button to set it to the **Off** position. When enabled, the toggle button will indicate green.

The **Static IP Address** and **Netmask** fields indicate the static IP address and netmask of the local area network interface. The R3 Communication Module ships with a default IP address of 192.168.1.1 and a netmask equal to 255.255.255.0.

Note: The static IP address for Ethernet 1 must match the default gateway address in the control in which it is installed, and that can be found in the IntelliLink® Setup Software on the *Setup>Communications>Ethernet* screen.

Ethernet 2 (WAN)

Ethernet 2 is the interface associated with the R3 Communication Module wide area network (WAN). See Figure 21. This section defines the IP addressing for the R3 Communication Module's Ethernet Port 2 and subsequent network linkage and settings respective to the customer's backhaul WAN network. Three toggle buttons are in the Ethernet 2 interface panel (**Enable Ethernet 2**, **Enable Ping**, and **DHCP Client**). Disabling Ethernet 2 results in loss of connectivity to any device physically connected to Ethernet port 2.

Enable Ethernet 2 is set to the **On** position by default, as indicated in Figure 21. It can be disabled by toggling the **Enable Ethernet 2** button from the **On** to **Off** position. When the **Enable Ethernet 2** button is set to the **Off** position, all remaining fields are disabled.

Note: This field is for WANs using Ethernet as a back-haul transport protocol. When serial back-haul networks are used or there is no WAN, this section will not require entries.



Figure 21. Enable Ethernet 2 set to “ON,” the default.

The **Enable Ping** setting on Ethernet 2 allows the user to send an ICMP ping to any device physically connected to Ethernet 2. The **Enable Ping** setting is in the **On** position on Ethernet 2 by default. To disable the **Ping** command on Ethernet 2, click on the **Enable Ping** toggle button to set it to the **Off** position. When enabled, the toggle button will indicate green.

DHCP Client “ON”

No IP address information is required to be configured by the user. The IP address, netmask, and default gateway IP address will be automatically assigned by DHCP server for devices attached to Ethernet port 2. See Figure 22.

DHCP Client “OFF”:

Three fields are required for this setting on Ethernet 2 when the **DHCP Client** setting is in the **Off** position: **Static IP Address**, **Default Gateway IP Address**, and **Netmask**.

- STEP 1.** In the **Static IP Address** field, enter the IP address for the Ethernet 2 port. The **Static IP Address** setpoint is the WAN IP address assigned to the R3 Communication Module.
- STEP 2.** Enter the netmask of the IP network.
- STEP 3.** Enter the Default Gateway IP address. The **Default Gateway IP Address** setpoint is the address of the network device physically connected to Ethernet 2.

The address entries are automatically verified to be sure they are compatible with the other values entered.

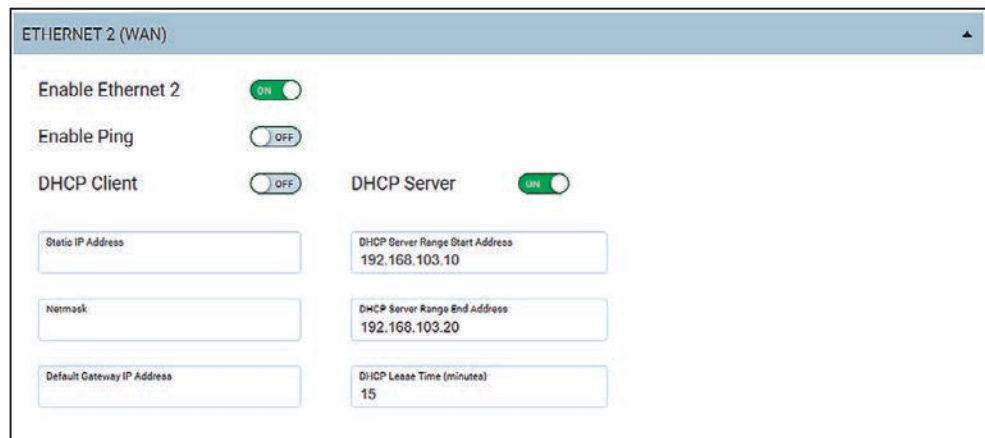


Figure 22. The *Interfaces* screen with the DHCP client disabled and the DHCP server enabled.

DHCP Server “ON”

When the DHCP client is disabled, the DHCP server can be enabled to a device connected to Ethernet port 2. This allows the R3 Communication Module to automatically provide an IP address, such as a filed area network radio. See Figure 22.

Wi-Fi

Wi-Fi Access Point

The Wi-Fi Access Point panel provides several configuration options to allow Wi-Fi-capable devices to communicate with the R3 Communication Module securely over a wireless network. In this manner, the network associated with the R3 Communication Module can be defined for devices connecting via the Wireless Local Area Network (WLAN). Seventeen settings are available: **Enable Wi-Fi Access Point**, **Enable Ping**, **Static IP Address**, **Netmask**, **DHCP Server Start IP Address**, **DHCP Server End IP Address**, **DHCP Lease Time**, **Broadcast SSID**, **Network Name (SSID)**, **Authentication Method**, **WPA2 Encryption**, **Wi-Fi Session Timeout**, **Wi-Fi to Ethernet 1 Routing**, **Mode**, **Channel**, **Width**, and **Transmit Power**. See Figure 23.

Figure 23. The Wi-Fi Access Point panel.

The **Enable Wi-Fi Access Point** setting is in the **On** position by default and is disabled by toggling the **Enable Wi-Fi Access Point** button from the **On** to **Off** position. Disabling the Wi-Fi access point will result in loss of wireless communications to the R3 Communication Module.

The **Enable Ping** setting is in the **On** position by default and is disabled by toggling the **Enable Ping** button from the **On** to **Off** position. Enabling ping allows the user to send an ICMP ping to any device physically connected to the R3 Communication Module on Ethernet 1 or Ethernet 2 (whichever physical devices have ping enabled when connected via Wi-Fi). When enabled, the toggle button will indicate green.

The **Static IP address** and **Netmask** fields indicate the static IP address and netmask of the local area Wi-Fi network interface. The R3 Communication Module ships with a default IP address of 192.168.101.1 and a netmask equal to 255.255.255.0.

The **DHCP Server Start IP Address** and **DHCP Server End IP Address** settings allocate a range of IP addresses to be assigned to devices communicating with the R3 Communication Module over the WLAN. The R3 Communication Module ships with a default DHCP Server Start IP address of 192.168.101.2 and a default DHCP Server End IP address of 192.168.101.10.

The **DHCP Lease Time** setting is used to assign the maximum amount of time (in minutes) a network device can use an IP address before it has to request a renewal to continue to use it. (Range: 1-30 minutes; Default:15 minutes)

The **Network Name (SSID)** setting is hard-coded with the serial number of the control it is connected to. This setting is read-only and cannot be changed here.

The **Broadcast SSID** setting shows the SSID associated with the R3 Communication Module. This setting is disabled in the **Off** position by default and enabled by toggling the **Broadcast SSID** button to “ON.” When enabled, the toggle button will indicate green and the SSID will be visible to all neighboring wireless devices.

The R3 Communication Module supports WPA2 encryption (AES 128-bit encryption) for Wi-Fi-protected access to a wireless network. When the default **WPA2-PSK Auto** setting is used, the encryption key is generated automatically. The user is not required to enter a passphrase for the R3 Communication Module to authenticate with the Wi-Fi module. The LinkStart application will auto-generate the same passphrase after the serial number is configured in the LinkStart application and a connection is attempted.

WPA2-PSK Manual Setting

A user can change the authentication method from the **WPA2-PSK Auto** setting by selecting the **WPA2-PSK Manual** setting from the list in the **Authentication Method** field drop-down menu. The **Authentication Method** field is displayed in the Wi-Fi Access Point panel on the *Interfaces* screen. When the **WPA2-PSK Manual** option is selected, an 8 to 16 character passphrase must be entered in the **WPA2 Passphrase** field. See Figure 24.



Figure 24. The Wi-Fi Access Point panel with the WPA2-PSK Manual authentication method.

If the **WPA2-PSK Manual** setting is used when connecting to the 6800 control, this WPA2-PSK passphrase must be entered when prompted by the Enter Passphrase dialog box on the LinkStart software *Wi-Fi Connection Management* screen. See Figure 25.

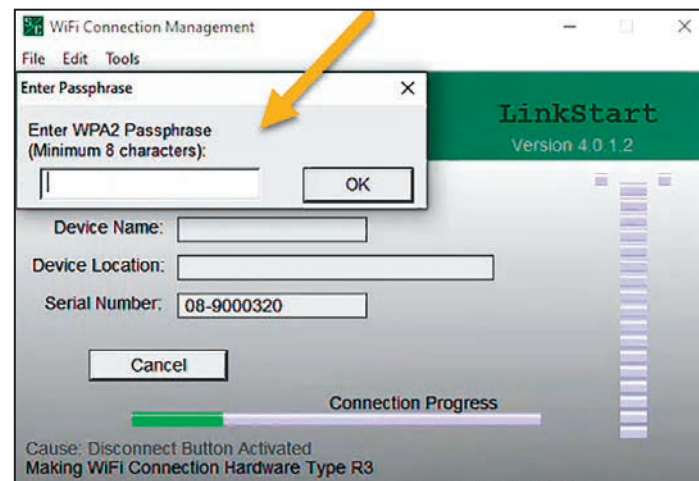


Figure 25. The Enter Passphrase dialog box.

The **Wi-Fi Session Timeout** setting determines the time the wireless session will automatically terminate because of inactivity. (Range: 1-60 minutes; Default: 15 minutes) When this timer expires, the R3 Communication Module will be disconnected from the wireless network, and manual restart of the session is required.

Wi-Fi to Ethernet 1 Routing

Note: This option is only available when using the R3 Communication Module with the IntelliRupter R3 Control Module.

The **Wi-Fi to Ethernet 1 Routing** setting allows a user to control whether Wi-Fi data are to be routed to the Ethernet 1 interface when the R3 Communication Module is wired to allow this. When enabled, which is the default, if the R3 Communication Module is wired to Ethernet Port 1, Wi-Fi data will be routed to the Ethernet 1 Port interface. When this setting is disabled, Wi-Fi data will only be routed through the serial interface and traffic will be blocked from being routed to the Ethernet Port 1 interface.

NOTICE
<p>The Ethernet 1 to Control Module setpoint must be set to the On position (default) when the Wi-Fi to Ethernet 1 Routing option is set to the On position. There may be a three-minute delay before changes to the Wi-Fi to Ethernet 1 Routing setpoint take effect. Any active IntelliLink Setup Software session should be terminated before making changes to the Wi-Fi to Ethernet 1 Routing setpoint.</p>

The **Mode** setting selects the preferred Wi-Fi transmission standard from the list of available options: **802.11b**, **802.11g**, and **802.11n**. (Default: 802.11n)

The **Channel** setting is the Wi-Fi channel over which the R3 Communication Module will communicate. There are 11 channel settings (Range: 1-11; Default 1). The **Channel** setting can be changed to reduce interference with other wireless signals.

The **Width** setpoint is the channel bandwidth in megahertz (MHz). This is presently a read-only setting, and only 20 MHz is used.

The **Transmit Power** setting adjusts the transmit power limit for the Wi-Fi Access Point signal. This setting reduces interference from neighboring devices by limiting the transmission distance of the broadcasted Wi-Fi signal. (Range: -15.0 dBm and 15.0 dBm; Default: 1.0 dBm)

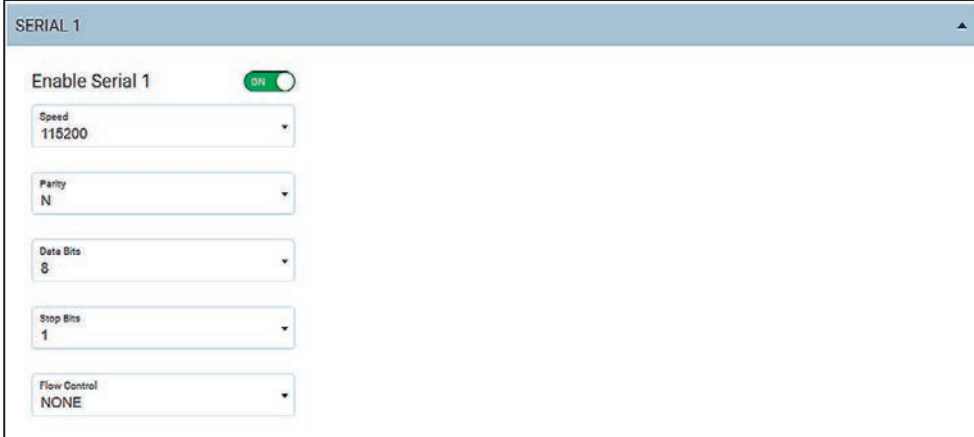
Serial 1 (DB9 Port)

This is the RS-232/DB9 port for connection to a radio serial console port. By default, the Serial 1 port is disabled. When enabled the following settings in Table 8 are displayed.

