WTI Part No. 14527
Rev. D

AFS-16-1

RJ45 Fallback Switch

Configuration and SetUp

Power & Console Solutions I wti.com

Warnings and Cautions:
Installation Instructions

Secure Racking

If Secure Racked units are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered.

1. The ambient within the rack may be greater than room ambient. Installation should be such that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 60°C. Consideration should be given to the maximum rated ambient.
2. Installation should be such that a hazardous stability condition is not achieved due to uneven loading.

Input Supply

Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.

Grounding

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit.

No Serviceable Parts Inside; Authorized Service Personnel Only

Do not attempt to repair or service this device yourself. Internal components must be serviced by authorized personnel only.

- **Shock Hazard - Do Not Enter**
- **Lithium Battery**
  CAUTION: Danger of explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Two Power Supply Cables

Note that the AFS-16 features two separate power inputs, and a separate power supply cable for each power input. Make certain to disconnect both power supply cables from their power source before attempting to service or remove the unit.

Disconnect Power

If any of the following events are noted, immediately disconnect the unit from the outlet and contact qualified service personnel:

1. If the power cord becomes frayed or damaged.
2. If liquid has been spilled into the device or if the device has been exposed to rain or water.

Disconnect Power Before Servicing

Before attempting to service or remove this unit, please make certain to disconnect the power supply cable(s) from the power source(s).

Modem Cables

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.

ATTENTION: Pour réduire les risques d'incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérieure.

Agency Approvals

FCC Part 15 Regulation

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment

EMC and Safety Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

- **Council Directive 2014/30/EU of 26 February 2014 on the approximation of the laws of Member States relating to electromagnetic compatibility;**

  and

- **Council Directive 2014/35/EC of 26 February 2014 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits.**

Industry Canada - EMI Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

Table of Contents

1. Introduction 1-1

2. Getting Started 2-1
2.1. Apply Power to the AFS 2-1
2.2. Connect Your PC to the AFS 2-1
2.3. Communicating with the AFS. 2-2
2.4. Fallback Switching 2-3
2.4.1. Fallback Switching - Text Interface. 2-3
2.4.2. Fallback Switching - Web Browser Interface 2-4

3. The User Interface. 3-1
3.1. Connect Your PC or Laptop to the AFS 3-1
3.2. The Web Browser Interface 3-2
3.3. The Command Line Interface (CLI) 3-2
3.3.1. Enabling Web Access and Telnet Access 3-3
3.4. The WMU Enterprise Management Solution 3-4

4. Status Screens 4-1
4.1. Product Status (/J*) 4-1
4.2. The Network Status Screen (/SN) 4-1
4.3. The Circuit Status Screen (/S) 4-1
4.4. The Circuit Group Status Screen (/SG) 4-2
4.5. The Port Diagnostics Screen (/SD) 4-2
4.6. The Alarm Status Screen (/AS) 4-2
4.7. The Port Parameters Screens (/W). 4-3
4.8. The Log Status Screens (/L) 4-3
4.8.1. Audit Log 4-3
4.8.2. Alarm Log. 4-3
4.8.3. Syslog. 4-3
4.8.4. Temperature Log 4-3

5. Control Functions 5-1
5.1. A/B Switching - Web Browser Interface 5-1
5.1.1. The Circuit Control Screen - Web Browser Interface. 5-1
5.1.2. The Circuit Group Control Screen - Web Browser Interface 5-2
5.2. A/B Switching - Text Interface. 5-3
5.2.1. The Circuit Status Screen - Text Interface 5-3
5.2.2. A/B Switching Commands - Text Interface 5-3
5.2.2.1. Applying Commands to Several Circuits - Text Interface. 5-5
5.3. The SSH/Telnet Connect Function (Web Browser Interface Only) 5-6
5.3.1. Initiating an SSH Shell Session via the Web Browser Interface 5-6
5.3.2. Initiating a Telnet Session via the Web Browser Interface. 5-7
5.4. Manual Operation. 5-8
5.5. Logging Out of the User Interface 5-8

6. Configuration Options 6-1
6.1. General Parameters 6-2
6.1.1. System Parameters 6-3
6.1.2. Real Time Clock 6-4
6.1.3. Invalid Access Lockout 6-6
6.1.4. Callback Security 6-8
6.1.5. Scripting Options 6-9
6.1.5.1. Automated Mode 6-10
6.2. Serial Setup Port Configuration 6-11
6.2.1. Serial Port Modes 6-14
6.2.1.1. Normal Mode 6-14
6.2.1.2. Modem Mode 6-14
6.2.1.3. Modem PPP Mode 6-14
6.3. Network Configuration 6-15
6.3.1. Network Configuration [eth0] IPv4 Menu 6-16
6.3.1.1. Shared Network Parameters 6-16
6.3.1.2. Network Parameters [eth0] IPv4 6-19
6.3.1.3. DHCP Server [eth0] IPv4 6-20
6.3.1.4. IP Tables IPv4 6-21
6.3.1.5. Static Route [eth0] IPv4 6-21
6.3.1.6. DNS Selection [eth0] IPv4 6-21
6.3.1.6.1. DNS Servers (Shared) 6-21
6.3.1.6.2. DDNS Parameters [eth0] IPv4 6-21
6.3.1.7. Negotiation [eth0] IPv4/IPv6 6-22
6.3.1.8. Web Selection [eth0] IPv4/IPv6 6-22
6.3.1.8.1. Web Access [eth0] IPv4/IPv6 6-22
6.3.1.8.2. SSL Certificates [eth0] 6-23
6.3.1.8.3. Import Wildcard Certs [eth0] (SSL Certificate Import) 6-24
6.3.1.9. Syslog Parameters IPv4/IPv6 6-25
6.3.1.9.1. Syslog Client Parameters IPv4 6-25
6.3.1.9.2. Syslog Server Parameters IPv4 6-26
6.3.1.10. SNMP Parameters [eth0] IPv4 6-27
6.3.1.10.1. SNMP V3 Users [eth0 / IPv4) 6-28
6.3.1.11. SNMP Trap Parameters [IPv4] 6-29
6.3.1.12. LDAP Parameters (Shared) 6-30
6.3.1.12.1. Kerberos Parameters (Shared) 6-32
6.3.1.12.2. LDAP Group SetUp (Shared) 6-33
6.3.1.13. TACACS Parameters [Shared] 6-33
6.3.1.13.1. Default TACACS User Access (Shared) 6-35
6.3.1.14. RADIUS Parameters [Shared] 6-36
6.3.1.14.1. Default RADIUS User Access (Shared) 6-38
6.3.1.14.2. Dictionary Support for RADIUS 6-39
6.3.1.15. Ping Parameters (Ping Access) [eth0] IPv4 6-40
6.3.1.16. Email Messaging [IPv4] 6-41
6.3.2. Network Configuration [eth0] IPv6 Menus 6-42
6.3.2.1. Network Parameters [eth0] IPv6 6-42
6.3.2.2. IP Tables IPv6 6-43
6.3.2.3. Static Route [eth0] IPv6 6-43
6.3.2.4. DNS Selection Menu [eth0 / IPv6] 6-43
6.3.2.4.1. DNS Servers (Shared) 6-43
6.3.2.4.2. DDNS Parameters [eth0] IPv6 6-44
6.3.2.5. Negotiation [eth0] IPv4/IPv6 6-44

6. Configuration Options (continued)
6.3.2.6. Web Selection [eth0] IPv4/IPv6 6-45
6.3.2.6.1. Web Access [eth0] IPv4/IPv6 6-45
6.3.2.6.2. SSL Certificates [eth0] 6-46
6.3.2.6.3. Import Wildcard Certs [eth0] (SSL Certificate Import) 6-47
6.3.2.7. Syslog Parameters IPv6 6-47
6.3.2.8. SNMP Parameters [eth0] IPv6 6-48
6.3.2.8.1. SNMP V3 Users [eth0 / IPv6) 6-49
6.3.2.9. SNMP Trap Parameters [IPv6] 6-50
6.3.2.10. Ping Parameters (Ping Access) [eth0] IPv6 6-50
6.3.2.11. Email Messaging [IPv6] 6-51
6.4. User Configuration 6-52
6.4.1. Access Levels 6-52
6.4.2. Adding Accounts 6-53
6.4.3. Viewing User Accounts 6-55
6.4.4. Modifying User Accounts 6-55
6.4.5. Deleting User Accounts 6-55
6.5. VPN Options 6-56
6.5.1. IPsec (Client Site-to-Site) Options 6-56
6.5.2. OpenVPN (Client Site-to-Site) Options 6-57
6.5.3. IPSec Server (Client Site-to-Site) Options 6-58
6.6. The Circuit Group Directory 6-59
6.6.1. Adding Circuit Groups 6-59
6.6.2. Viewing Circuit Groups 6-59
6.6.3. Modifying Circuit Groups 6-59
6.6.4. Deleting Circuit Groups 6-59
6.7. Circuit Parameters 6-60
6.8. Ping No Answer Configuration 6-61
6.8.1. Adding Ping-No-Answer Triggers 6-61
6.8.1.1. Viewing Ping-No-Answer Profiles 6-63
6.8.1.2. Modifying Ping-No-Answer Profiles 6-63
6.8.1.3. Deleting Ping-No-Answer Profiles 6-63
6.9. Alarm Configuration 6-64
6.9.1. The Output Contacts 6-65
6.9.2. The Over Temperature Alarms 6-66
6.9.3. The Ping-No-Answer Alarm 6-68
6.9.3.1. Ping No Answer Alarm 6-68
6.9.4. The Serial Port Invalid Access Lockout Alarm 6-70
6.9.5. The Power Cycle Alarm 6-72
6.9.6. The Alarm Input Alarm 6-73
6.9.6.1. The Alarm Input Alarm - Circuits to Switch 6-74
6.9.6.2. Monitor Input Level Settings 6-75
6.9.6.2.1. Monitor Input Signal - Trigger When Low 6-76
6.9.6.2.2. Monitor Input Signal - Trigger When High 6-76
6.9.7. The No Dialtone Alarm 6-77
6.10. Telemetry Options 6-79
6.10.1. Continuous (Streaming Data) Telemetry Menu 6-79
6.10.2. Event Based (One Shot Data) Telemetry Menu 6-80
6.11. Download Unit Configuration 6-81
6.11.1. Restoring Saved Configuration Parameters 6-81
6.12. Firmware Upgrade 6-82
6.13. The Test Menu 6-82