Table 8. The Serial 1 (DB9 Port) Settings

Setting	Default Value
Speed	115200
Parity	N
Data Bits	8
Stop Bits	1
Flow Control	None

If RTS/CTS is required, keep the **Flow Control** setpoint configured to “None.” See Figure 26.



The screenshot shows the SERIAL 1 configuration interface. At the top, there is a header 'SERIAL 1'. Below it, the 'Enable Serial 1' toggle is turned ON. The configuration options are as follows:

Parameter	Value
Speed	115200
Parity	N
Data Bits	8
Stop Bits	1
Flow Control	NONE

Figure 26. The Interfaces screen with Serial 1 enabled.

Port Numbers

This section displays three configurable port numbers the R3 Communication Module uses to receive packets via the Wi-Fi interface. See Figure 27.



The screenshot shows the WI-FI PORT NUMBERS configuration panel. It contains three input fields with their respective values and ranges:

Port Name	Value	Range
IntelliLink UDP Port	9797	Min - 1024, Max - 65,535
LinkStart Keepalive UDP Port	8829	Min - 1024, Max - 65,535
Radio Console TCP Port	8828	Min - 1024, Max - 65,535

Figure 27. The default Wi-Fi Port Numbers panel.

The **IntelliLink UDP Port** setting is used to receive local IntelliLink software packets from a device attached via Wi-Fi. (Range: 1024-65535; Default: 9797)

The **LinkStart Keepalive UDP Port** setting is used to provide connection information to the LinkStart desktop application on the user's device. (Range: 1024-65535; Default: 8829)

The **Radio Console TCP Port** setting is used to receive packets from a Wi-Fi device intended to be redirected to the serial console interface of a field area network radio device. These packets are directed through the R3 Communication Module's DB9 port to the radio device. (Range: 1024-65535; Default: 8828)

Note: To modify any of these port values, the same configuration settings in the LinkStart software must also be modified. In LinkStart, click on the **Tools** tab, and select the TCP/IP Port Options entry. Three similar settings must be set to the same values as the port numbers in the R3 Communication Module. In LinkStart, the **R3 IntelliLink UDP Port** setting corresponds to the communication module's **IntelliLink UDP Port** setting, the **R3 Keepalive UDP Port** setting corresponds to the LinkStart **Keepalive UDP Port** setting, and the **R3 VCOM TCP Port** setting corresponds to the **Radio Console TCP Port** setting. See Table 9.

Table 9. The Port Numbers

Input Name	Input Type	Input Restrictions	Minimum Input Length/Size	Maximum Input Length/Size
IntelliLink UDP Port	Non-Negative Integer	1024 through 65535	Four characters	Five characters
LinkStart Keepalive UDP Port	Non-Negative Integer	1024 through 65535	Four characters	Five characters
Radio Console TCP Port	Non-Negative Integer	1024 through 65535	Four characters	Five characters

Backup and Restore

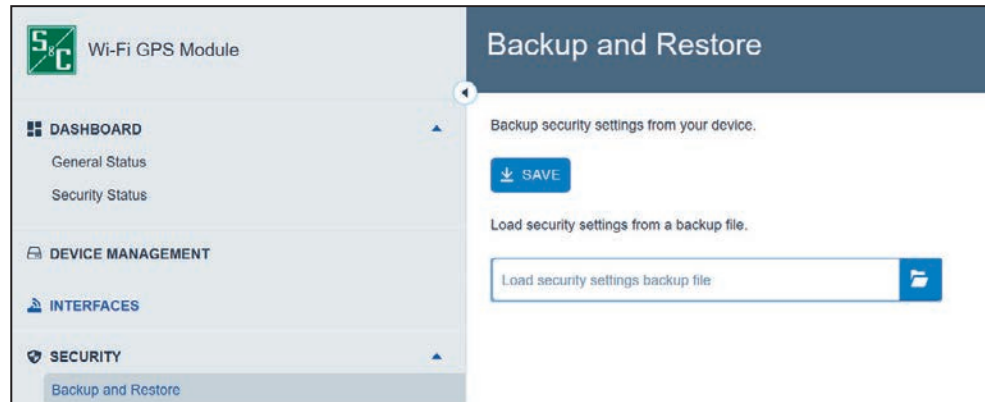


Figure 28. The Security>Backup and Restore screen.

The R3 Communication Module supports backup of security-related settings. The **Save** button writes the present security settings to a compressed file (.tgz file extension) for export to a local hard drive or external memory device. The **Load Security Settings Backup File** option imports data from a saved .tgz file into the R3 Communication Module. Clicking on the **Folder** icon invokes a series of dialog boxes allowing navigation on a PC to a saved settings file. See Figure 28.

User Accounts

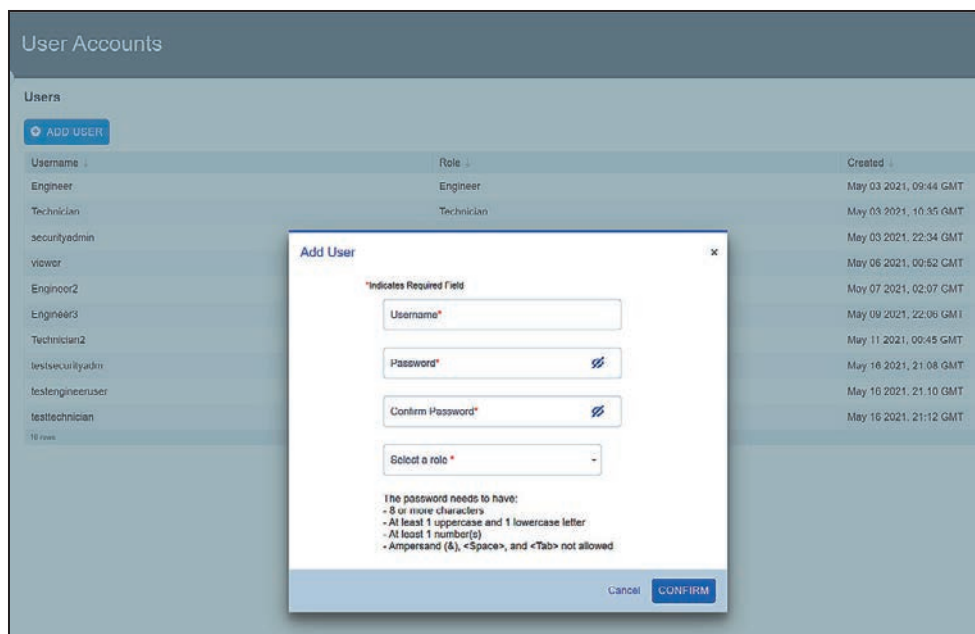


Figure 29. The Security>User Accounts screen.

The *User Accounts* screen permits adding a new user account to the R3 Communication Module. The addition of a user is initiated by clicking on the **Add User** button. A dialogue box appears with the required **Username**, **Password**, and **Confirm Password** fields, and a dropdown box to select the user **Role** setpoint. Clicking on a user entry in the list opens the dialog box to edit information for that user. See Figure 29. Table 10 on page 30 displays available default user roles. Only the admin user can define custom roles. See the “User Role Configuration” section on page 51 for information about creating custom roles.

Note: The default admin user is assigned the security administrator role, and it cannot be changed.

Configuration in the “Security” section is only for use by the admin user or any other user assigned the security administrator role.

Default user roles cannot be modified. To create a custom role, go to the *Advanced > User Role Configuration* screen. See the “User Role Configuration” section on page 51. The permissions provided to each of the default user roles is summarized in Table 10.

Table 10. User Role Permissions

Screen	Element Within Screen	Admin User	Security Admin	Engineer Role 2	Technician Role 3	Viewer Role 4
General Status	All	Read Only	Read Only	Read Only	Read Only	Read Only
Dashboard - Security	All	Read Only	Read Only	Read Only	Read Only	Read Only
Device Management	System Name	Allowed	Allowed	Allowed	Allowed	Read Only
	Firmware Upgrade	Allowed	Allowed	Allowed	Read Only	Read Only
	Settings (Config)	Allowed	Allowed	Allowed	Allowed	Read Only
	Reboot Device	Allowed	Allowed	Allowed	Allowed	Read Only
Interfaces	Ethernet 1	Allowed	Allowed	Allowed	Read Only	Read Only
	Ethernet 2	Allowed	Allowed	Allowed	Read Only	Read Only
	Wi-Fi	Allowed	Allowed	Allowed	Read Only	Read Only
	Serial 1	Allowed	Allowed	Allowed	Read Only	Read Only
	Port Numbers	Allowed	Allowed	Allowed	Read Only	Read Only
Security	Save and Load Settings	Allowed	Allowed	Read Only	Read Only	Read Only
	User Accounts	Allowed	Allowed	Read Only	Read Only	Read Only
	Certificate Management	Allowed	Allowed	Read Only	Read Only	Read Only
	VPN	Allowed	Allowed	Read Only	Read Only	Read Only
	Syslog	Allowed	Allowed	Read Only	Read Only	Read Only
	Remote Web Access	Allowed	Allowed	Read Only	Read Only	Read Only
Security - Advanced	Password Complexity	Allowed	Allowed	Read Only	Read Only	Read Only
	User Role Configuration	Allowed	Read Only	Read Only	Read Only	Read Only
	Firewall	Allowed	Allowed	Read Only	Read Only	Read Only
	Advanced Syslog	Allowed	Allowed	Read Only	Read Only	Read Only
Diagnostics	Diagnostic Log	Allowed	Allowed	Allowed	Allowed	Read Only
Support	Support Document	Read Only	Read Only	Read Only	Read Only	Read Only
Logout	--	Allowed	Allowed	Allowed	Allowed	Allowed
Profile	--	Allowed	Allowed	Allowed	Allowed	Allowed

Certificate Management

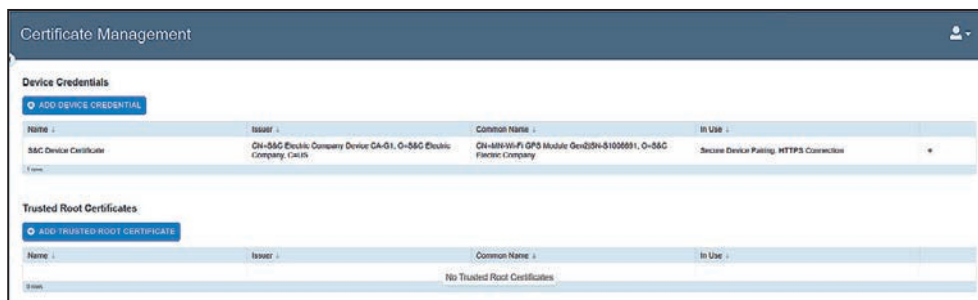


Figure 30. The Security>Certificate Management screen.

Digital X.509 certificates are managed using the *Certificate Management* screen. See Figure 30. S&C Electric Company preprograms default device credentials at the time of manufacture, and the credentials cannot be removed. These credentials are used by default for the HTTPS web interface. Users can override the S&C device certificate using their own Digital X.509 certificate with the **Add Device Credential** button:

STEP 1. Click on the **Add Device Credential** button. A dialog box will open. See Figure 31.

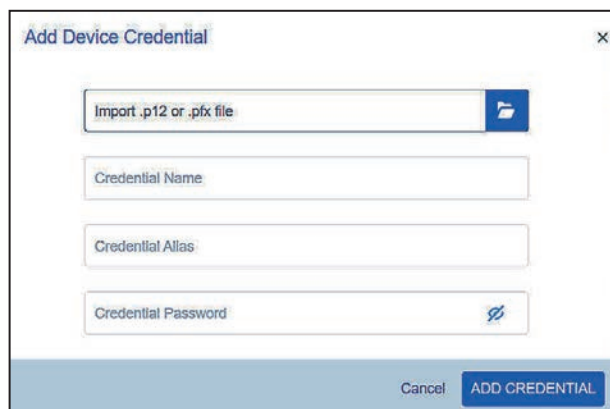


Figure 31. The Add Device Credential dialog box.

STEP 2. Browse and import the desired Digital X.509 certificate that will be used for device credentials (.p12 or .pfx file extension).

STEP 3. Assign a Credential Name, Credential Alias, and/or Credential Password entry before clicking on the **Add Credential** button.

Trusted root certificates can also be added to the device for use with Syslog and VPN tunnels. Users can add their own trusted root certificates with the **Add Trusted Root Certificate** button:

STEP 1. Click on the **Add Trusted Root Certificate** button. A dialog box will open. See Figure 32.

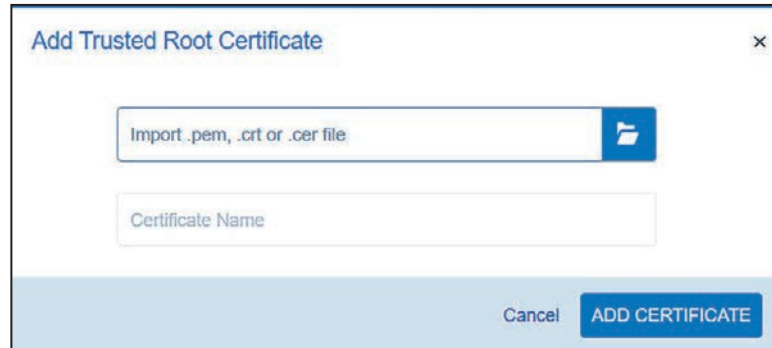


Figure 32. The Add Trusted Root Certificate dialog box.

STEP 2. Browse and import the desired trusted root certificate (.pem, .crt or .cer file extension).

STEP 3. Add a certificate name, and click on the **Add Certificate** button.

Web Access Configuration

Web Access Configuration

To access the user interface remotely through the field area network, set the **Remote Web Access** setpoint to the **On** position. See Figure 33.

Note: The **Remote Web Access** setpoint is not available until the default admin password is changed. Also, remote access requires the field area network to be routed through the Wi-Fi/GPS module.

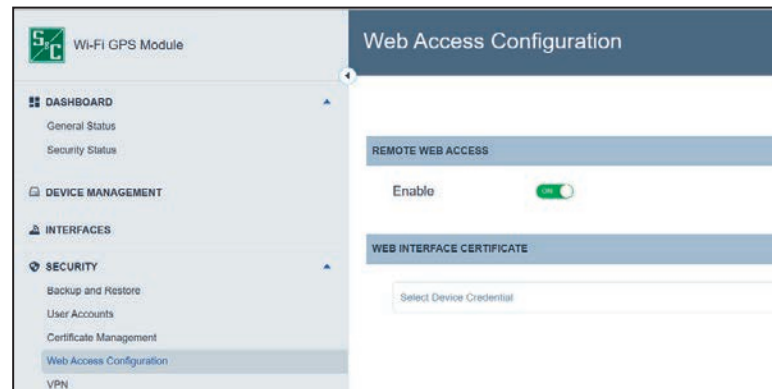


Figure 33. The Security>Web Access screen.

The **Remote Web Access** toggle button enables Web-user interface access via Ethernet Port 2. Only the admin user can update this configuration setting, after the admin user has changed the default password or by a user with the security admin role.

NOTICE

When a SpeedNet™ Radio is the field area network radio, the remote Web user's computer will require an additional setting to be updated to enable Web access. The user must reduce the maximum transmission unit (MTU) size to a value of 500 or less. S&C recommends using an MTU size of 500 for optimal performance. To change the MTU size, use the following command on a Windows 10 machine:
netsh interface ipv4 set subinterface "Local Area Connection" mtu=500 store=persistent.

Web Interface Certificate

The HTTPS interface requires a valid device certificate. By default, the default factory-loaded S&C Device Certificate is used. To change this, select the desired certificate using the **Select Device Credential** drop-down menu option. See Figure 34

Note: A message will be displayed in this dialog box if the device is missing a valid factory-loaded S&C Device Certificate.



Figure 34. The Web Interface Certificate dialog box.

A valid certificate is required to allow this R3 Communication Module to securely pair with an R3 Control Module and enable faster local IntelliLink software traffic. If the R3 Communication Module has a valid certificate, click on the **Download Device Certificate** button to retrieve and view the certificate details. If the R3 Communication Module does not have a valid certificate, call S&C's Global Support and Monitoring Center for additional instructions at 888-762-1100 or by contacting S&C through the S&C Customer Portal at sandc.com/en/support/sc-customer-portal/.

VPN

NOTICE

Cryptographically secured connections (i.e., Syslog and VPN) require time sync on the R3 Communication Module. More specifically, these operations require the system time to fall within the validity period of the certificates used for the connection. If the system time is not accurate or the validity period on the certificate used is not within the present system time, these connections will not become active.

The *VPN Configuration* screen provides options for configuration and setup of the Virtual Private Network (VPN). See Figure 35.

The screenshot shows the 'VPN Configuration' interface. At the top, there is a dropdown menu labeled 'Select VPN Type' with 'OpenVpn' selected. Below this, there are three columns: 'Active VPN', 'Server IP', and 'Server Port', each with a 'No data to display' message. A 'Split Tunneling' section contains an 'ADD SPLIT TUNNELING' button. At the bottom, there is a 'Network Segment' section, also with a 'No data to display' message.

Figure 35. The *Security>VPN Configuration* screen.

The R3 Communication Module supports three options for configuring a VPN tunnel. On the *VPN Configuration* screen, enter the **Select VPN Type** setting based on the list of allowable modes: **OpenVPN**, **L2TP/Ethernet IPsec**, or **L2TP/PPP IPsec**.

Note: Only one VPN configuration is allowed. Selecting a second VPN configuration will overwrite the active VPN configuration.

OpenVPN

When the **OpenVPN** mode is selected, the following screen will open. See Figure 36 on page 35.

Figure 36. The Security>OpenVPN Configuration screen.

The following fields are required to properly configure a VPN tunnel using the **OpenVPN** option: **Server IP**, **Server Port**, **Transport Protocol**, **Authentication Type**, **Cipher**, **Compression**, **IP Masquerading**, **Digest (HMAC)**, **TLS Auth Security**, **TLS Auth Key**, **Device Credential**, and **CA Certificate Name**.

Server IP—This is the IP address of the physical OpenVPN server and is a mandatory entry.

Server Port—This is the port number of the OpenVPN server.

Transport Protocol— This specifies the communication protocol used to transport data when the VPN is established. The available modes are **TCP** or **UDP**.

Note: When using **OpenVPN** mode over a communications network where the IP addresses are NAT'd, TCP is typically a better option to use because it reduces the keep alive traffic needed to keep the session established.

Authentication Type—This is the encryption key type used for the authentication between connecting peers. The private key/public key pair on each side of the connection must be the same authentication type. The modes are **RSA** and **ECC**.

Cipher—This is the symmetrical encryption algorithm used for traffic traversing the VPN tunnel after initial authentication is complete. There are four cipher modes to choose from: **AES-128-CBC**, **AES-256-CBC**, **AES-128-GCM**, and **AES-256-GCM** (recommended and the most secure option).

Compression—This reduces the size of IP packets, improving bandwidth utilization. When enabled, the speed of data traversing the OpenVPN tunnel is improved.

IP Masquerading—This allows the source IP addresses of traffic entering the VPN tunnel from the client device side to be either hidden or visible. In the **On** position, source IP addresses are hidden.

Digest Hash-based Message Authentication Code (HMAC)—This verifies the integrity and authenticity of data packets passing through the VPN. The cryptographic hash modes are **SHA256** or **SHA384** (recommended and the most secure option).

TLS Auth Security—This mode enables additional security between the VPN tunnel endpoints. This is an additional layer of security above the other encryption options specified and is optional. The available modes are **None**, **Auth**, and **Crypt**. Selecting **None** (default) disables the function. Selecting **Auth** adds an additional HMAC signature to all SSL/TLS handshake packets for integrity verification. Selecting **Crypt** (the most secure option) adds an additional layer of encryption and authentication for all data running within the TLS channel, so data are encrypted and authenticated twice.

TLS Auth Key—This field is enabled when the **TLS Auth Security** setting is enabled and the **Auth** mode is selected. The shared **Auth** key is then displayed in this field.

TLS Crypt Key—This field is enabled when the **TLS Auth Security** setting is enabled and the **Crypt** mode is selected. The shared **CRYPT** key is then displayed in this field.

Device Credential—This is the device-specific private/public key pair and certificate saved in the keystore intended for use with the connection. The certificate must be signed by the same certificate authority (CA) that signed the OpenVPN server-side certificates. The device certificate must be loaded into the *Certificate Management* screen before it can be selected. See the “Certificate Management” section on page 31 for additional information.

CA Certificate—This is the Certificate Authority certificate stored in the device keystore and used for the connection.

Configuring the OpenVPN Tunnel

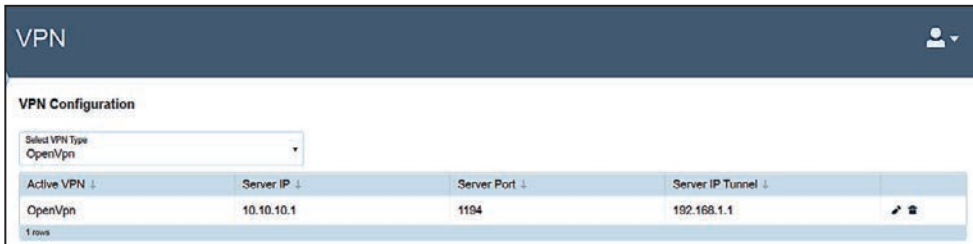
Note: A valid device or CA certificate must have been loaded to set up a VPN tunnel. If no device or CA certificate has been loaded into the device, go to the “Certificate Management” section on page 31 and load one of these into the device before proceeding with these steps.

Follow these steps to add an OpenVPN tunnel:

- STEP 1.** Enter the physical IP address of the OpenVPN server in the **Server IP** field.
- STEP 2.** Enter the OpenVPN server port number in the **Server Port** field.
- STEP 3.** Select either the **UDP** or **TCP** mode in the **Transport Protocol** field.
- STEP 4.** Select the desired AES cipher key value in the **Cipher** field. The **AES-256-GCM** mode is the most secure and recommended cipher key.
- STEP 5.** Set data compression by toggling the **Compression** button to the **On** position.
- STEP 6.** Hide or display the source IP address by toggling the **IP Masquerading** button. Hiding is recommended and more secure.
- STEP 7.** Select the desired entry in the **Digest (HMAC)** field. The recommended mode **SHA-384** is the most secure.

- STEP 8.** When additional security is needed, select either the **Auth** or **Crypt** mode in the **TLS Auth Security** field. The recommend setting is **Crypt**, the most secure. The **None** setting adds no additional security.
- STEP 9.** When the **Auth** or **Crypt** mode is selected for the **TLS Auth Security** setting, enter the TLS Auth or TLS Crypt key in the **TLS Auth Key/TLS Crypt Key** field.
- STEP 10.** Select the device credential from the drop-down list in the **Device Credential** field.
- STEP 11.** Select the associated Certificate Authority certificate in the **CA Certificate** field.
- STEP 12.** Click on the **Confirm** button to add the OpenVPN tunnel to the device.

The configured OpenVPN tunnel will be displayed in the **Active VPN** field. Tunnel deletions and modifications are managed by selecting buttons at the right on this screen. See Figure 37.



The screenshot shows the 'VPN Configuration' interface. At the top, there is a 'Selected VPN Type' dropdown menu set to 'OpenVpn'. Below this is a table with columns for 'Active VPN', 'Server IP', 'Server Port', and 'Server IP Tunnel'. A single row is visible with the values 'OpenVpn', '10.10.10.1', '1194', and '192.168.1.1'. To the right of the table, there are icons for edit and delete. At the bottom left of the table, it says '1 rows'.



Active VPN ↓	Server IP ↓	Server Port ↓	Server IP Tunnel ↓	
OpenVpn	10.10.10.1	1194	192.168.1.1	 

Figure 37. The *Active OpenVPN Tunnel Configuration* screen.