7. Creating Web Certificates 7-1
7.1. Creating a Self Signed Certificate 7-2
7.2. Creating a Signed Certificate 7-3
7.3. Downloading the Server Private Key 9-5
7.4. Harden Web Security 9-5
7.5. TLS Mode 9-5

8. Saving and Restoring Configuration Parameters 8-1
8.1. Sending Parameters to a File 8-1
8.1.1. Downloading & Saving Parameters via CLI 8-1
8.1.2. Downloading & Saving Parameters via Web Browser Interface 8-2
8.2. Restoring Downloaded Parameters 8-3
8.3. Restoring Recently Saved Parameters 10-4

9. Upgrading Software 9-1
9.1. WMU Enterprise Management Software (Recommended) 9-1
9.2. The Firmware Upgrade Function (Web Browser Interface) 9-2
9.3. The Upgrade Software Function (Command Line Interface) 9-3

10. The Command Line Interface (Scripting) 10-1
10.1. Accessing the Command Line Interface (CLI) 10-1
10.2. Command Conventions 10-3
10.3. Command Summary 10-4
10.4. Command Set 10-5
10.4.1. Display Commands 10-5
10.4.2. Control Commands 10-8
10.4.3. Configuration Commands 10-12

Appendices:

A. Customer Service Apx-1

B. Automation Apx-2

C. Zero Touch Provisioning (ZTP) Apx-3

D. SSH & Telnet Functions Apx-4
D.1. Network Port Numbers Apx-4
D.2. SSH Encryption Apx-4

E. Syslog Messages Apx-5
E.1. Configuration Apx-5

F. SNMP Traps Apx-6
F.1. Alarm Notification via SNMP Traps Apx-6

G. Operation via SNMP Apx-7
G.1. AFS SNMP Agent Apx-7
G.2. SNMPv3 Authentication and Encryption Apx-7
G.3. Configuration via SNMP Apx-8
G.3.1. Viewing Users Apx-9
G.3.2. Adding Users Apx-9
G.3.3. Modifying Users Apx-9
G.3.4. Deleting Users Apx-9
G.4. Circuit Control via SNMP Apx-10
G.4.1. Controlling Circuits Apx-10
G.4.2. Controlling Circuit Groups Apx-11
G.5. Configuring Serial Ports Apx-12
G.6. Viewing Unit Status via SNMP Apx-13
G.6.1. System Status - Ethernet Port MAC Addresses Apx-13
G.6.2. Power Input Status Apx-13
G.6.3. Circuit Status Apx-13
G.6.4. Unit Temperature Status Apx-14
G.6.5. Serial Number Apx-14
G.6.6. Alarm Status Apx-14
G.7. Sending Traps via SNMP Apx-16

1. Introduction

The AFS-16-1 is a versatile switching system, designed for applications that require routing of analog or digital signals between a common RJ45 jack and “A” and “B RJ45 jacks. The AFS is ideal for switching RS232, RS422/485, Ethernet/UTP or telephone lines.

The system consists of a Card Rack, one Power Supply Module, one Control Module, and up to 16 Circuit Modules. Each Circuit Module is capable of switching all 8 pins of the Common RJ45 jack between Jack “A” or Jack “B”. Each card can be switched by alarm, manually, or by command.

The AFS includes an assortment of alarm features, which allow the unit to monitor temperature, power interruptions, and invalid access attempts and then notify you via Email, text message, Syslog message or SNMP trap when critical conditions are detected. The AFS can also monitor device response to ping commands and then switch A/B paths and provide notification when devices fail to respond.

WTI Management Utility

The WMU Enterprise Management Solution provides a centralized interface that can be used to configure, manage and control multiple WTI out-of-band management devices spread throughout a large corporate network infrastructure. When installed at your network operation center or support facility, the WMU eliminates the need to individually access WTI units in order to perform software updates, control power switching functions, edit user accounts and perform other management and control functions.

The WMU software and user’s guide can be downloaded at:

ftp://ftp.wti.com/pub/TechSupport/WMU/WTIManagementUtilityInstall.exe

Security and Co-Location Features:

Secure Shell (SSHv2) encryption and address-specific IP security masks help to prevent unauthorized access to command and configuration functions.

The AFS provides four levels of security for user accounts: Administrator, SuperUser, User and ViewOnly. The Administrator level provides complete access to all command functions, status displays and configuration menus. The SuperUser level allows control of switched circuits, but does not allow access to configuration functions. The User level allows access to only a select commands. The ViewOnly level allows you to check unit status, but does not allow access to command functions configuration menus. The AFS includes full RADIUS, LDAP, SNMP and TACACS capability, DHCP, an IP Tables menu and an invalid access lockout feature. An Audit Log records all user access, login and logout times and command actions, and an Alarm Log records user-defined alarm events.

Environmental Monitoring and Management:

The AFS can constantly monitor temperature levels, ping response and other factors. If the AFS detects that user defined thresholds for these values have been exceeded, the unit can promptly provide notification via email, SNMP Trap, or Syslog. When temperature readings exceed user-defined critical values, the AFS can also intelligently decrease the amount of heat being generated within the rack by temporarily shutting down nonessential devices; when readings return to acceptable levels, the AFS can restore power to devices to return to normal operating conditions. The AFS also record temperature readings to a convenient log file.

About this User's Guide

Due to the manner in which various web browsers deal with external links in PDF documents, links to external URLs in this document may not function properly depending on the web browser used. For best results, WTI recommends downloading and saving this User's Guide and then viewing the saved copy with Adobe Acrobat. In addition to providing more reliable access to external URLs, other document navigation features may also perform more reliably when viewed via Adobe Acrobat rather than your browser's native PDF viewer.

Typographic Conventions

^ (e.g. **^X**)	Indicates a control character. For example, the text "**^X**" (Control X) indicates the **[Ctrl]** key and the **[X]** key must be pressed simultaneously.
`COURIER FONT`	Indicates characters typed on the keyboard. For example, **`/RB`** or **`/ON 2`**.
[Bold Font]	Text set in bold face and enclosed in square brackets, indicates a specific key. For example, **[Enter]** or **[Esc]**.
`< >`	Indicates required keyboard entries: For Example: **`/P <n>`**.
`[ ]`	Indicates optional keyboard entries. For Example: **`/P [n]`**.

2. Getting Started

This section describes a simplified bench test procedure for the AFS, which will allow you to communicate with the unit in order to demonstrate basic features and check for proper operation. For a detailed description of configurations options and advanced operating features, please refer to the remainder of this User's Guide.

2.1. Apply Power to the AFS

First, check the safety precautions listed at the beginning of this User's Guide, and refer to the power rating label on the unit regarding power requirements and maximum load and then connect the AFS to an appropriate power source.

> **Note:** *The AFS includes two power inlets. You can connect either one or both of these inputs to your power source. If both power inlets are connected, they should be connected to separate power sources in order that the second power source can serve as a redundant back up in the event of failure.*

Connect the power supply cable(s) to the unit's power inlet(s) and then connect the cable(s) to appropriate power supplies.

Set the Power Switch on the AFS Power Module to the ON Position. The ON LED on the Power Module and the A/B indicators on the Control Module should light. After about 90 seconds, the A/B indicators should go out, indicating that the unit is ready to receive commands.

2.2. Connect Your PC to the AFS

The AFS can either be controlled by a local PC Serial Port, controlled via modem, or controlled via TCP/IP network. In order to select parameters or control switching functions, commands are issued to the AFS via either the Ethernet Port or RS232 Setup Port.

- **Ethernet Port:** Connect your 10Base-T or 100Base-T network interface to the AFS Control Module's 10/100Base-T Network Port.
- **RS232 Port:** Use the supplied Ethernet cable and adapter to connect your PC COM port to the RS232 Setup Port on the AFS Control Module.
- **Modem:** If desired, an external modem can also be installed at the RS232 Port.

> **Note:** *For cable recommendations and other information regarding the procedure for connecting network elements and other equipment to the AFS, please refer to Hardware Guide.*

2.3. Communicating with the AFS

Notes:

- *Default serial port parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this bench test procedure, it is recommended to configure your communications program to accept the default parameters.*
- *The AFS features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network IPv4 access to the Command Line Interface, providing that you are contacting the AFS from a node on the same subnet.*
- *When connecting only a single network cable to an AFS unit that includes two Ethernet ports, make certain to connect to Port eth0.*

1. **Access the User Interface:** Start your communications program and (e.g., Tera Term, Putty, etc.) then press **[Enter]**.

2. **Username** / **Password Prompt:** A message will be displayed, which prompts you to enter your username (Login) and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**". If a valid username and password are entered, the AFS will display either the Main Menu (Web Browser Interface) or the Port Status Screen (Text Interface.)

3. **Review Help Menu:** If you are communicating with the AFS via the text interface (SSH, Telnet or Modem), type **`/H`** and press **[Enter]** to display the Help Menu, which lists all available AFS commands. Note that the Help Menu is not available via the Web Browser Interface.

2.4. Fallback Switching

A/B fallback switching can be controlled via the Text Interface or Web Browser Interface.

2.4.1. Fallback Switching - Text Interface

Access the AFS Text Interface as described in Section 3.3 and then proceed as follows:

1. **Review the Help Menu:** At the Text Interface command prompt, type **`/H`** and press **[Enter]** to display the Help Menu, which provides a basic listing of all available AFS commands.

2. **Manual A/B Switching:** Use the manual circuit switches to change A/B paths. Note that this example assumes that the Master A/B Gang Switch and individual circuit module switches have not been disabled.

   a) **Master A/B Gang Switch:** Toggle the Master A/B Gang Switch between the "A" and "B" positions. The LED indicators should follow the Master Switch, indicating that each circuit has switched the "A" and "B" paths.

   b) **Circuit Module A/B Switch:** Choose an individual Circuit Module and toggle the module's A/B Switch between "A" and "B". The LED indicators should indicate that the module has switched the A/B path.