L2TP/Ethernet IPsec Configuration

When the **L2TP/Ethernet IPsec** mode is selected in the **Select VPN** field, the screen in Figure 38 opens.

The screenshot shows the 'L2TP/Ethernet IPsec Configuration' dialog box. It has a title bar with a close button. Below the title, there is a note: '*Indicates Required Field'. The 'IPSec' section includes:

- IPSec Phase1 Encryption *
- IPSec Phase1 Hash *
- IPSec Phase1 DH Group *
- IPSec Phase2 Hash *
- IPSec Phase2 Encryption *
- IPSec Authentication *
- IPSec Conf FQDN *
- IPSec Conf Server *
- IPSec PSK (with a key icon)
- Device Credential
- CA Certificate Name

 The 'L2TP Ethernet' section includes:

- Session ID * (0)
- Tunnel ID * (0)
- Peer Tunnel ID * (0)
- Peer Session ID * (0)
- Source Address *
- Destination Address *
- Source Port * (0)
- Destination Port * (0)
- Subnet Mask * (0)

 At the bottom right, there are 'Cancel' and 'Confirm' buttons.

Figure 38. The L2TP/Ethernet IPsec Configuration screen.

The following settings are required to properly configure the VPN tunnel in the L2TP/Ethernet IPsec configuration: **Phase1 Encryption, Phase 1 Hash, Phase 1 DH Group, Phase 2 Encryption, Phase 2 Hash, Server FQDN, Authentication Method, Pre-shared Key, Server IP, Device Credential, CA Certificate, Local Session ID, Local Tunnel ID, Peer Tunnel ID, Peer Session ID, Local IP Address, Peer IP Address, Local Port, Peer Port, and CIDR Subnet Mask.**

IPsec Phase1 Encryption—This sets a secure encrypted channel through which the two peers can negotiate Phase 2. The R3 Communication Module supports both **AES-128** and **AES-256** bit encryption modes. AES-256 is recommended and the most secure.

IPsec Phase1 Hash—This specifies the authentication algorithm for Phase 1. The **AES-256** mode is presently the only supported option.

IPsec Phase1 DH Group—This specifies the strength of the key used in the key exchange process. Within a group type (MODP or ECP), higher Diffie-Hellman (DH) groups are more secure.

Note: Both peers in the VPN exchange must use the same DH group. The R3 Communication Module supports these Diffie-Hellman groups:

MODP: Diffie-Hellman Group 5 (1536-bit), Diffie-Hellman Group 14 (2048-bit), Diffie-Hellman Group 15 (3072-bit)

ECP: Diffie-Hellman Group 19 (256-bit random), Diffie-Hellman Group 20 (384-bit random)

IPSec Phase 2 Encryption—This establishes the IPsec SA tunnel. The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN and how to encrypt and authenticate that traffic. The R3 Communication Module supports both **AES-128** and **AES-256** bit encryption modes. AES-256 is the most secure and recommended.

IPSec Phase 2 Hash—This specifies the authentication hash algorithm for Phase 2. The available modes are **SHA256**, **SHA384**, and **SHA512** (recommended and most secure).

IPSec Conf FQDN—This specifies the fully qualified domain name of the remote VPN server.

IPSec Authentication—This specifies the authentication method used when authenticating with the IPsec peer. **Pre-shared Key (PSK)** and **Keystore** modes are supported. For the **Pre-shared Key** mode, a pre-shared key is required in the **Pre-Shared Key** field. For **Keystore** mode, a device credential and CA certificate name are required, and the R3 Communication Module uses those for authentication purposes.

IPSec Pre-shared Key (PSK)—This specifies the pre-shared key used for authenticating with the VPN server. This field is only required when the **Pre-shared Key** mode is selected for the IPsec authentication method.

IPSec Conf Server—This specifies the IP address of the remote VPN server.

Device Credential—This is the device certificate saved in the keystore which is used for the VPN connection. The certificate needs to be signed by the same certificate authority (CA) that signed the server-side certificates.

CA Certificate Name—This is the CA certificate stored in the device keystore and used for the connection.

Session ID—This is the unique session number assigned to the device for the duration of the session.

Tunnel ID—This is the unique VPN tunnel identifier assigned to the device for the associated IPsec tunnel.

Peer Tunnel ID—This is the unique VPN tunnel identifier assigned to the peer device (point where the IPsec tunnel terminates) for the associated IPsec tunnel.

Peer Session ID—This is the unique session number assigned to the peer device for the duration of the session.

Source Address—This is the IP address of the physical interface associated with the device.

Destination Address—This is the IP address of the physical interface associated with the peer device (i.e. VPN server)

Source Port—This is the logical port used by the device for communications.

Destination Port—This is the logical port used by the peer device (i.e. VPN server) for communications.

Subnet Mask—This identifies the CIDR subnet mask used for both the source (R3 device side) and destination (peer side) devices on the network.

Configuring the L2TP/Ethernet IPsec Tunnel

Note: A valid device or CA certificate must have been loaded into the device to set up a VPN tunnel. If no device or CA certificate has been loaded into the device, go to the “Certificate Management” section on page 31 and load one into the device before proceeding with these steps.

NOTICE

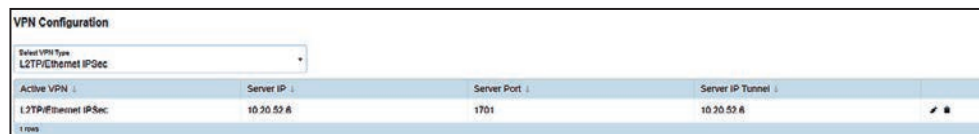
Ethernet 2 configuration will be affected. Configuring L2TP/Ethernet IPsec will bridge the Ethernet 2 and VPN interfaces. Split-tunneling will not be available in this configuration.

Follow these steps to add an L2TP/Ethernet IPsec tunnel:

- STEP 1.** Select the **Phase 1 Encryption** setting used to establish the IPsec tunnel. AES-256 is recommended and the most secure.
- STEP 2.** Select the **Phase 1 Hash** setting used to establish the IPsec tunnel.
- STEP 3.** Select the **Phase 1 DH Group** setting used to establish the IPsec tunnel. Group 20 is recommended and the most secure.
- STEP 4.** Select the **Phase 2 Encryption** setting used to establish the IPsec tunnel. AES-256 is recommended and the most secure.
- STEP 5.** Select the desired **Phase 2 Hash** setting used to establish the IPsec tunnel. SHA512 is recommended and the most secure.
- STEP 6.** Enter the **Config FDQN** setting (remote end-point), the fully qualified domain name.
- STEP 7.** Select the **IPsec Authentication** setting to be used. Keystore is the recommended and most secure. When Keystore is selected, skip to Step 9.
- STEP 8.** When the **PSK** mode is selected for the **IPsec Authentication** setting, enter the IPsec pre-shared key that will be used to authenticate the IPsec connection in the **IPsec PSK** field.
- STEP 9.** Enter the IP address of the remote IPsec server in the **IPsec Conf Server** field.
- STEP 10.** If Keystore was selected for the **IPsec Authentication** setting, select the device credential from the dropdown list in the **Device Credential** field.
- STEP 11.** If Keystore was selected for the **IPsec Authentication** setting, select the associated CA certificate in the **CA Certificate Name** field.
- STEP 12.** Enter the local L2TP session ID for the R3 Communication Module in the **Session ID** field.
- STEP 13.** Enter the local L2TP tunnel ID for the R3 Communication Module in the **Tunnel ID** field.

- STEP 14.** Enter the L2TP peer tunnel ID for the remote peer device in the **Peer Tunnel ID** field.
- STEP 15.** Enter the L2TP peer session ID for the remote peer device in the **Peer Session ID** field.
- STEP 16.** Enter the local IP address of the R3 Communication Module in the **Source Address** field.
- STEP 17.** Enter the remote peer device IP address in the **Destination Address** field.
- STEP 18.** Enter the local communications port number that will be used by the R3 Communication Module in the **Source Port** field.
- STEP 19.** Enter the remote peer device communications port number that will be used by the remote device in the **Destination Port** field.
- STEP 20.** Enter the CIDR subnet mask that will be used for both the local and remote L2TP networks in the **Subnet Mask** field.
- STEP 21.** Click on the **Confirm** button to add the L2TP/Ethernet IPsec tunnel to the device.

The configured L2TP/Ethernet IPsec tunnel will appear in the *Active VPN* screen. Tunnel deletions and modifications are managed by selecting buttons on the right on the *Active VPN* screen. See Figure 39.



The screenshot shows the 'VPN Configuration' interface. At the top, there is a dropdown menu for 'Select VPN Type' with 'L2TP/Ethernet IPsec' selected. Below this is a table with the following columns: 'Active VPN', 'Server IP', 'Server Port', and 'Server IP Tunnel'. The table contains one entry for 'L2TP/Ethernet IPsec' with the following values: Server IP: 10.20.52.6, Server Port: 1701, and Server IP Tunnel: 10.20.52.6. There are also some small icons on the right side of the table row.

Active VPN	Server IP	Server Port	Server IP Tunnel
L2TP/Ethernet IPsec	10.20.52.6	1701	10.20.52.6

Figure 39. The active L2TP/Ethernet IPsec tunnel configuration.

L2TP/PPP IPsec Overview

When the **L2TP/PPP IPsec** configuration setting is selected, the screen shown in Figure 40 on page 42 opens.

Figure 40. The L2TP/PPP IPsec Configuration screen.

The following settings are required to configure the VPN tunnel in the L2TP/PPP IPsec configuration: **Phase1 Encryption**, **Phase1 Hash**, **Phase1 DH Group**, **Phase2 Encryption**, **Phase2 Hash**, **Config FQDN**, **Authentication**, **Pre-shared Key (PSK)**, **Config Server**, **Device Credential**, **CA Certificate Name**, **LNS Address**, **LNS Subnet Local Address**, **LNS Subnet Mask**, **Port Number**, **Username**, and **Password**.

Phase1 Encryption—This sets up a secure encrypted channel through which the two peers can negotiate Phase 2. The R3 Communication Module supports both **AES-128** and **AES-256** bit encryption settings. AES-256 is recommend and the most secure.

Phase1 Hash—This specifies the authentication algorithm for Phase I. The S&C default is AES-256 and is presently the only supported option.

Phase1 DH Group—This specifies the strength of the key used in the key exchange process. Within a group type (**MODP** or **ECP**), higher Diffie-Hellman (DH) groups are more secure.

Note: Both peers in the VPN exchange must use the same DH group. The R3 Communication Module supports these DH groups:

MODP: Diffie-Hellman Group 5 (1536-bit), Diffie-Hellman Group 14 (2048-bit), and Diffie-Hellman Group 15 (3072-bit)

ECP: Diffie-Hellman Group 19 (256-bit random), and Diffie-Hellman Group 20 (384-bit random)

Phase2 Encryption—This is used to establish the IPsec SA tunnel. IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN and how to encrypt and authenticate that traffic. The R3 Communication Module supports both **AES-128** and **AES-256** bit encryption modes. AES-256 is recommended and the most secure.

Phase2 Hash—This specifies the authentication hash algorithm for Phase 2. The available modes are **SHA256**, **SHA384**, and **SHA512**, which is recommended and the most secure.

Conf FQDN—This is used to specify the fully qualified domain name of the remote VPN server.

IPsec Authentication—This specifies the authentication method to be used when authenticating with the IPsec peer. **Pre-shared Key (PSK)** and **Keystore** modes are supported. When **Pre-shared Key** mode is selected, a pre-shared key will be required in the **Pre-Shared Key** field. When **Keystore** mode is selected, a device credential and CA certificate name will be required. When Keystore is used, the R3 Communication Module uses the **Device Credential** and **CA Certificate Name** settings for authentication purposes.

IPsec PSK—This specifies the pre-shared key to be used for authenticating with the VPN server. This field is only required when **Pre-shared Key** mode is selected for the **Authentication** setting.

Config Server—This specifies the IP address of the remote VPN server.

Device Credential—This refers to the device certificate saved in the keystore used for the VPN connection. The certificate must be signed by the same certificate authority (CA) that signed the server-side certificates.

CA Certificate Name—This refers to the CA certificate used and is stored in the device keystore and used for the connection.

LNS Address—This specifies the remote peer LNS IP address.

LNS Subnet Local Address—This is the IP address of the physical interface associated with the device.

LNS Subnet Mask—This specifies the CIDR subnet mask for the remote peer network.

Port Number—This is the logical port used by the peer device for communication.

Configuring the L2TP/PPP IPsec Tunnel

Note: A valid device or CA certificate must have been previously loaded into the device to set up a VPN tunnel. If no device or CA certificate has been loaded, go to the “Certificate Management” section on page 31 and load one into the device before proceeding.

Follow these steps to add an L2TP/PPP IPsec tunnel:

- STEP 1.** Select the desired **Phase1 Encryption** setting to be used to establish the IPsec tunnel. **AES-256** mode is the most secure and recommended
- STEP 2.** Select the desired **Phase1 Hash** setting to be used to establish the IPsec tunnel.
- STEP 3.** Select the **Phase1 DH Group** setting to be used to establish the IPsec tunnel. **Group 20** mode is recommended and the most secure.

- STEP 4.** Select the **Phase2 Encryption** setting to be used to establish the IPsec tunnel. **AES-256** mode is recommended and is the most secure.
- STEP 5.** Select the desired **Phase2 Hash** setting to be used to establish the IPsec tunnel. **SHA512** mode is recommended and the most secure.
- STEP 6.** Enter the **Config FQDN** setting (remote end-point) fully qualified domain name.
- STEP 7.** Select the **IPsec Authentication** setting to use. **Keystore** mode is recommended and the most secure. If **Keystore** mode is selected, go to Step 9.
- STEP 8.** When **PSK** mode is selected for the **IPsec Authentication** setting, enter the IPsec pre-shared key to be used to authenticate the IPsec connection.
- STEP 9.** Enter the IP address of the remote IPsec server in the **Config Server** field.
- STEP 10.** When **Keystore** mode is selected for the **Authentication** setting, select the device credential from the dropdown list in the **Device Credential** field.
- STEP 11.** When **Keystore** mode is selected for the **Authentication** setting, select the associated CA certificate in the **CA Certificate Name** field.
- STEP 12.** Enter the LNS IP address in the **LNS Address** field.
- STEP 13.** Enter the local IP address for the R3 Communication Module in the **LNS Subnet Local IP Address** field.
- STEP 14.** Enter the peer CIDR subnet mask for the remote peer network in the **LNS Subnet Mask** field.
- STEP 15.** Enter the remote peer device communication port number to be used by the remote device in the **Port Number** field.
- STEP 16.** Enter the PPP username to be used to authenticate the PPP session in the **User Name** field.
- STEP 17.** Enter the PPP password to be used to authenticate the PPP session in the **Password** field.
- STEP 18.** Click on the **Confirm** button to add the L2TP/Ethernet IPsec tunnel to the device.

The configured L2TP/PPP IPsec tunnel will be displayed in the **Active VPN** field. Tunnel deletions and modifications are managed by selecting buttons on the right in this screen. See Figure 41.

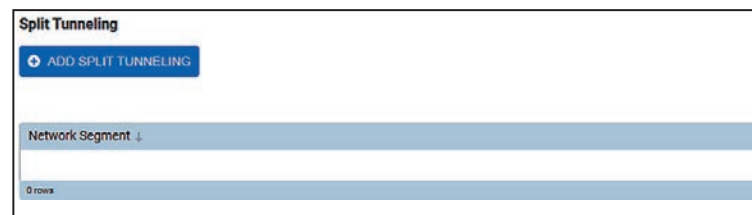


Figure 41. The *Split Tunneling* screen.

Split Tunnel Overview

Split tunneling can be used to separate data between the VPN tunnel and the non-encrypted default IP route. This allows important data to be sent to a remote secure end-point and less important data to be sent over a non-secure IP route. When using an **OpenVPN** or **L2TP/PPP IPsec VPN** mode, the split tunnel must be configured to route data through the VPN tunnel.

Note: The **L2TP/Ethernet IPsec** mode presently does not support **Split Tunnel** functionality. When **L2TP/Ethernet IPsec** mode is used, all traffic is routed through the VPN tunnel.

Split Tunnel Configuration

Follow these steps to enable the **Split Tunnel** feature to force traffic through a specified encrypted tunnel:

- STEP 1.** Click on the **Add Split Tunneling** button on the *VPN Configuration* screen. See Figure 36 on page 35. The Add Split Tunneling dialog box appears. See Figure 42.
- STEP 2.** In the **Server IP Segment/IP Address** field, select the source or destination address (Server IP segment/IP address) to be used to define the IP traffic routed through the VPN tunnel.

Figure 42. The Add Split Tunneling dialog box.

- STEP 3.** Click on the blue **Confirm** button to add the split tunnel. A dialogue box will appear to indicate successful execution. See Figure 43.
- STEP 4.** The **VPN Kill Switch** function defaults to **Off** mode when the **Split Tunnel** feature is configured.

Figure 43. The successful execution dialog box.

When the **VPN Kill Switch** function is enabled by toggling the **VPN Kill Switch** button to “ON,” if the VPN tunnel becomes unstable and loses connectivity to the VPN end-point, all traffic will be dropped that is destined for the VPN tunnel. No packets bound for the VPN tunnel will be forwarded until the VPN connection is re-established.

If the **VPN Kill Switch** function is desired, toggle the **VPN Kill Switch** button to the **On** position. See Figure 44.

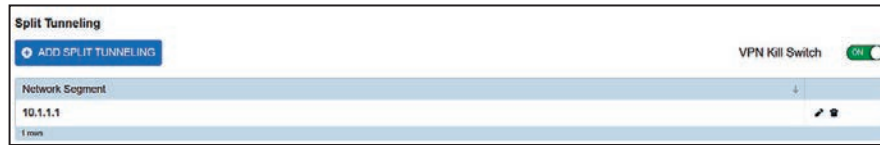


Figure 44. The VPN Kill Switch function in the On position.

Syslog

NOTICE

Cryptographically secured connections (i.e., Syslog and VPN) require time sync on the R3 Communication Module. More specifically, these operations require the system time to fall within the validity period of the certificates used for the connection. If the system time is not accurate or the validity period on the certificate used is not within the present system time, these connections will not become active.

The *Syslog Configuration* screen is used to configure the R3 Communication Module for remote logging of events. This feature allows the R3 module to record and send system log or event messages to a specified server and/or backup server. See Figure 45.

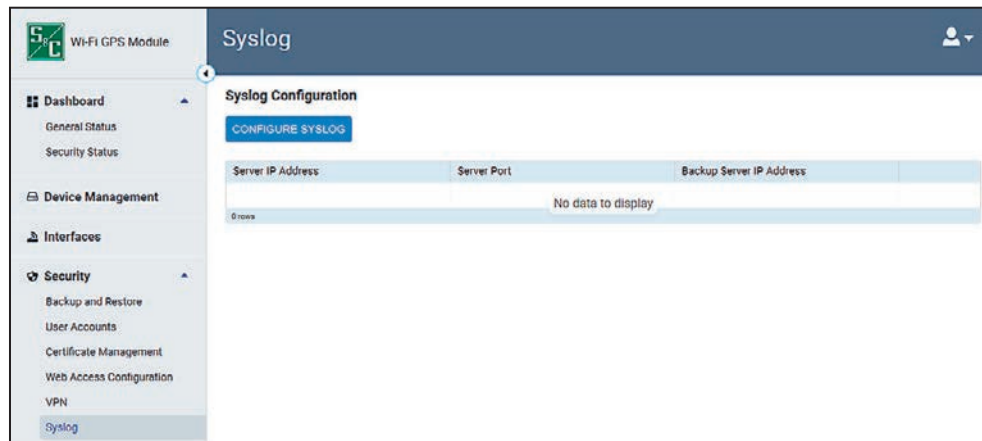


Figure 45. The Syslog Configuration screen.

Note: When this screen displays “No data to display,” the R3 Communication Module has not been configured for remote logging.

Follow these steps to configure the R3 Communication Module:

- STEP 1.** Click on the blue **Configure Syslog** button on the *Syslog Configuration* screen. See Figure 43 on page 45. The Configure Syslog dialog box appears. See Figure 46.

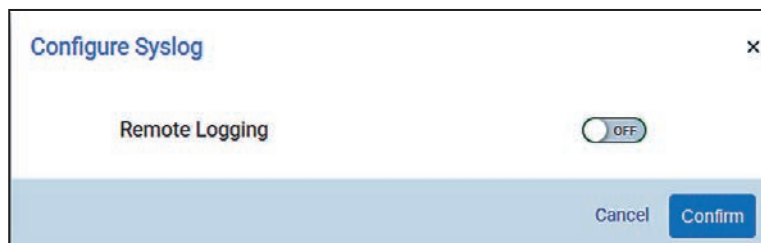


Figure 46. The Configure Syslog dialog box.

- STEP 2.** Toggle the **Remote Logging** button from the **Off** to **On** position.

- STEP 3.** Click on the blue **Confirm** button to enable the **Remote Logging** feature. The Configure Syslog dialog box appears. See Figure 47.

Note: Remote logging may be disabled by toggling the **Remote Logging** button from the **On** to **Off** position and clicking on the **Confirm** button.

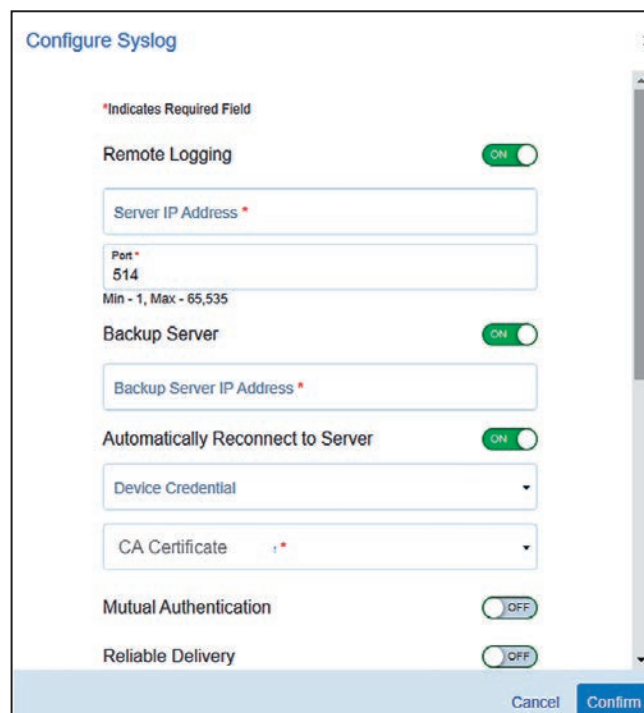


Figure 47. Upper section of the Configure Syslog dialog box.

To complete the setup process, enter data in the appropriate fields. The following fields are required: **Server IP Address**, **Port**, and **CA Certificate**:

- STEP 4.** Enter a valid address in the **Server IP Address** field. The Server IP address is the primary destination server and/or syslog server that will collect the logs.
- STEP 5.** Enter a number in the **Port** field. This is the logical port for sending and receiving logs to and from the syslog server. Syslog uses the TCP protocol on port 514 (recommended) but can be configured to use any port.
- STEP 6.** Select a valid CA Certificate entry. The CA Certificate must be signed from the certificate authority that also signed the device credentials used by the remote syslog server. See the “Certificate Management” section on page 31 for information about uploading the CA Certificate.
- STEP 7.** Proceed to Step 11 to select the event types and filters or proceed to Step 8 to select from the list of additional configuration options.
- STEP 8.** (Optional) To configure the R3 Communication Module to send syslog events to a backup server when the connection is lost to the primary server, toggle the **Backup Server** button from the **Off** to **On** position. Additional fields will be displayed. See Figure 48.

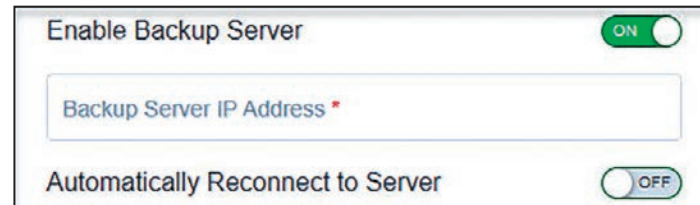


Figure 48. The Backup Server dialog box.

- (a) Enter a valid Backup Server IP Address entry for the backup server.