3. **Code Activated Switching:** To control A/B fallback switching using ASCII commands, invoke the following commands at the AFS command prompt:

   a) Type **`/T *,B`** and press **[Enter]**. All Circuit Modules should switch to the "B" path.

   b) Type **`/T 1,A`** and press **[Enter]**. Circuit Module number 1 should switch to the "A" path.

   c) Type **`/T 2,3,4,A`** and press **[Enter]**. Circuit Modules 2, 3, and 4 should switch to the "A" path.

2.4.2. Fallback Switching - Web Browser Interface

In the default state, the Web Browser Interface will not be available until you have enabled Web Access as described in Section 3.3.1. After Web Access has been enabled, access the AFS Web Browser Interface as described in Section 3.2 and then proceed as follows:

1. **Access the Circuit Control Menu:** Click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control menu. The Circuit Control menu includes a series of dropdown menus that are used to select the desired switching action for each Circuit Module.

   Note: *The Circuit Control menu also lists the number and user-defined name of each Circuit Module present, the name of the currently selected A/B circuit path, the A/B position of the switch, a brief description of the reason for the last switching action and a column that shows if each circuit is controlled by the Monitor/Alarm Input feature.*

2. **Select the Switching Action:** Use the dropdown menu to select an A/B switching operation for the desired Circuit Module. For example, to switch Circuit 1 to the B position, click on the down arrow in the "Action" column for Circuit 1 to display the dropdown menu, select the "B" option from the dropdown menu and then click on the "Confirm Circuit Actions" button.

   Notes:

   - *The dropdown menu for each circuit allows you to select position A, position B or the default position. Normally, the "Default" option will switch the circuit to the user-defined Default position that is selected as described in Section 5.. However, in the case of this Quick Start procedure, the Default circuit positions have not yet been defined.*
   - *The Circuit Control Menu also includes the ability to switch all AFS Circuit Modules. If desired, the dropdown menu in the "All Circuits" row can be used to switch all AFS circuits.*

3. **Confirm Switching Actions:** After you click on the "Confirm Circuit Actions" button, the AFS will display a screen which summarizes the selected switching operation(s) and asks for confirmation before executing the command. To proceed with the selected switching operation, click on the "Execute Circuit Actions" button.

4. The AFS will execute the switching operation and then display the Circuit Status screen.

Prior to placing the unit into operation, it is recommended to refer to the remainder of this user's guide for important information regarding advanced configuration options and more detailed operation instructions. If you have further questions regarding the AFS unit, please contact WTI Customer Support as described in Appendix A.

3. The User Interface

The AFS offer two separate user interfaces; the Web Browser Interface and the Command Line Interface (or CLI.) Although both of these interfaces offer access to more-or-less the same set of control and configuration functions, users often choose their preferred interface based on the nature of their specific application:

- **Web Browser Interface:** Command and configuration functions are selected and defined using a Web based menuing system. The Web Browser Interface is often preferred by users that require operator initiated control of a limited number of devices.
- **Command Line Interface (CLI):** Command and configuration functions are initiated using simple, ASCII text commands. The CLI is often chosen by users who need control a large number of devices. The principal advantage of the CLI is that it allows users to employ custom scrips, which are often issued by an enterprise management program in order to control multiple AFS units automatically.

  Note: *AFS units can also be controlled and managed via the included WMU Enterprise Management Software. For more information on the WMU Enterprise Management Software, please refer to Section 3.4.*

3.1. Connect Your PC or Laptop to the AFS

In the default state, communication with the AFS via Telnet, HTTP and HTTPS are disabled. When connecting your PC or Laptop to the AFS for the first time, you will need to access the Command Line Interface (CLI) via either the Mini USB Port (CPM and DSM Series Units Only), the Serial SetUp Port or the Network Port.

- **Mini USB Port:** (DSM and CPM Series units only.) Use a standard USB-to-Mini-USB Cable. In the default state, the Mini USB Port is configured for 9600 bps.
- **Serial SetUp Port:** Use the Ethernet Cable and Adapter supplied with the AFS. In the default state, the Serial SetUp Port is configured for 9600 bps.
- **Network Port:** Use the Ethernet Cable supplied with the unit. The default IPv4 address for the Network Port is 192.168.168.168.

Notes:

- *If your AFS includes dual Ethernet Ports and you only intend to connect to one of the two available Network Ports, connect to eth0*
- *For cable recommendations and other information regarding the procedure for connecting network elements and other equipment to the AFS, please refer to WTI Hardware Guide for your product.*

3.2. The Web Browser Interface

The Web Browser Interface consists of a series of web forms, which can be used to select configuration parameters and manage switch circuits.

Notes:

- *When communicating with the AFS for the first time, you will not be able to contact the unit via HTTP or HTTPS until you have accessed the CLI via the Serial SetUp Port using an SSH Client, and enabled HTTP and/or HTTPS via the Network Parameters Menu as described in Section 3.3.1.*
- *The AFS features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network IPv4 access to the Command Line Interface, providing that you are contacting the AFS from a node on the same subnet.*

After HTTP and/or HTTPS have been enabled as described in Section 3.3.1, proceed as follows to access the Web Browser Interface:

1. Start your Web Browser, key the AFS's default IPv4 format address (192.168.168.168) into the web browser's address bar, and press **[Enter]**.
2. **Username** / **Password Prompt:** A message box will prompt you to enter your username and password. The default username is **`super`** (all lower case), and the default password is also **`super`**.

3.3. The Command Line Interface (CLI)

The Command Line Interface consists of a series of text menus, which allow you to set options and parameters using simple text commands. The CLI is particularly useful for applications that require control by scripting.

Note: *When communicating with the AFS for the first time, you will not be able to contact the unit via Telnet until you have accessed the CLI via the Serial SetUp Port using an SSH Client, and enabled Telnet via the Network Parameters Menu as described in Section 3.3.1.*

To access the CLI, proceed as follows:

Note: *Default serial port parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this bench test procedure, it is recommended to configure your communications program to accept the default parameters.*

1. **Access the User Interface:** Start your communications program and (e.g., Tera Term, Putty, etc.) then press **[Enter]**. Note that when viewed by a PC running Windows XP or later, the Serial COM Port menu will list the USB Mini Port as, "USB to Serial."
2. **Username** / **Password Prompt:** A message will be displayed, which prompts you to enter your username (Login) and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**". If a valid username and password are entered, the AFS will display the Status Screen.

3.3.1. Enabling Web Access and Telnet Access

Once you have accessed the AFS's CLI, you can enable HTTP, HTTPS and/or Telnet as follows:

1. **Enable Telnet Access:**

   a) Type **/N** and press **[Enter]** to display the Network Parameters menu for eth0 IPv4.

   b) When the Network Parameters menu appears, key in the number for the Telnet Access option and press **[Enter]** to display the Telnet Access submenu.

   c) From the Telnet Access submenu, key in the number for Enable and use the resulting submenu to enable Telnet Access.

2. **Enable HTTP and/or HTTPS Access:**

   a) Type **/N** and press **[Enter]** to display the Network Parameters menu for eth0 IPv4.

   b) When the Network Parameters menu appears, key in the number for the Web Access option and press **[Enter]** to display the Web Access submenu.

   c) **HTTP Access:** From the Web Access submenu, key in the number for HTTP Enable, and use the resulting submenu to enable HTTP Access.

   d) **HTTPS Access:** From the Web Access submenu, key in the number for HTTPS Enable, and use the resulting submenu to enable HTTPS Access.

Once access is enabled, you will then be able to use the CLI to communicate with the AFS via Serial Setup Port, Web, SSH, or Telnet connection. You can also access the CLI via Dial-up Modem or Cellular Modem, providing that those options are present.

- **Access via Network:** The AFS must be connected to your TCP/IP Network, and your PC must include a communications program (such as TeraTerm or PuTTy.)
- **Access via Dial-Up Modem:** A phone line must be connected to the internal modem (if present.) In addition, your PC must include a communications program.
- **Access via Cellular Modem:** AFSs that include the Cellular Modem Option allow cellular access to the user interface. For more information, please refer to Section 7.4 and Section 8 in this User's Guide, plus the WTI Hardware Guide for your product.
- **Access via Local PC:** Your PC must be connected to the AFS's Serial SetUp Port, the SetUp Port must be configured for Any-to-Any Mode, (default port Mode for the SetUp Port.) Your PC must include a communications program. Serial Port 1 is designated as a Set Up Port, and by default, is configured for communication with a local control device. DSM, CPM and REM Series units also include a USB Mini format SetUp Port. For instructions regarding configuration of the USB Mini SetUp Port, please refer to Section 7.3.1.

  Note: *For more information regarding CLI commands and scripting, please refer to Section 12*

Once Telnet, HTTP and/or HTTPS are enabled, you can then access the CLI as follows:

1. **Contact the AFS:**

   a) **Via SetUp Port or Mini USB Port:** Start your communications program and press **[Enter]**. Wait for the connect message, then proceed to Step 2.

   b) **Via Network:** The AFS includes a default IPv4 format IP address (192.168.168.168) and a default IPv4 format subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit.

      i. **Via SSH Client:** Start your SSH client, and enter the AFS's IP Address. Invoke the connect command, wait for the connect message, then proceed to Step 2.

      ii. **Via Telnet:** Start your Telnet Client, and then Telnet to the AFS's IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Dial-Up Modem:** If your AFS unit includes the optional external modem or if you have installed a modem at one of the AFS's serial ports, you can then use your communications program to dial the number for the phone line that you have connected to the modem.

   d) **Via Cellular:** If your AFS includes the Cellular Modem Option, and the cellular modem has been set up as described in Section 8 in this User's Guide and the WTI Hardware Guide, you can then use your communications program to connect to the IP address for the cellular modem.

2. **Login** / **Password Prompt:** A message will be displayed, which prompts you to enter a username (login name) and password. The default username is super (all lower case,) and the default password is also super.

   Note: *If a Login Banner has been defined, then a banner page will appear before the command prompt is displayed. The Login Banner can be used to display legal warnings or other information.*

3.4. The WMU Enterprise Management Solution

The WMU Enterprise Management Solution provides a centralized interface that can be used to configure, manage and control multiple WTI out-of-band management devices spread throughout a large corporate network infrastructure. When installed at your network operation center or support facility, the WMU eliminates the need to individually access WTI units in order to perform software updates, control power switching functions, edit user accounts and perform other management and control functions.