Note: The **Backup Server IP Address** field is required when using a backup server and it must be different from the **Primary Server IP Address** entry.

- (b) (Optional) To configure the device to automatically restart sending messages to the primary server when service to the primary server has been restored, toggle the **Automatically Reconnect to Server** button to the **On** position.

- STEP 9.** (Optional) To configure the device for mutual authentication, toggle the **Mutual Authentication** button to the **On** position.

Note: When the **Mutual Authentication** feature is enabled, the **Device Credential** field becomes a required field. Select a device credential from the drop-down list that was signed from the same Certificate Authority that signed the CA Certificate selected in Step 6 above. See Figure 49 on page 49.

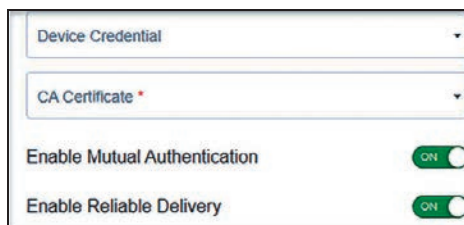


Figure 49. The Mutual Authentication and Reliable Delivery options.

With the **Mutual Authentication** feature enabled, the R3 Communication Module and the syslog server must share digital certificates to prove their identities before communication can be established.

STEP 10. (Optional) To configure the **Reliable Delivery** feature, toggle the **Reliable Delivery** button to the **On** position. Reliable delivery ensures logs that cannot be sent because of a lost connection get queued and eventually sent when the connection is re-established. See Figure 50.

STEP 11. Select from the list of available event types and filters. There are three event types: “Info,” “Warning,” and “Alert.” There are 11 event categories: “Device Management,” “VPN,” “Firmware Upgrade,” “Certificate Management,” “Firewall,” “User Accounts and Roles,” “Security Configuration,” “Syslog Diagnostics,” “User Session Management,” and “Control Link.” See Figure 50.

Note: At a minimum, “Info,” or “Warning,” or “Alert” must be selected along with one of the event categories. When nothing is selected, no log messages will be sent through syslog.

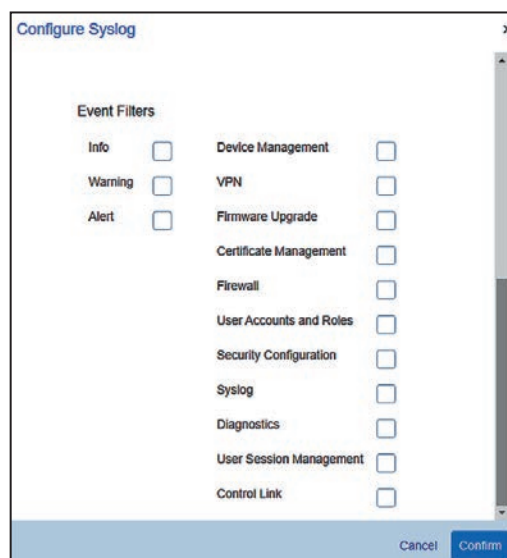
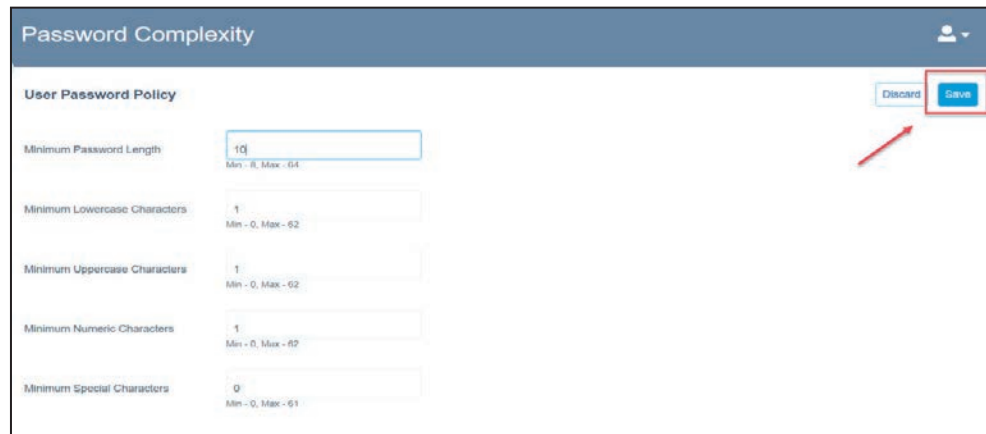


Figure 50. The Event Filters dialog box.

STEP 12. Click on the **Confirm** button to complete the setup process.

Password Complexity

The *Password Complexity* screen allows the administrator to specify policy rules for passwords and assign them to individual user roles. See Figure 51.



The screenshot shows the 'Password Complexity' configuration screen. The title bar is blue with the text 'Password Complexity' and a user icon. Below the title bar, the section is titled 'User Password Policy'. There are five input fields, each with a label and a value: 'Minimum Password Length' (10), 'Minimum Lowercase Characters' (1), 'Minimum Uppercase Characters' (1), 'Minimum Numeric Characters' (1), and 'Minimum Special Characters' (0). Each field has a range below it: 'Min - 8, Max - 64', 'Min - 0, Max - 62', 'Min - 0, Max - 62', 'Min - 0, Max - 62', and 'Min - 0, Max - 61' respectively. In the top right corner, there are two buttons: 'Discard' (grey) and 'Save' (blue). A red arrow points to the 'Save' button.

Figure 51. The *Security>Password Complexity* screen.

The R3 Communication Module is provisioned with a default set of password policy rules that applies globally to all users. Default complexity requirements for passwords are: minimum 8 characters in length, at least one uppercase character, one lowercase character, and one numeric character. A value of zero in any field will remove that item from the password complexity policy.

To establish a new password complexity policy, in the **User Password Policy** menu, enter the desired value for the associated entry field. The **Save** button will turn blue. Click on the **Save** button.

When the **Save** button is clicked and the new password complexity is saved, the device will reboot and the user will be re-directed to the *Login* screen.

Note: The password complexity policy changes will only affect new users. Existing user accounts need to be manually changed to meet the new password complexity requirements.

User Role Configuration

The R3 Communication Module allows the admin user to create custom user roles that can be assigned to new users. See Figure 52.



Figure 52. The *User Role Configuration User Roles* screen.

Up to five custom user roles can be configured along with the desired access controls. See Table 11 on page 53. To create a custom user role, click on the **Add Custom Role** button. Enter a role name and description. Choose between the available selections for access permissions: Allowed or Read-Only. See Figure 53 on page 52.

Note: Selecting the **Allowed** radio button enables read-write permissions for the newly created user role. On the *Device Management* screen, enter any combination of access permissions for the “Device Name,” “Device Upgrade,” “Device Configuration,” and “Device Reboot” sections. Repeat these steps for the Interface, Security, and Diagnostics panels before clicking on the **Save** button.

User Role Configuration 👤

Configure Custom User Role Discard Save

NAME	PERMISSION
DEVICE MANAGEMENT ▲	
Device Name	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Device Upgrade	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Device Configuration	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Device Reboot	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
INTERFACES ▲	
Ethernet 1	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Ethernet 2	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Wi-Fi Access Point	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Serial 1	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Wi-Fi Port Numbers	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
SECURITY ▲	
Backup and Restore	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Certificate Management	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Web Access Configuration	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
VPN	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Syslog	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
ADVANCED	
Password Complexity	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
Firewall	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only
DIAGNOSTICS ▲	
Diagnostics	<input type="radio"/> Allowed <input checked="" type="radio"/> Read-Only

Figure 53. The *User Role Configuration* screen.

Table 11. Advanced Editable User Interface Control Settings

Screen	Element Within Screen	(Name) Role 5	(Name) Role 6	(Name) Role 7	(Name) Role 8	(Name) Role 9
General Status	All	Read Only	Read Only	Read Only	Read Only	Read Only
Dashboard - Security	All	Read Only	Read Only	Read Only	Read Only	Read Only
Device Management	System Name	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Firmware Upgrade	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Settings (Config)	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Reboot Device	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
Interfaces	Ethernet 1	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Ethernet 2	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Wi-Fi Wi-Fi	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Serial 1	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Port Numbers	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
Security	Save and Load Settings	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	User Accounts	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Certificate Management	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	VPN	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Syslog	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Remote Web Access	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
Security - Advanced	Password Complexity	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	User Role Configuration	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Firewall	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
	Advanced Syslog	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO
Diagnostics	Diagnostic Log	Allowed/RO	Allowed/RO	Allowed/RO	Allowed/RO	Read Only
Support	Support Document	Read Only	Read Only	Read Only	Read Only	Read Only
Logout		Allowed	Allowed	Allowed	Allowed	Allowed
Profile		Allowed	Allowed	Allowed	Allowed	Allowed

Firewall

The *Firewall* screen displays the firewall rules presently active for the R3 Communication Module. See Figure 54.

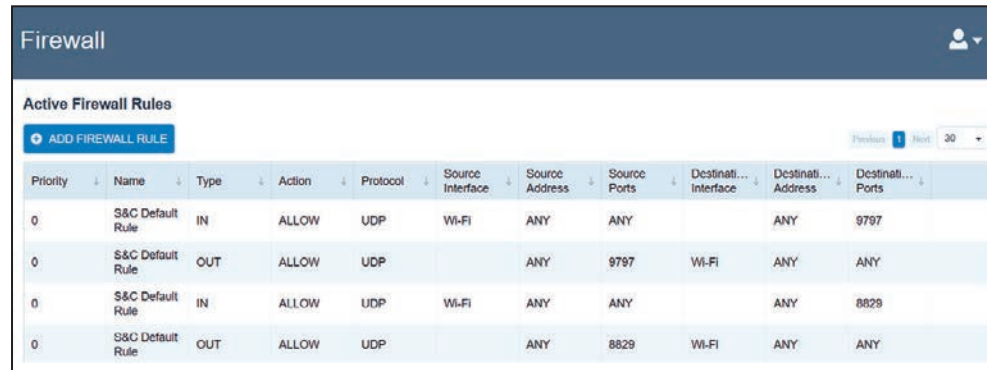


Figure 54. The Active Firewall Rules screen.

The admin user or a user with a security administrator role may create, edit, or delete additional firewall rules as needed to enhance device security. Three types of firewall rules can be added to the device: “In,” “Out,” and “Fwd.” These steps add new firewall rules when needed. See Table 12 for firewall policy creation validation.

Note: The R3 Communication Module has been configured with S&C default firewall rules. The S&C default rules have been assigned the highest priority to ensure device configuration, and operation and cannot be edited or removed.

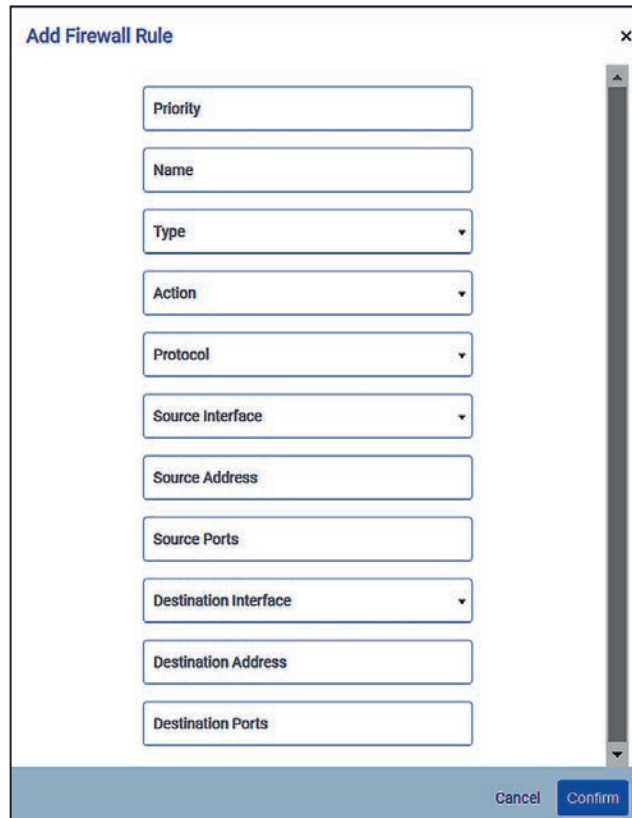
Table 12. Validation Table for Firewall Policy Creation

Input Name	Input Type	Input Restrictions	Minimum Input Length/Size	Maximum Input Length/Size
Priority	Non-Negative Integer	1 (highest) through 50 (lowest)	1 character	2 characters
Name	String	Allowed characters: <space>!\"#\$%&'()*+,-./0-9 :;?@ A-Z^_` a-z	1 character	64 characters
Type	Dropdown	IN, OUT, FWD	N/A	N/A
Action	Dropdown	ALLOW, DROP	--	--
Protocol	Dropdown	TCP, UDP, BOTH	--	--
Source Interface	Dropdown	Ethernet 1, Ethernet 2, Wi-Fi, All	N/A	N/A
Source IP Address	String	CIDR Format, Any	N/A	N/A
Source Ports	String	Non-Negative Integer, a pair of Non-Negative Integers joined by a colon, Any	1 character	11 characters
Destination Interface	Dropdown	Ethernet 1, Ethernet 2, Wi-Fi, Any	N/A	N/A
Destination IP Address	String	CIDR Format, Any	N/A	N/A
Destination Ports	String	Non-Negative Integer, a pair of Non-Negative Integers joined by a colon, Any	1 character	11 characters

Adding New Custom Firewall Rules

Follow these steps to add an IN (Inbound, data traffic coming into the device) firewall rule:

- STEP 1.** Click on the **Add Firewall Rule** button on the *Active Firewall Rules* screen. The Add Firewall Rule dialog box will appear. See Figure 55.