The WMU software and user's guide can be downloaded at:

ftp://ftp.wti.com/pub/TechSupport/WMU/WTIManagementUtilityInstall.exe

4. Status Screens

The Status Screens are used to display information regarding the AFS, including current alarm states, selected configuration parameters, circuit status and other information.

Note: *In addition to the Web Browser Interface Status Screens that are discussed in this section, the Command Line Interface also provides additional Status Screens. For more information, please refer to Section 10.4.1.*

4.1. Product Status (/J*)

The Product Status Screen lists the software version, model number, power rating, product serial number and other information regarding the AFS.

Note: *The Information provided by the Product Status Screen is intended mainly to assist WTI support personnel.*

4.2. The Network Status Screen (/SN)

The Network Status screen shows activity at the AFS's virtual network ports. To view the Network Status Screen, you must access the user interface using a password that permits access to Administrator Level commands.

4.3. The Circuit Status Screen (/S)

The Circuit Status Screen shows the status of the AFS's Circuit Modules, and also lists the unit's temperature, Monitor/Alarm Input status, and Alarm Contact Output status.

Note:

- *When the Circuit Status screen is viewed by an account with Administrator or SuperUser command access, all AFS Circuit Modules present are listed. When the Circuit Status screen is viewed by an account with User or ViewOnly command access, then the screen will list only the Circuit Modules that are allowed by the account.*
- *If a Circuit Module slot is empty, then the Circuit Status screen will display a row of dashes for that Circuit Module position.*

To display the Circuit Status Screen via the Text Interface, type `/s` and then press **[Enter]**. To display the Circuit Status Screen via the Web Browser Interface, click on the "Circuit Status" link.

4.4. The Circuit Group Status Screen (/SG)

The Circuit Group Status screen shows the configuration details and A/B switching status for the AFS's user-defined Circuit Groups.

Notes:

- *When the Circuit Group Status Screen is viewed by an account with Administrator or SuperUser command access, all AFS Circuit Modules and Circuit Groups will be shown. When the Circuit Status Screen is viewed by an account with User or ViewOnly command access, then the unit will only display the Circuit Modules and Circuit Groups that are allowed by the account.*
- *In order to display the Circuit Group Status screen, you must first define at least one Circuit Group.*

To display the Circuit Group Status Screen via the Text Interface, type **/SG** and then press **[Enter]**. To display the Circuit Group Status Screen via the Web Browser Interface, click on the "Circuit Group Status" link.

4.5. The Port Diagnostics Screen (/SD)

The Port Diagnostics Screen provides more detailed information about the serial port. To display the Port Diagnostics Screen, access the Text Interface command mode and type **/SD [Enter]**.

Note: *The Port Diagnostics Screen is only available via the Text Interface.*

4.6. The Alarm Status Screen (/AS)

The Alarm Status Screen lists all available user-defined alarms and indicates whether or not each alarm has been triggered. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm. For a list of alarm arguments, please refer to Section 10.4.1.

4.7. The Port Parameters Screens (/W)

The /W (Who) command displays currently selected configuration parameters for the serial port and network port. Rather than listing general connection information for the ports, the Port Parameters screen lists all defined parameters for each port.

When the /W command is invoked by an Administrator or SuperUser level account, it can be used to display parameters for either the serial port or the Network Port. If the /W command is invoked by a User or ViewOnly level account, then it will only display parameters for the serial port.

The /W command offers the following options:

- Display Serial Port Parameters: (Administrators and SuperUsers Only) **`/w 1` [Enter]**
- Display Network Port Parameters: **`/w` [Enter]**

Note: *The Port Parameters screens are only available via the Text Interface*

4.8. The Log Status Screens (/L)

The Log Status Screens are used to display or download the Audit Log and the Alarm Log.

4.8.1. Audit Log

The Audit Log lists all user activity on the AFS, including user account logins and logouts, port connection, circuit switching and other events. Each audit record in the log includes a time stamp, the name of the user account that initiated each action and a brief description of each action. The Audit Log can either be displayed or downloaded in ASCII text format.

4.8.2. Alarm Log

The Alarm Log lists all automatically generated alarms that have occurred at the AFS. Each log record includes a time stamp, the name of the Alarm that was triggered and a brief description of the event that triggered the alarm. The Alarm Log can either be displayed or downloaded in ASCII text format. For more information on Alarm functions, please refer to Section 6.9.

4.8.3. Syslog

Lists all Syslog status messages.

4.8.4. Temperature Log

The temperature log provides a record of AFS temperature readings, in reverse chronological order, with the most recent events appearing at the top of the list.

5. Control Functions

As discussed in Section 3, the AFS offers two separate command interfaces; the Web Browser Interface and the Text Interface. Both interfaces offer essentially the same options and features, and in most cases, parameters defined via the Web Browser Interface will also apply when communicating via the Text Interface (and vice versa.)

5.1. A/B Switching - Web Browser Interface

When using the Web Browser Interface, A/B switching commands are invoked via the Circuit Control Screen and Circuit Group Control Screen.

5.1.1. The Circuit Control Screen - Web Browser Interface

The Circuit Control Screen lists the current A/B status of the AFS's Circuit Modules and is used to control switching of each A/B circuit. To perform A/B switching or set circuits to user-defined default states, proceed as follows:

1. Access the AFS Command Mode, and then click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control Screen.

   Notes:

   - *When the Circuit Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched circuits will be displayed.*
   - *When the Circuit Control Screen is displayed by an account that permits User or ViewOnly command access, the screen will only include the circuits that are specifically allowed by the account.*

2. **A/B Switching:** From the Circuit Control Menu, click the down arrow in the "Action" column for the desired circuit(s), then select position "A" or position "B" from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Actions" button to complete the command.

3. **Setting Circuits to the Default State:** From the Circuit Control Menu, click the down arrow in the "Action" column for the desired circuits, then select "Default" from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching actions and asks for confirmation before proceeding. Click on "Execute Actions" to complete the command; all selected circuits will be set to their user-defined default state.

4. **Applying a Command to All Circuits:** From the Circuit Control Menu, click the down arrow in the "Action" column in the "All Circuits" row, then select the desired operation from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Actions" button to apply the selected command to all AFS Circuits.

   Note: *When each command is complete, the Circuit Status Screen will be displayed. At that time, the Status Screen will list the updated A/B status of each circuit.*

5.1.2. The Circuit Group Control Screen - Web Browser Interface

The Circuit Group Control Screen is used to apply A/B switching commands to all circuits in a user-defined Circuit Group. Circuit Groups allow you to define a group of circuits, dedicated to a similar purpose or client, and then direct switching commands to the group, rather than switching one circuit at a time.

To invoke A/B switching commands, proceed as follows:

1. Access the AFS Command Mode, and then click on the "Circuit Group Control" link on the left hand side of the screen to display the Circuit Group Control Screen.

   Notes:

   - *When the Circuit Group Control Screen is displayed by an account that permits Administrator or SuperUser command access, all user-defined Circuit Groups will be displayed.*
   - *When the Circuit Control Screen is displayed by an account that permits User or ViewOnly level commands, the screen will only include the Circuit Groups that are allowed by the account.*

2. **A/B Switching - Circuit Groups:** From the Circuit Group Control Menu, click the down arrow for the desired Circuit Group(s), then select "A" or "B" from the dropdown menu and click on the "Confirm Group Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Group Actions" button to execute the command(s.)

3. **Switching Circuit Groups to Defaults:** From the Circuit Group Control Menu, click the down arrow for the desired group(s), then select "Default" from the dropdown menu and click on the "Confirm Group Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Group Actions" button to execute the command; all selected circuit groups will be set to their user-defined default states.

   Note: *When each Circuit Group command is completed, the Circuit Status Screen will be displayed. At that time, the Status Screen will show the updated A/B status of each circuit.*

5.2. A/B Switching - Text Interface

When using the Text Interface, all A/B switching functions are performed by invoking simple, ASCII commands. The Text Interface includes a Help Menu, which summarizes all available AFS commands. To display the Text Interface Help Menu, type /H and press [Enter].

Note: *When the Help Menu is displayed by an account that permits SuperUser, User or ViewOnly level commands, the screen will not include commands that are only available to Administrators.*

5.2.1. The Circuit Status Screen - Text Interface

The Circuit Status Screen lists the current status of the Circuit Modules, and also displays the current temperature, Monitor/Alarm Input status, Alarm Contact Output status and the user-defined Site I.D. Message. The Circuit Status Screen will be redisplayed each time a command is successfully executed.

5.2.2. A/B Switching Commands - Text Interface

These commands can be used to switch AFS's circuit modules, and can also be used to set circuits to the user-defined default A/B positions. Circuits may be specified by number, name or Circuit Group Name.

Notes:

- *When the Port and Circuit Status Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched circuits will be displayed.*
- *When the Port and Circuit Status Screen is displayed by an account that permits ViewOnly or User command access, the screen will only include the switched circuits that are specifically allowed by the account.*
- *When you have accessed command mode using an account that permits Administrator or SuperUser level commands, switching commands can be applied to all circuits.*
- *When you have accessed command mode using an account that permits only User level commands, switching commands can only be applied to the circuits that are specifically allowed by that account.*
- *Text Interface commands are not case sensitive. When used in command lines, circuit names and Circuit Group names are also not case sensitive.*

When A/B switching commands are executed, the AFS will list specified switching actions for each applicable Circuit Module, then display a "Sure?" prompt and wait for a user response before completing the command. The unit will then return to the Circuit Status Screen.

To switch Circuits or Circuit Groups, proceed as follows:

1. **Switch Circuit(s) to "A" Position:** Type **/TA n** and press **[Enter]**. Where "**n**" is the number or name of the desired Circuit or Circuit Group. For example:

   /TA 1 [Enter] or, **/TA DATACENTER [Enter]**

2. **Switch Circuit(s) to "B" Position:** Type **/TB n** and press **[Enter]**. Where "**n**" is the number or name of the desired Circuit or Circuit Group. For example:

   /TB 2 [Enter] or ,**/TB SERVERS [Enter]**

3. **Set All Permitted Circuits to Default A/B Positions:** Type **/DC** and press **[Enter]**. All circuits permitted by your account will be set to their default A/B status, which can be defined via the Circuit Parameters Menu.

   Notes:

   - *When you have accessed command mode using an account that permits Administrator or SuperUser level command access, the Default command will be applied to all circuits.*
   - *When you have accessed command mode using an account that only permits User level command access, the Default command will only be applied to the circuits specifically allowed by that account.*
   - *Switching commands are not available in ViewOnly mode.*

4. **The "Toggle" Command:** As an alternative to the /TA and /TB commands, the /T (Toggle) command can also be used to perform A/B switching. Type **/T n,p** and press **[Enter]**. Where "**n**" is the number or name of the desired Circuit or Circuit Group and "**p**" is the desired A/B position. For example:

   /T 2,B [Enter], or **/T SERVERS,A [Enter]**

5. **Suppress Command Confirmation Prompt:** To execute a switching or default command without displaying the "Sure?" prompt, you can either disable command confirmation via the System Parameters Menu, or include the "**,Y**" option at the end of the command line. For example:

   /TA ROUTER,Y [Enter] or, **/T 2,B,Y [Enter]**

5.2.2.1. Applying Commands to Several Circuits - Text Interface

As described below, A/B switching commands can be applied to only one Circuit Module, or to an assortment of circuits.

1. **Switch Several Circuits:** To apply the /TA, TB or /T command to several circuits, enter the numbers or names for the circuits, separated by a "plus sign" (+) or a comma (,). For example to switch circuits 1, 3, and 4 to the "B" position, enter one of the following commands:

   `/TB 1+3+4` [Enter]
   or,
   `/T 1+3+4,B` [Enter]

   Note: *When the "+" or "," are used, do not enter spaces between the circuit name or number and the plus sign or comma.*

2. **Switch a Range of Circuits:** To apply the /TA or /TB command to a series of circuits, enter the numbers for the circuits that mark the beginning and end of the range, separated by a colon. For example to switch circuits 1 through 3 to the "A" position, enter the following:

   `/TA 1:3` [Enter]

   Note: *The "Range" argument is not available when using the /T command to switch circuits. The Range (:) argument can only be used with the /TA and /TB commands.*

4. **All Circuits:** To apply a command to all circuits, enter an asterisk in place of the name or number. For example, to switch all circuits to the "B" position, enter one of the following commands:

   `/TB *` [Enter] or **`/T *,B` [Enter]**

   Note: *When this command is invoked by an account that permits only User level command access, it will be applied only to the circuits that are allowed by that account.*

5.3. The SSH/Telnet Connect Function (Web Browser Interface Only)

The SSH/Telnet Connect function allows you to open an SSH Shell Session or Telnet Session without leaving the Web Browser interface. Once you have successfully opened an SSH Shell Session or Telnet Session, you can then use ASCII commands to configure and operate the AFS unit.

5.3.1. Initiating an SSH Shell Session via the Web Browser Interface

To initiate an SSH Shell Session from the AFS Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the SSH option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. **Start Java:** Click on the File menu and select "Open Shell Session"

3. The AFS will display a prompt that asks the user to enter a valid username and host name (IP Address.) Key in the username and host name (IP address) using the following format and then click on the "OK" button:

   `username@ip_address`

   Notes:

   - *The username entered must be a valid username that has been previously defined via the AFS User Directory as described in Section 6.4.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another AFS unit, providing that the username entered is present on the other AFS unit too.*

4. After the username and host name are entered, the AFS will prompt you to enter your password. Key in the password that has been defined for the username entered in step 3 above and then click on the "OK" button.

5. The AFS will display the Circuit Status Screen, followed by the command prompt. You may now invoke AFS commands.

6. To terminate the SSH Session, type **`/x`** and press **[Enter]**.

5.3.2. Initiating a Telnet Session via the Web Browser Interface

To initiate a Telnet Session from the AFS Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the Telnet option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. Log in to the Telnet Session:

   a) The AFS will display the "login" prompt. Key in a valid username that has been previously defined via the AFS User directory and then press [Enter].

   b) The AFS will display the "password" prompt. Key in the valid password for the username entered above and then press **[Enter]**.

   Notes:

   - *The username entered must be a valid username that has been previously defined via the AFS User Directory.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another AFS unit, providing that the username entered is present on the other AFS unit too.*

3. The AFS will display the Circuit Status Screen, followed by the command prompt. You may now invoke AFS commands.

4. To terminate the Telnet Session, type **`/x`** and press **[Enter]**.

5.4. Manual Operation

In addition to the command driven functions available via the Web Browser Interface and CLI, some functions can also be controlled manually. For a summary of front panel control functions, please refer to the Hardware Installation Guide for your AFS.

5.5. Logging Out of the User Interface

When you have finished communicating with the AFS it is recommended to disconnect from the device using the LogOut button on the left hand side of the screen. Note that you can also log out from the CLI using the /X command.

Logging out helps to ensure that the AFS has completely exited from the user interface, and is not waiting for the inactivity timeout period to elapse before allowing additional connections.

6. Configuration Options

This section describes the basic configuration procedure for AFS Series RJ45 Fallback Switches. Although this section focuses primarily on the Web Browser Interface, all of the parameters and options described here can also be defined via the Command Line Interface. For instructions regarding configuration via the CLI, please refer to Section 10.

All menus discussed in the section can be accessed by clicking on the Configuration link on the left hand side of the Web Browser Interface. Clicking on the Configuration link will expand the menu to reveal additional submenu choices. Likewise, clicking on each submenu will also reveal additional configuration menus.

Notes:

- *To access the user interface, proceed as described in Section 3.2.*
- *Configuration menus are only available when you have logged into the user interface using a password that permits Administrator Level commands. SuperUser accounts are able to view configuration menus, but are not allowed to change parameters.*
- *Some parameters described in this section are only available on specific WTI product families and models.*

6.1. General Parameters

The General Parameters menus allow you to define parameters related to general unit setup, calibration, security and scripting. As described in the following sections, the General Parameters link provides access to the System Parameters Menu, Real Time Clock Menu, Invalid Access Lockout Menu, Callback Security Menu, and Scripting Options Menu.

6.1.1. System Parameters

The System Parameters Menu is used to define the Site ID tag for the AFS, select the temperature format, enable/disable log functions, enable/disable front panel controls, calibrate temperature and voltage metering and to set other system related parameters. The table below summarizes the items in the System Parameters Menu.

Parameter (Default)	Description
Site ID (Default = Undefined)	A text field, generally used to note the installation site or name for the AFS. **Note:** *The Site ID will be cleared if the AFS is reset to default settings.*
Temperature Format (Default = Fahrenheit)	Determines whether the temperature is displayed as Fahrenheit or Celsius format.
Temperature Calibration (Default = Undefined)	Used to calibrate the unit's internal temperature metering abilities.
Audit Log (Default = On without Syslog)	Enables/disables the Audit Log and enables/disables Syslog notification when new Audit records are added. The Audit Log will create a record of all power switching and toggle activity at the AFS, including toggles and switching caused by the Ping No Answer alarm.
Audit Log Facility (Default = 0)	The Facility number used to generate Syslog Messages for Audit Log Events.
Audit Log Level (Default = Info)	The severity level used to generate Syslog Messages for Audit Log Events
Alarm Log (Default = On without Syslog)	Enables/disables the Alarm Log and enables/disables Syslog notification when new Alarm records are added. The Alarm Log will create a record of each instance where an Alarm is triggered or cleared
Control Card A/B Switch (Default = On)	
Control Card Reset Switch (Default = On)	
Syslog Server Format (Default = Standard)	The format used in Syslog Server Log.
Temperature Log (Default = On)	Enables/disables the Temperature Log
Analog Modem Phone No. (Default = Undefined)	If the AFS includes the optional internal dial-up modem, this parameter can be used to record the phone number. When the AFS is used in conjunction with the WMU Enterprise Management Solution, the WMU will retrieve the phone defined here for use when contacting the unit via dial-up.
Asset Tag (Default = Undefined)	Allows a descriptive tag or tracking number to be assigned to the AFS. Once defined, the Asset Tag can be displayed via the Product Status Screen
Location (Default = Undefined)	This field can be used to record the installation location for the AFS unit.

6.1.2. Real Time Clock

The Real Time Clock menu is used to set the AFS's internal clock and calendar. The configuration menu for the Real Time Clock offers the following options:

Notes:

- *The AFS will contact the NTP server and update the time whenever you change NTP parameters.*
- *To cause the AFS to immediately contact the NTP server at any time, make certain that the NTP feature is enabled and configured, then click on the Change RTC Parameters link. The AFS will save parameters and then attempt to contact the server, per currently defined NTP parameters.*
- *In order for the Test NTP Servers feature to function, your network and/or firewall must be configured to allow ping commands.*

Parameter (Default)	Description
Date (Default = Undefined)	Sets the Month, Date, Year and day of the week.
Time (Default = Undefined)	Sets the Hour, Minute and Second for the AFS unit's real time clock/calendar. Key in the time using the 24-hour (military) format.
Time Zone (Default = Undefined)	Sets the time zone, relative to Greenwich Mean Time. Note that the Time Zone setting will function differently, depending upon whether or not the NTP feature is enabled and properly configured • **NTP Enabled:** The Time Zone setting is used to adjust the Greenwich Mean Time value (received from the NTP server) in order to determine the precise local time for the selected time zone. • **NTP Disabled:** If disabled, or if the unit cannot access the NTP server, then status screens and activity logs will list the selected Time Zone and Real Time Clock value, but will not apply the correction factor to the Real Time Clock value.
NTP Enable (Default = Off)	When enabled, the AFS will contact an NTP server (defined via the NTP Address prompts) once a day, and update its clock based on the NTP server time and selected Time Zone. **Note:** *The AFS will also contact the NTP server and update the time whenever you change NTP parameters.*
Primary NTP Address (IPv4) (Default = Undefined)	Defines the IPv4 protocol IP address or domain name for the primary NTP server. **Note:** *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 6.3.1.6.1.*