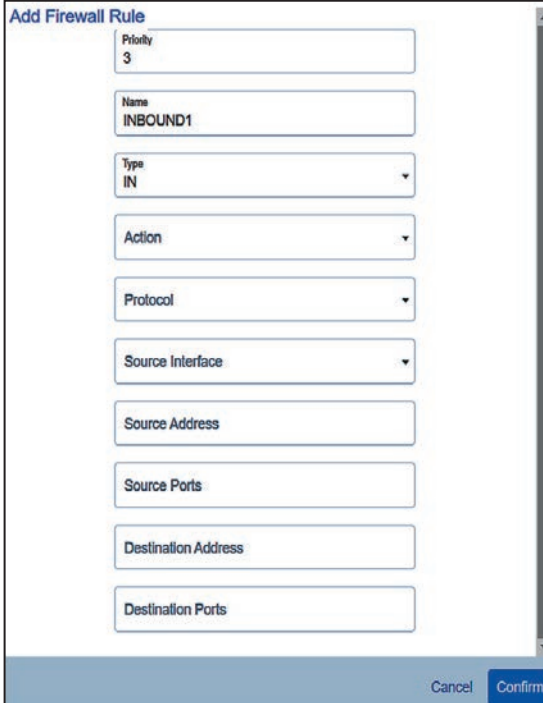
The screenshot shows a dialog box titled "Add Firewall Rule" with a close button (X) in the top right corner. The dialog contains the following fields from top to bottom:

- Priority (text input)
- Name (text input)
- Type (dropdown menu)
- Action (dropdown menu)
- Protocol (dropdown menu)
- Source Interface (dropdown menu)
- Source Address (text input)
- Source Ports (text input)
- Destination Interface (dropdown menu)
- Destination Address (text input)
- Destination Ports (text input)

At the bottom right of the dialog, there are two buttons: "Cancel" and "Confirm".

Figure 55. The Add Firewall Rule dialog box.

- STEP 2.** Enter a **Priority** value for the firewall rule. The firewall rule priority is an integer from 1 to 50, inclusive. Lower integers indicate higher priorities.
- Note:** If two rules have the same priority and conflict with one another, the one entered first will take precedence.
- STEP 3.** Enter a unique name for the firewall rule. The entry must have a minimum of one character and a maximum of 64 characters. Any combination of special characters can be used as shown in Table 12 on page 54.
- STEP 4.** In the **Type** field, select “IN” from the dropdown list. The In type is used for traffic coming into the device. The configuration area will then automatically be updated as shown in Figure 56 on page 56.



The screenshot shows a configuration window titled "Add Firewall Rule". The fields are as follows:

- Priority: 3
- Name: INBOUND1
- Type: IN (dropdown)
- Action: (dropdown)
- Protocol: (dropdown)
- Source Interface: (dropdown)
- Source Address: (text input)
- Source Ports: (text input)
- Destination Address: (text input)
- Destination Ports: (text input)

Buttons: Cancel, Confirm

Figure 56. The IN (Inbound) type firewall rule configuration.

- STEP 5.** In the **Action** field, make a selection from the dropdown list. This determines the action the firewall rule is intended to perform. The available selections are: “Allow” and “Drop.” The **Allow** option permits traffic of the specified type. The **Drop** option drops traffic for the specified type.
- STEP 6.** In the **Protocol** field, make a selection from the dropdown list. Choose the protocol for the firewall rule to assess the data against. The available selections are: “TCP,” “UDP,” or “Both.”
- STEP 7.** In the **Source Interface** field, make a selection from the dropdown list. This refers to the source interface on the R3 Communication Module to which the rule will be applied. The available selections are: “Ethernet 1,” “Ethernet 2,” “Wi-Fi,” and “All.”
- STEP 8.** In the **Source Address** field, enter a source IP address or enter “Any” to create a rule for any source IP address. This is the IP address where the data comes from.
- STEP 9.** In the **Source Ports** field, enter a valid source port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port the firewall rule is intended for.

Note: In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.

STEP 10. In the **Destination Address** field, enter a valid IP address or enter “Any” to create a rule for any destination IP address. This is the IP address where the data are sent.

STEP 11. In the **Destination Ports** field, enter a valid destination port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port for which the firewall rule is intended.

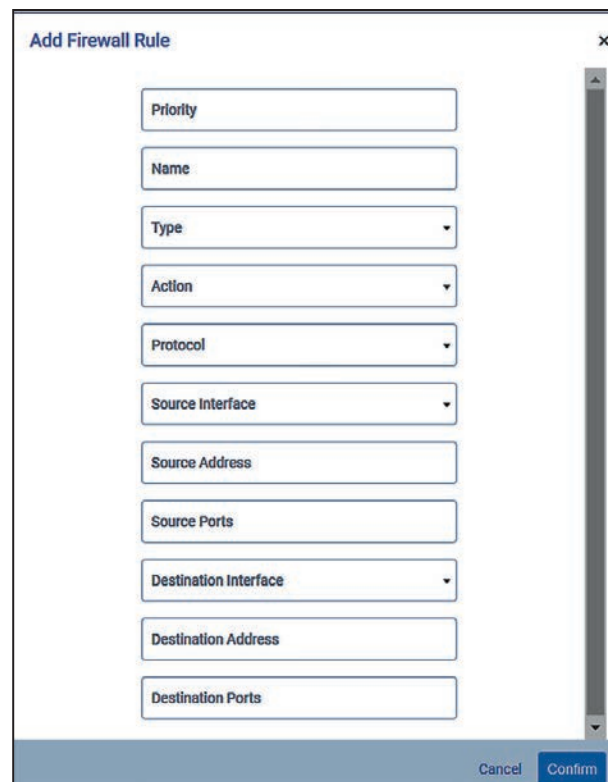
Note: In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.

STEP 12. Click on the **Confirm** button to save the new firewall rule.

Note: Custom firewall rules must be saved before changes will take effect. There may be a 10-second delay between clicking on the **Confirm** button and when the firewall rules are saved and active.

Follow these steps to add an OUT (Outbound, data out of the device) firewall rule:

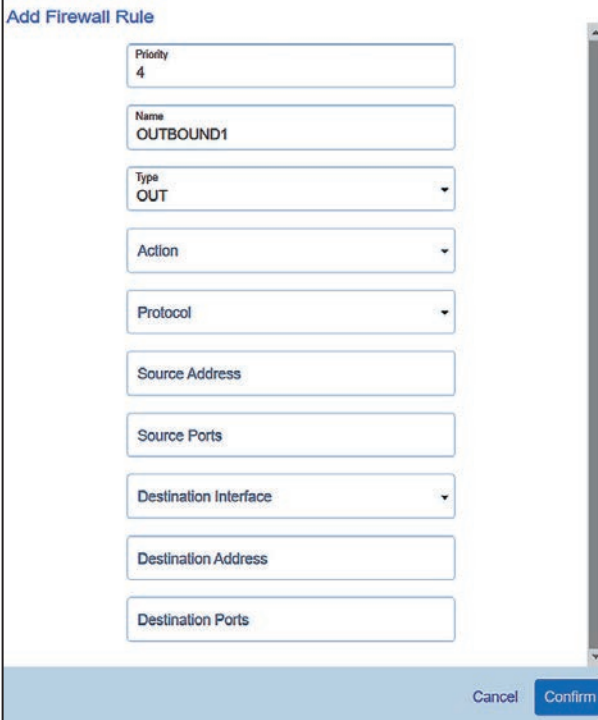
STEP 1. Click on the **Add Firewall Rule** button on the *Active Firewall Rules* screen. The Add Firewall Rule dialog box will appear. See Figure 57.



The image shows a screenshot of the 'Add Firewall Rule' dialog box. The dialog box has a title bar with 'Add Firewall Rule' and a close button (X). The main area contains the following fields from top to bottom: 'Priority' (text input), 'Name' (text input), 'Type' (dropdown menu), 'Action' (dropdown menu), 'Protocol' (dropdown menu), 'Source Interface' (dropdown menu), 'Source Address' (text input), 'Source Ports' (text input), 'Destination Interface' (dropdown menu), 'Destination Address' (text input), and 'Destination Ports' (text input). At the bottom right, there are two buttons: 'Cancel' and 'Confirm'.

Figure 57. The Add Firewall Rule dialog box.

- STEP 2.** Enter a **Priority** value for the firewall rule. The firewall rule priority is an integer from 1 to 50, inclusive. Lower integers indicate higher priorities.
Note: If two rules have the same priority and conflict with one another, the one entered first will take precedence.
- STEP 3.** Enter a unique name for the firewall rule. The entry must have a minimum of one character and a maximum of 64 characters. Any combination of special characters can be used as shown in Table 12 on page 54.
- STEP 4.** In the **Type** field, select the OUT entry from the dropdown list. The OUT type is used for traffic going out of the device. The configuration area will then automatically be updated as shown in Figure 58.



The screenshot shows a web-based configuration interface titled "Add Firewall Rule". The form contains the following fields and values:

- Priority:** 4
- Name:** OUTBOUND1
- Type:** OUT (selected from a dropdown menu)
- Action:** (empty dropdown menu)
- Protocol:** (empty dropdown menu)
- Source Address:** (empty text box)
- Source Ports:** (empty text box)
- Destination Interface:** (empty dropdown menu)
- Destination Address:** (empty text box)
- Destination Ports:** (empty text box)

At the bottom right of the form, there are two buttons: "Cancel" and "Confirm".

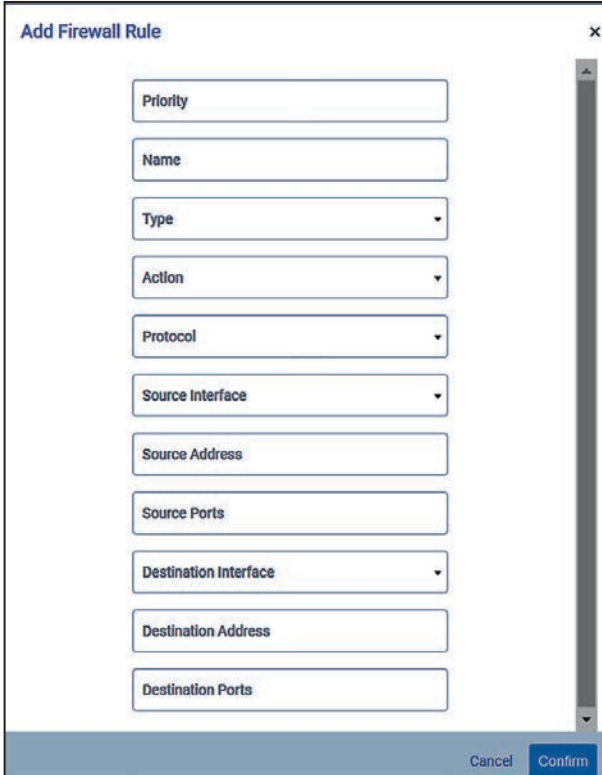
Figure 58. The OUT (Outbound) type firewall rule configuration.