Parameter (Default)	Description
Secondary NTP Address (IPv4) (Default = Undefined)	Defines the IPv4 protocol IP address or domain name for the secondary, fallback NTP Server. **Note:** *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 6.3.1.6.1.*
Primary NTP Address (IPv6) (Default = Undefined)	Defines the IPv6 protocol IP address or domain name for the primary NTP server. **Note:** *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 6.3.1.6.1.*
Secondary NTP Address (IPv6) (Default = Undefined)	Defines the IPv6 protocol IP address or domain name for the secondary, fallback NTP Server.
NTP Timeout (Default = 3 Seconds)	The amount of time in seconds that will elapse between each attempt to contact the NTP server. When the initial attempt is unsuccessful, the AFS will retry the connection four times. If neither the primary nor secondary NTP server responds, the AFS will wait 24 hours before attempting to contact the NTP server again.
Test NTP Servers	Allows you to ping the IP addresses or domain names defined via the Primary and Secondary NTP Address prompts in order to check that a valid IP address or domain name has been entered. **Note:** *In order for the Test NTP Servers feature to function, your network and/or firewall must be configured to allow ping commands.*

6.1.3. Invalid Access Lockout

When properly configured and enabled, the Invalid Access Lockout feature can monitor all login attempts. If a counter exceeds the user-defined threshold for maximum invalid attempts, then the corresponding port or protocol will be automatically disabled for the length of time specified by the Lockout Duration parameter. The Invalid Access Lockout menu allows you to select the following parameters:

Notes:

- *When the Serial Port Invalid Access Lockout Alarm has been enabled as described in Section 6.9.4, the AFS can also provide notification via email, Syslog Message, and/or SNMP trap when an Invalid Access Lockout occurs.*
- *If the Network Port has been locked by the Invalid Access Lockout feature, it will still respond to the ping command (providing that the ping command has not been disabled at the Network Port.)*

Parameter (Default)	Description
Serial Port Lockout Parameters	
Serial Port Lockout (Default = Off)	Enables/Disables the Invalid Access Lockout function for the serial SetUp Port. When enabled and excessive Invalid Access attempts are detected at the SetUp Port, the SetUp Port will be locked for the defined Serial Port Lockout Duration period.
Serial Port Lockout Attempts (Default = 9)	When the Serial Port Lockout function is enabled, this parameter determines the number of invalid attempts that must occur at the Serial Port in order to trigger the Invalid Access Lockout feature at the Serial Port.
Serial Port Lockout Duration (Default = 30 Minutes)	When the Serial Port Lockout function is enabled, this item selects the length of time that the serial SetUp Port will remain locked when an Invalid Access Lockout occurs. If the duration is set at “Infinite”, then ports will remained locked until the /UL command is issued.
SSH Protection Parameters	
SSH Protection (Default = Off)	Enables/Disables SSH Protection. When SSH Protection is enabled and excessive Invalid Access Attempts via SSH are detected, then the AFS will lock out the offending MAC address for the user-defined SSH Duration period.
SSH Hit Count (Default = 20)	When SSH Protection is enabled, this item defines the number of invalid attempts that must occur via SSH during the specified SSH Duration period in order to trigger the SSH Invalid Access Lockout function.
SSH Duration (Default = 2 Minutes)	When SSH Protection is enabled, this item selects both the length of time that an SSH Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When an SSH Lockout occurs, the offending MAC address will be prevented from establishing an SSH connection to the AFS for the defined SSH Lockout Duration period.

Parameter (Default)	Description
Telnet Protection Parameters	
Telnet Protection (Default = Off)	Enables/Disables Telnet Protection. When Telnet Protection is enabled and excessive Invalid Access Attempts via Telnet are detected, then the AFS will lock out the offending MAC address for the user-defined Telnet Duration period.
Telnet Hit Count (Default = 20)	When Telnet Protection is enabled, this item defines the number of invalid attempts that must occur via Telnet during the specified Telnet Duration period in order to trigger the Telnet Invalid Access Lockout function.
Telnet Duration (Default = 2 Minutes)	When Telnet Protection is enabled, this item selects both the length of time that a Telnet Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Telnet Lockout occurs, the offending MAC address will be prevented from establishing a Telnet connection to the AFS for the defined Telnet Duration period.
Web Protection Parameters	
Web Protection (Default = Off)	Enables/Disables Web Protection. When enabled, and excessive Invalid Access Attempts via Web are detected, the AFS will lock out the offending MAC address for the user-defined Web Duration period
Web Hit Count (Default = 20)	When Web Protection is enabled, this item defines the number of invalid attempts that must occur via Web during the specified Web Duration period in order to trigger the Web Invalid Access Lockout function.
Web Duration (Default = 2 Minutes)	When Web Protection is enabled, this item selects both the length of time that a Web Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Web Lockout occurs, the offending MAC address will be prevented from establishing a Web connection to the AFS for the defined Web Duration period.

6.1.4. Callback Security

The Callback function provides additional security when callers attempt to access the user interface via dial-up modem. When properly configured, dial-up users will not be granted immediate access to the user interface upon entering a valid password. Instead, the unit will disconnect, and dial a pre-defined number before allowing access via that number. If desired, users may also be required to re-enter the password after the AFS dials back. The Callback Security Menu offers the following options:

Notes:

- *After configuring and enabling Callback Security, you must then define a callback phone number for each desired user account (as described in Section 6.4) in order for this feature to function properly.*
- *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback number will be allowed to access the user interface without callback verification.*

Parameter (Default)	Description
Callback Enable (Default = On - Callback (Without Password Prompt))	This prompt offers five different configuration options for the Callback Security feature: • **Off:** All Callback Security is disabled. • **On - Callback (Without Password Prompt):** Callbacks will be performed for accounts that include a Callback Number. The login prompt will not be displayed when the user's modem answers. If the account does not include a Callback Number, the user will be granted immediate access and a Callback will not be performed. • **On - Callback (With Password Prompt):** Callbacks will be performed for accounts that include a Callback Number. The login prompt will be displayed when the user's modem answers; accounts that include a Callback Number will be required to re-enter their username/password when their modem answers. If the account does not include a Callback Number, then the user will be granted immediate access and a Callback will not be performed. • **On - Callback ONLY (Without Password Prompt):** Callbacks will be performed for accounts that include a Callback Number, and the username/password prompt will not be displayed when the user's modem answers. Accounts that do not include a Callback Number will not be able to access the user interface via modem. • **On - Callback ONLY (With Password Prompt):** Callbacks will be performed for accounts that include a Callback Number. The username/password prompt will be displayed when the user's modem answers (users will be required to re-enter their username/password when their modem answers.) Accounts that do not include a Callback Number will not be able to access the user interface via modem.
Callback Attempts (Default = 3)	The number of times that the AFS will attempt to contact the Callback number.
Callback Delay (Default = 30 Seconds)	The amount of time that the AFS will wait between Callback attempts.

6.1.5. Scripting Options

The Scripting Options submenu provides access to parameters that are used to set up the AFS for running various scripts. The Scripting Options menu allows the following parameters to be defined:

> **Note:** *The functions provided by the Scripting Options menu are intended for use in applications where scripts are employed to control the AFS. Improper use of Scripting Options menu functions can cause the AFS to become unresponsive. Prior to attempting to use the functions provided by the Scripting Options menu, it is recommended to contact WTI Technical Support.*

Parameter (Default)	Description
Command Confirmation (Default = On)	When enabled, a "Sure" prompt will be displayed before switching and toggle commands are executed. When disabled, commands are executed without further prompting.
Automated Mode (Default = Off)	When enabled, the unit will execute switching and toggle commands without displaying a confirmation prompt, status screen or confirmation messages. For more information on Automated Mode, please refer to Section 6.1.5.1.
Reverse DNS (Default = On)	Determines the manner in which ARP requests are handled. When enabled (On,) the unit will check an external DNS in order to resolve domain names. When disabled (Off,) the unit will not check an external DNS when resolving domain names.
Port 1 Mode Override (Default = Off)	In order to ensure local access to command functions, normally Serial Port 1 can only be configured as a Passive Mode Port or Any-to-Any Mode Port. When the Port 1 Mode Override option is enabled, Serial Port 1 can be configured as a Buffer Mode Port, Modem Mode Port or Modem PPP Mode Port. **Note:** *Configuring Serial Port 1 as a Buffer Mode Port can disable local access to command functions via serial port.*
Keep Alive (Default = 7,200 Seconds)	In cases where Linux regularly times out and disrupts network communication with the unit, this parameter can be used to keep the network connection active. **Note:** *The "Modem Hunt Telnet" option is recommended for transmitting ASCII data and the "Modem Hunt Raw" option is recommended for transmitting binary data.*
TCP Time Stamps (Default = On - Using Random Resets)	
Reset Unit	Restarts the AFS operating system. **Note:** *The Reset function does not switch off power to the AFS. The Reset Unit function only restarts the AFS operating system.*

6.1.5.1. Automated Mode

The Automated Mode allows the AFS to execute switching and toggle commands without displaying menus or generating response messages. Automated Mode is designed to allow the AFS to be controlled by programs or devices that can generate commands to control power switching functions without human intervention.

Although Automated Mode can be enabled using either the Web Browser Interface or CLI, Automated Mode is designed primarily for users who wish to send ASCII commands to the AFS without operator intervention, and therefore does not specifically apply to the Web Browser Interface. When Automated Mode is enabled, the Web Browser Interface can still be used to invoke switching and toggle commands.

Notes:

- *When the Automated Mode is enabled, password prompts will not be displayed at login, and you will be able to access Administrator Level command functions (including the configuration menus) and control circuits without entering a password.*
- *If you need to enable the Automated Mode, but want to restrict network access to configuration menus, it is strongly recommended to enable and configure the IP Tables function as described in Section 6.3.1.4.*

When enabled, AFS functions will change as follows:

1. **All Password Security Suppressed:** When a user attempts to access the user interface, the password prompt will not be displayed at either the Setup Port or Network Port. Unless specifically restricted by the IP Security Function, all users will be allowed to access the user interface, and all commands will be immediately accepted without the requirement to enter a password.
2. **Status Screen Suppressed:** The Circuit Status Screen will not be automatically displayed after commands are successfully executed. Note however, that the Circuit Status Screen can still be displayed as needed.
3. **Confirmation Prompts Suppressed:** All commands are executed without prompting for user confirmation.
4. **Error Messages Suppressed:** Most error messages will be suppressed. Note however, that an error message will still be generated if commands are invoked using invalid formats or arguments.

All other status display and configuration commands will still function as normal.