- STEP 5.** In the **Action** field, make a selection from the dropdown list. This determines the action the firewall rule is intended to perform. The available selections are: "Allow" and "Drop." The **Allow** option permits traffic of the specified type. The **Drop** option drops traffic for the specified type.
- STEP 6.** In the **Protocol** field, make a selection from the dropdown list. Choose the protocol for the firewall rule to assess the data against. The available selections are: "TCP," "UDP," or "Both."

- STEP 7.** In the **Source Address** field, enter a source IP address or enter “Any” to create a rule for any source IP address. This is the IP address where the data comes from.
- STEP 8.** In the **Source Ports** field, enter a valid source port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port the firewall rule is intended for.
- Note:** In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.
- STEP 9.** In the **Destination Interface** field, make a selection from the dropdown list. This refers to the destination interface on the R3 Communication Module to which the rule will be applied. The available selections are: “Ethernet 1,” “Ethernet 2,” “Wi-Fi,” and “All.”
- STEP 10.** In the **Destination Address** field, enter a valid IP address or enter “Any” to create a rule for any destination IP address. This is the IP address where the data are sent.
- STEP 11.** In the **Destination Ports** field, enter a valid destination port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port for which the firewall rule is intended.
- Note:** In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.
- STEP 12.** Click on the **Confirm** button to save the new firewall rule.
- Note:** Custom firewall rules must be saved before changes will take effect. There may be a 10 second delay between clicking on the **Confirm** button and when the firewall rules are saved and active.

Follow these steps to add a FWD (Forward, traffic forwarded to another device) firewall rule:

- STEP 1.** Click on the **Add Firewall Rule** button on the *Active Firewall Rules* screen. The Add Firewall Rule dialog box will appear. See Figure 59.



The screenshot shows a dialog box titled "Add Firewall Rule" with a close button (X) in the top right corner. The dialog box contains the following fields and controls:

- Priority: Text input field
- Name: Text input field
- Type: Dropdown menu
- Action: Dropdown menu
- Protocol: Dropdown menu
- Source Interface: Dropdown menu
- Source Address: Text input field
- Source Ports: Text input field
- Destination Interface: Dropdown menu
- Destination Address: Text input field
- Destination Ports: Text input field

At the bottom right of the dialog box, there are two buttons: "Cancel" and "Confirm".

Figure 59. The Add Firewall Rule dialog box.

- STEP 2.** Enter a **Priority** value for the firewall rule. The firewall rule priority is an integer from 1 to 50, inclusive. Lower integers indicate higher priorities.

Note: If two rules have the same priority and conflict with one another, the one entered first will take precedence.

- STEP 3.** Enter a unique name for the firewall rule. The entry must have a minimum of one character and a maximum of 64 characters. Any combination of special characters can be used as shown in Table 12 on page 54.

- STEP 4.** In the **Type** field, select “FWD” from the dropdown list. The FWD type is used for traffic being forwarded by the device to another device. The configuration area will then automatically be updated, as shown in Figure 60 on page 61.

The screenshot shows a configuration window titled "Add Firewall Rule". It contains the following fields and values:

- Priority: 5
- Name: FORWARD1
- Type: FWD
- Action: (empty dropdown)
- Protocol: (empty dropdown)
- Source Interface: (empty dropdown)
- Source Address: (empty text box)
- Source Ports: (empty text box)
- Destination Interface: (empty dropdown)
- Destination Address: (empty text box)
- Destination Ports: (empty text box)

At the bottom right, there are "Cancel" and "Confirm" buttons.

Figure 60. The FWD (Forward) type firewall rule configuration.

- STEP 5.** In the **Action** field, make a selection from the dropdown list. This determines the action the firewall rule is intended to perform. The available selections are: “Allow” and “Drop.” The **Allow** option permits traffic of the specified type. The **Drop** option drops traffic for the specified type.
- STEP 6.** In the **Protocol** field, make a selection from the dropdown list. Choose the protocol for the firewall rule to assess the data against. The available selections are: “TCP,” “UDP,” or “Both.”
- STEP 7.** In the **Source Interface** field, make a selection from the dropdown list. This refers to the source interface on the R3 Communication Module to which the rule will be applied. The available selections are: “Ethernet 1,” “Ethernet 2,” “Wi-Fi,” and “All.”
- STEP 8.** In the **Source Address** field, enter a source IP address or enter “Any” to create a rule for any source IP address. This is the IP address where the data comes from.
- STEP 9.** In the **Source Ports** field, enter a valid source port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port the firewall rule is intended for.

Note: In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.

STEP 10. In the **Destination Interface** field, make a selection from the dropdown list. This refers to the destination interface on the R3 Communication Module to which the rule will be applied. The available selections are: “Ethernet 1,” “Ethernet 2,” “Wi-Fi,” and “All.”

STEP 11. In the **Destination Address** field, enter a valid IP address or enter “Any” to create a rule for any destination IP address. This is the IP address where the data are sent.

STEP 12. In the **Destination Ports** field, enter a valid destination port or a range of ports (that are adjoined by a colon, e.g., 4000:5000). This is the logical port for which the firewall rule is intended.

Note: In this field a non-negative integer is represented as a string. The “Any” entry in this field enforces the firewall rule for all inbound data traffic on any port.

STEP 13. Click on the **Confirm** button to save the new firewall rule.

Note: Custom firewall rules must be saved before changes will take effect. There may be a 10-second delay between clicking on the **Confirm** button and when the firewall rules are saved and active.

Editing or Deleting Firewall Rules

To edit or delete a new firewall rule, click on the **Edit** or **Delete** icon next to the rule. See Figure 61.

Priority	Name	Type	Action	Protocol	Source Interface	Source Address	Source Ports	Destination Interface	Destination Address	Destination Ports	
1	sdc1	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY	
2	test-sdc	IN	DROP	TCP	Ethernet 1	ANY	ANY		ANY	ANY	
2	test1-sdc	IN	ALLOW	UDP	Wi-Fi	ANY	ANY		ANY	ANY	
2	testfirewall10	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY	
2	check	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY	
1	testfirewall	IN	ALLOW	UDP	Ethernet 1	ANY	ANY		ANY	ANY	
5	testnew	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY	
3	ALLOW1	IN	ALLOW	BOTH	Ethernet 2	ANY	8080		ANY	8080	

Figure 61. The *Active Firewall Rules* screen.

Follow these steps to edit a firewall rule:

STEP 1. Click on the **Edit** (pencil) icon on the right of the firewall rule to be edited.

STEP 2. A dialog box appears to allow the rule to be edited. See Figure 62 on page 63. Make the edits and click on the **Confirm** button.

Figure 62. The Edit Firewall Rules dialog box.

STEP 3. The edited rule will be saved and a notification will be seen in the upper right corner. See Figure 63.

Note: There may be a 10-second delay between the time the **Confirm** button is clicked and when the firewall rules are saved and changes become active.

Priority	Name	Type	Action	Protocol	Source Interface	Source Address	Source Ports	Destination Interface	Destination Address	Destination Ports
1	s6c1	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY
2	test-s6c	IN	DROP	TCP	Ethernet 1	ANY	ANY		ANY	ANY
2	testfirewall10	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY
2	check	IN	ALLOW	TCP	Ethernet 1	ANY	ANY		ANY	ANY
1	testfirewall	IN	ALLOW	UDP	Ethernet 1	ANY	ANY		ANY	ANY
5	testinew	IN	ALLOW	TCP	Ethernet 1	192.123.191.231	ANY		192.123.191.231	ANY
3	ALLOW1	IN	ALLOW	BOTH	Ethernet 2	ANY	8081		ANY	8080

Figure 63. The successful update notification on the *Active Firewall Rules* screen.

Follow these steps to delete a firewall rule:

- STEP 1.** Click on the **Delete** (trash can) icon on the right of the firewall rule that will be edited. See Figure 60 on page 61.
- STEP 2.** A dialog box appears to allow the rule to be deleted. See Figure 64. To delete the firewall rule, click on the **Delete** button.

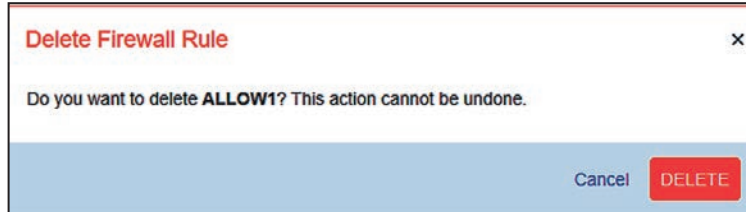


Figure 64. The Delete Firewall Rule dialog box.

- STEP 3.** After clicking on the **Delete** button, the rule will be deleted and a notification will be seen in the upper right corner. See Figure 65

Note: There may be a 10-second delay between the time the **Delete** button is clicked and when the firewall rules are deleted and changes become active.

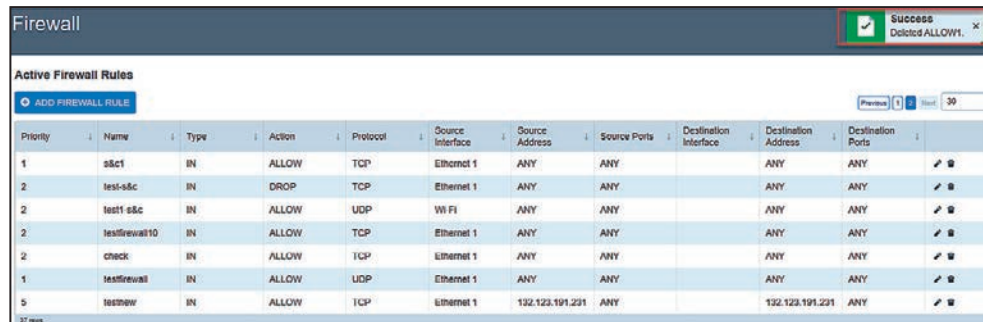


Figure 65. The successful deletion notification on the *Active Firewall Rules* screen.

Diagnostics

The *Diagnostics* screen initiates the retrieval of the Diagnostic and Security log files. See Figures 66 and 67.

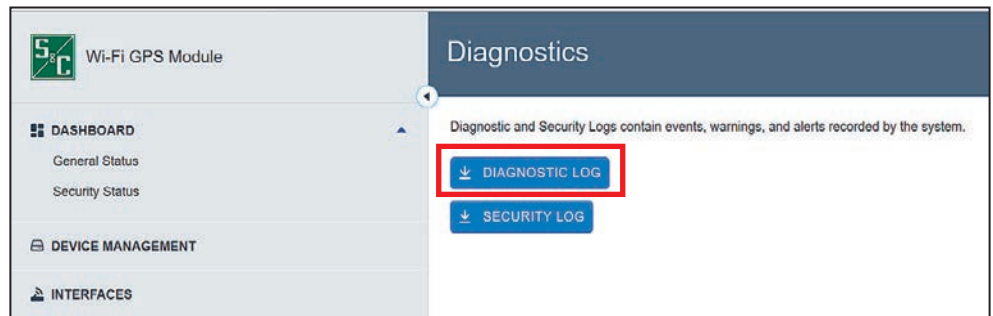


Figure 66. The retrieve full Diagnostics Log button on the *Diagnostics* screen.

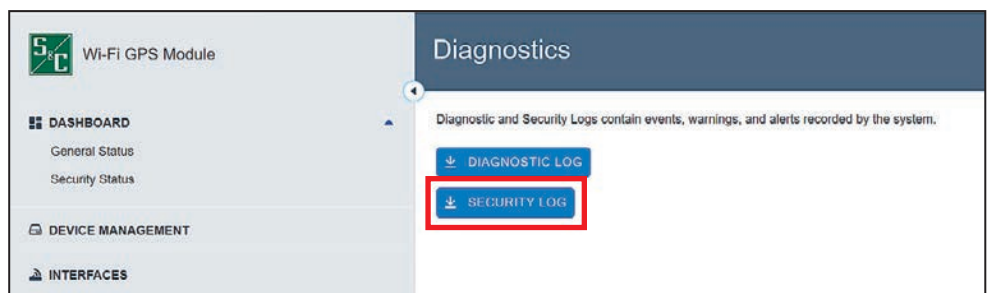


Figure 67. The retrieve Security Log button on the *Diagnostics* screen.