6.2. Serial Setup Port Configuration

The Port Configuration menu allows you to select parameters for the AFS unit's RJ45 Serial Setup Port. In addition to setting the port mode and communication parameters, the Port Configuration menus can also be used to select a number of other parameters described in the table below.

Parameter (Default)	Description
Communication Settings	
Baud Rate (Defaults; RJ45 Serial Ports and USB Ports = 9600 bps; Internal Modem Port = 57.6K bps)	Any standard rate from 300 bps to 230.4 kbps.
Bits/Parity (Default = 8-None)	The Data Bits and Parity settings for the Serial Port.
Stop Bits (Default = 1)	The Stop Bits setting for the Serial Port.
Handshake Mode (Default = RTS/CTS)	XON/XOFF, RTS/CTS (hardware), Both, or None.
General Parameters	
Administrator Mode (Default = Permit)	Permits/denies port access to Administrator level accounts. When enabled (Permit), the port will be allowed to invoke Administrator level commands, providing they are issued by an account that permits them. If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access the user interface via this port. **Note:** *Administrator Mode cannot be disabled at Serial Port 1 (the SetUp port.)*
Logoff Character (Default = **^x**)	Defines the CLI Logoff Character. In the CLI, the Logoff Character determines the command(s) or character(s) that must be issued at this port in order to disconnect. Note that the Logoff Character does not apply to Direct Connections.
Sequence Disconnect (Default = One Character)	Enables/Disables and configures the Resident Disconnect command in the CLI interface. This option allows users to disable the CLI Sequence Disconnect, select a one character format or a three character format.

Parameter (Default)	Description
General Parameters (continued)	
Inactivity Timeout (Default = 5 Minutes)	Enables and selects the Timeout Period for this port. If enabled, the Serial Port will disconnect when no additional data activity is detected for the duration of the timeout period. **Notes:** • *When disabled, ports will automatically reconnect after a power interruption. When power is restored, pairs of ports that were previously connected will be automatically reconnected, providing that the Inactivity Timeout is disabled at both ports, and the two ports have been connected for at least ten minutes prior to the power interruption.* • *The only exception to this rule is Serial Port 1, which will remain disconnected after power is restored in order to provide a free serial port for local access to the user interface.*
Command Echo (Default = On)	Enables/Disables command echo for the CLI at this port. When disabled, commands sent to the Serial Port will still be invoked, but the keystrokes will not be displayed on your monitor.
Accept Break (Default = On)	Determines whether the port will accept breaks received from the attached device. When enabled, breaks received at the port will be passed to any port this port is connected to. When disabled, breaks will be refused at this port.
Port Mode Parameters	
Port Name (Default = Undefined)	This parameter is used to assign a descriptive name to the Serial Port.
Port Mode (Default = Normal Mode))	The operation mode for this port; Normal Mode, Modem Mode or Modem PPP Mode. For more information, please refer to Section 6.2.1.
DTR Output (Default = Pulse)	(Any-to-Any Mode Ports and Passive Mode Ports only) Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high.
Modem Reset String (Default = **`ATZ`**)	(Modem Mode and Modem PPP Mode Only) Redefines the modem reset string. The Reset String can be sent prior to the Initialization string.
Modem Initialization String (Default = **`AT&C1&D2S0=1&B1&H1&R2`**)	(Modem Mode and Modem PPP Mode Only) Defines a command string that can be sent to initialize a modem to settings required by your application.
Modem Hang-Up String (Default = Undefined)	(Modem Mode and Modem PPP Mode Only) Although the AFS will pulse the DTR line to hang-up an attached modem, the Hang-Up string can be used for controlling modems that do not use the DTR line.
Reset/No Dialtone Interval (Default = 15 Minutes)	(Modem Mode and Modem PPP Mode Only) Defines the Periodic Modem reset duration, (which determines how often the Reset String will be sent to a modem at this port) and also sets the trigger value for the No Dialtone Alarm. If this value is set to "0," then the No Dialtone Alarm will not function. For more information, please refer to Section 6.9.7.

Parameter (Default)	Description
Port Mode Parameters (Continued)	
No Dialtone Alarm Enable (Default = Off)	(Modem Mode and Modem PPP Mode Only) Enables/Disables the No Dialtone Alarm. This item must be enabled in order for the No Dialtone Alarm to function.
Reset/No Dialtone Scaler (Default = 15 Minutes)	(Modem Mode and Modem PPP Mode Only) Determines the number of Periodic Modem Reset sequences that must occur in order to initiate a No Dialtone Check. If set to "0," then the No Dialtone Alarm will not function. When both this parameter and the Reset/No Dialtone Interval are set to a value from 1 to 99 and the No Dialtone Alarm is enabled, the AFS will initiate a No Dialtone Check after a time period equal to the defined Reset/No Dialtone Interval value multiplied by the Reset/No Dialtone Scaler value.
PPP Parameters	
PPP Phone Number (Default = Undefined)	(Modem PPP Mode Only) The phone number for the line that will be used for PPP communication.
Username (Default = Undefined)	(Modem PPP Mode Only) The username for the ISP account that will be used for PPP communication.
Password (Default = Undefined)	(Modem PPP Mode Only) The password for the ISP account that will be used for PPP communication.
Periodic Reset Location (Default = Undefined)	(Modem PPP Mode Only) The IP address or URL for the website that will be used to keep the PPP connection alive when not in use. The AFS will regularly ping the selected IP address or URL to keep the connection alive. **Notes:** • *In order to select a domain name as the Periodic Reset Location, you must first define the Domain Name Servers as described in Section 6.3.2.6.1.* • *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication is started.*
IP Address (Default = Undefined)	(Modem PPP Mode Only) The temporary IP address assigned to the PPP communication session by the ISP. This item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is initiated.
P-t-P (Default = Undefined)	(Modem PPP Mode Only) Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started.
Subnet Mask (Default = Undefined)	(Modem PPP Mode Only) Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started.

6.2.1. Serial Port Modes

The Serial Setup Port offers three different serial port operation modes:

- **Normal Mode:** The default Port Mode for the Serial Setup Port. Allows local access to AFS command and configuration functions.
- **Modem Mode:** Allows an external modem to be connected to the Serial Setup Port. Modem Mode allows definition of a Hang-Up String, Reset String, and Initialization String and other modem-related parameters.
- **Modem PPP Mode:** Allows data normally sent via Ethernet to be sent via phone line to a modem connected to the Serial Setup Port. Modem PPP Mode allows definition of a Hang-Up String, Reset String, Initialization String, IP Address and other communication-related parameters.

6.2.1.1. Normal Mode

Allows local access via serial connect to AFS command and configuration functions. Typically, Normal Mode is selected when your primary means of communication with the AFS unit will be via local connection to the Serial Setup Port. Normal Mode is the default mode for the Serial Setup Port.

6.2.1.2. Modem Mode

Modem Mode allows an external modem to be connected to the Serial Setup Port, and provides features specifically related to dial-up modem communication. Modem Mode also supports all of the functions normally available in Normal Mode.

When a call is received, the unit will prompt the caller to enter a username and password. The AFS allows three attempts to enter a valid username and password. If a valid username and password is not entered within three attempts, or if the user does not respond to the login prompt within 30 seconds, the modem will disconnect.

> **Note:** *When a Modem Mode port exits the user interface, or the DCD line is lost while the user interface is active, the AFS will pulse DTR to the dial-up modem. The unit will then send the user-defined modem command strings to make certain the modem is properly disconnected and reinitialized.*

6.2.1.3. Modem PPP Mode

The Modem PPP Mode allows data normally sent via Ethernet to be sent via phone line. Modem PPP Mode also supports all of the functions that are available in Normal Mode, but Modem PPP Mode also allows definition of additional communications-related parameters.

When a call is received, the unit will prompt the caller to enter a username and password. The AFS allows three attempts to enter a valid username and password. If a valid username and password is not entered within three attempts, or if the user does not respond to the login prompt within 30 seconds, the modem will disconnect.

> **Note:** *When set to Modem PPP Mode, the Serial Setup Port will appear in the Network Configuration menu, listed as [ppp0].*

6.3. Network Configuration

The Network Parameters Menus are used to select parameters and options for the Network Port and also allow you to implement various security and authentication features.

Notes:

- *The Network Parameters Menu selects parameters for all logical Network Ports.*
- *The IP Address, Subnet Address and Gateway Address cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the unit via the CLI.*
- *When a new IP Address is selected, or the status of the DHCP feature is changed, the unit will disconnect and reconfigure itself with the new values when you exit the Network Parameters Menu. When configuring the unit, make certain your DHCP server is set up to assign a known, fixed IP address in order to simplify reconnection to the unit after the new address has been assigned.*
- *The Network Parameters menu is only available when you have logged into the user interface using an account and port that permit Administrator level commands (Administrator Mode enabled.)*

Automation

AFS units support both Ansible 2.7 and RESTful API. For more information regarding Ansible 2.7 and RESTful API, please refer to the WTI.com Knowledge Base.

6.3.1. Network Configuration [eth0] IPv4 Menu

The Network Configuration [eth0] IPv4 Menu is used to assign IPv4 parameters for the Ethernet Port (eth0.) In addition, this menu is also used to assign Shared Parameters that apply to both IPv4 and IPv6 IP Protocols. IPv4 parameters for eth0 are sorted into a series of submenus, according to function.

6.3.1.1. Shared Network Parameters

This menu is used to define Network Parameters that will be shared by both IPv4 and IPv6 protocols. The Shared Network Parameters Menu includes the following parameters:

Parameter (Default)	Description
Administrator Mode (Default = Permit)	Permits/denies access to Ethernet Port(s) by accounts that allow Administrator level commands. When enabled (Permit), the Administrator Mode accounts will be allowed to access the user interface via the Ethernet Port(s). If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access the user interface via the Ethernet Port(s). **Note:** *On CPM and DSM Series units, the setting for the Administrator Mode parameter will also be applied to the USB Mini format SetUp Port.*
Logoff Character (Default = **^x** (**[Ctrl]** plus **[X]**))	Defines the CLI Logoff Character for the Ethernet Port(s.) This determines the command that must be issued at this port in order to disconnect from a second port. **Notes:** • *The Sequence Disconnect parameter can be used to pick a one character or a three character logoff sequence.* • *On CPM and DSM Series units, the setting for the Logoff Character parameter will also be applied to the USB Mini format SetUp Port.*
Sequence Disconnect (Default = One Character)	Enables/Disables and configures the Resident Disconnect command for the CLI. Offers the option to either disable the Sequence Disconnect, or select a one character, or three character command format. **Notes:** • *The One Character Disconnect is intended for situations where the destination port should not receive the disconnect command. When the Three Character format is selected, the disconnect sequence will pass through to the destination port prior to breaking the connection.* • *When the Three Character format is selected, the Resident Disconnect uses the format "***[Enter]**`LLL`**[Enter]***", where* `L` *is the selected Logoff Character.* • *On CPM and DSM Series units, the setting for the Sequence Disconnect parameter will also be applied to the USB Mini format SetUp Port.*

Parameter (Default)	Description
Inactivity Timeout (Default = 5 Minutes)	Enables and selects the Inactivity Timeout period for the Ethernet Port(s.) If enabled, and the port does not receive or transmit data for the specified time period, the port will disconnect. **Note:** *On CPM and DSM Series units, the setting for the Inactivity Timeout parameter will also be applied to the USB Mini format SetUp Port.*
Command Echo (Default = On)	Enables or Disables command echo for the Ethernet Port(s.). **Note:** *On CPM and DSM Series units, the setting for the Command Echo parameter will also be applied to the USB Mini format SetUp Port.*
Accept Break (Default = On <ASCII 28>)	Determines how the Ethernet Port(s) will handle breaks received from the attached device. When disabled, all break codes are ignored and passed through untouched to the serial port. When enabled, ASCII 28 and/or IETF/RFC4335 SSH break sequences are stripped and a 'break' sequence is initiated on the connected serial port. **Note:** *On CPM and DSM Series units, the setting for the Accept Break parameter will also be applied to the USB Mini format SetUp Port.*
Telnet Access (Default = Off)	Enables/disables Telnet access to the Ethernet Port(s.) When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the Ethernet Port(s) or initiate outbound Telnet connections.
Telnet Port (Default = 23)	Selects the TCP/IP port number used for Telnet connections.
Max. Per Source (Default = 4)	The maximum number of sessions that will be allowed per user MAC address. **Note:** *After changing the "Max Per Source" parameter, you must log out of all pre-existing sessions in order for the new maximum value to be applied.*
SSH Access (Default = On)	Enables/disables SSH communication at the Ethernet Port(s.) **Note:** *For instructions regarding setting up SSH Public Key Authentication, please refer to the WTI.com Knowledge Base.*
SSH Port (Default = 22)	The TCP/IP port number used for SSH connections to the Ethernet Port(s.)

Parameter (Default)	Description
Outbound Access (Default = Off)	Enables/Disables the ability to create outbound SSH/Telnet connections via the AFS unit's Ethernet Port(s.) When enabled, users connected to the AFS user interface via one of the serial ports will be able to connect to the Ethernet Port(s,) and then invoke the /TELNET and/or /SSH commands to create an outbound SSH or Telnet connection. For more information, please refer to Appendix D.
Outbound Secure Level (Default = Serial Only)	When Outbound Access is enabled, this parameter is used to determine whether outbound connections may be established via both Serial Port and Network Port, or via Serial Port only.
Raw Socket Access (Default = Off)	Enables/Disables Raw Socket Protocol access to the Ethernet Port(s) via Direct Connect and selects either port 3001 or 23 for Raw Socket Access.

6.3.1.2. Network Parameters [eth0] IPv4

This menu is used to assign the IP Address, Subnet Mask and other IPv4 parameters for the Ethernet Port (eth0).

Parameter (Default)	Description
IP Address (Default = 192.168.168.168)	The IPv4 format address for the Ethernet Port, eth0. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the AFS via the CLI and invoke the /P command as described in Section 10.4.3.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the Ethernet Port, eth0. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the AFS via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the Ethernet Port, eth0. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the AFS via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol. When enabled, the AFS will perform a DHCP request. In the CLI, the MAC address is listed on the Network Status Screen. **Notes:** • *If needed, a separate DHCP configuration can be defined for each Ethernet Port and the Cell Port and both IPv4 and IPv6 format IP addresses can be defined for each port.* • *Prior to configuring this feature, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the AFS.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the AFS via the CLI.*

6.3.1.3. DHCP Server [eth0] IPv4

The DHCP Server menu allows you to define DHCP Server parameters for IPv4 communication via the Ethernet Port (eth0.)

Note: *For further instructions regarding setting up DHCP Server parameters, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables DHCP Server protocol for IPv4 at the Ethernet Port (eth0.)
Gateway (Default = Undefined)	The IPv4 format Gateway Address for the Ethernet Port (eth0.) **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the AFS via the CLI.*
Primary DNS (Default = Undefined)	The primary IPv4 format DNS address for the Ethernet Port (eth0.)
Secondary DNS (Default = Undefined)	The secondary IPv4 format DNS address for the Ethernet Port (eth0.)
Domain (Default = Undefined)	The IPv4 format Domain address for the Ethernet Port (eth0.)
Default Lease (Default = 600)	The default lease time in seconds that the IP is leased.
Max Lease (Default = 7000)	The maximum lease time in seconds that the IP can be leased.
Pool Start (Default = 1)	Start of address pool.
Pool End (Default = 254)	End of address pool.
Ping DNS Servers	Allows you to ping the IP addresses or domain names defined via the Primary and Secondary DNS Address prompts in order to check that a valid IP address or domain name has been entered. **Note:** *In order for the Ping DNS Servers feature to function, your network and/or firewall must be configured to allow ping commands.*

6.3.1.4. IP Tables IPv4

The IP Tables menu allow the AFS to restrict unauthorized IPv4 format IP addresses from establishing inbound connections to the unit. To define a firewall via the IP Tables menu, use Linux syntax routing commands to determine which IP address(es) will be allowed access and which IP address(es) will be denied. In most cases, the IP Tables should allow access to administrators and deny access to everybody else.

Note: *For instructions regarding setting up IP Tables, please refer to the WTI. com Knowledge Base.*

6.3.1.5. Static Route [eth0] IPv4

The Static Route menu is used to define Linux routing commands that are automatically executed each time a user accesses the AFS via the Ethernet Port (eth0.)

6.3.1.6. DNS Selection [eth0] IPv4

The DNS option is used to define DNS and DDNS parameters. In the [eth0] IPv4 menu, the DNS option is used to select either the DNS Parameters menu or the DDNS parameters menu.

6.3.1.6.1. DNS Servers (Shared)

The DNS Parameters menu is used to select IPv4 or IPv6 format IP addresses for Domain Name Servers for the Ethernet Port, [eth0] . When web and network addresses are entered, the Domain Name Server interprets domain names (e.g., www.wti.com), and translates them into IP addresses. Note that if you don't define at least one DNS server, then IP addresses must be used, rather than domain names.

The Domain Name Server menu includes a Ping Test feature that allows you to ping the IP addresses for each user-defined domain name server.

Note: *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

6.3.1.6.2. DDNS Parameters [eth0] IPv4

The DDNS Servers menu is used to select parameters and define hosts for Dynamic DNS services. The DDNS Parameters menu includes the following parameters:

Parameter (Default)	Description
Services (Default = None)	Sets the service type to either Dyn or None.
Host Name (Default = Undefined)	The IP Address for the DDNS Service.
Username (Default = Undefined)	The Username for your DDNS Account.
Password (Default = Undefined)	The Password for your DDNS Account.
Maximum Update Times (Default = Every 1 Hour)	Determines how often the AFS will ping the DDNS host address.

6.3.1.7. Negotiation [eth0] IPv4/IPv6

This parameter can be used to solve synchronization problems when the AFS negotiates communication parameters with another device.

Notes:

- *If the other device is set for automatic negotiation, then the AFS unit's Negotiation parameter should also be set to Auto.*
- *If the other device is not set for automatic negotiation, then the AFS unit's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*

6.3.1.8. Web Selection [eth0] IPv4/IPv6

This link provides access to the Web Access Menu, SSL Certificates Menu and Import Wildcard Certs Menu for both IPv4 and IPv6 access to the Ethernet Port (eth0.)

6.3.1.8.1. Web Access [eth0] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the Ethernet Port (eth0.)

Note: *For further information regarding web security, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
HTTP Access (Default = Off)	Enables/disables the Web Browser Interface. When disabled, users will not be allowed communicate with the unit via the Web Browser Interface.
HTTP Port (Default = 80)	Selects the TCP/IP port number used for HTTP connections.
HTTPS Access (Default = Off)	Enables/disables HTTPS communication. For instructions on setting up SSL/TLS encryption, please refer to Section 7.
HTTPS Port (Default = 443)	Selects the TCP/IP port number that will be used for HTTPS connections.
Harden Web Security (Default = Medium)	Offers three different Web Security settings: • **Off:** All SSL protocols are enabled. (Allows compatibility with older browsers.) • **Medium:** Only SSLv3/TLS1.x Protocols and MEDIUM/HIGH ciphers are enabled. • **High:** Only TLS1.x Protocol and HIGH ciphers enabled.
TLS Mode (Default = TLSv1.1/TLSv1.2)	Selects the TLS version that will be used. This parameter can select either TLSv1 only, both TLSv1.1 and TLSv1.2 or TLSv1.2 Only. For more information, please refer to Section 7.
Trace Method (Default = Off)	Enables/disables the Web Trace Method.
OCSP Stapling (Default = Off)	OCSP stapling improves performance and privacy by eliminating the need for a browser to check with a third party in order to determine if a security certificate is valid.

6.3.1.8.2. SSL Certificates [eth0]

Defines SSL Certificate parameters for the Ethernet Port (eth0.)

Notes:

- *For instructions regarding installing SSL certificates via the CLI, please refer to the WTI.com Knowledge Base.*
- *For instructions regarding installing SSL certificates via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
Common Name (CN) (Default = Undefined)	The Common Name is typically composed of Host + Domain Name (e.g., "www.yoursite.com".) SSL Certificates are specific to the Common Name to which they have been issued at Host level. The Common Name must be the same as the Web address you will access when connecting to the secure site.
State or Province (S) (Default = Undefined)	The full name of the State or Province where your organization is registered to operate by national, state or local authorities.
Locality (L) (Default = Undefined)	The name of the town or city where your organization is located.
Country Code (C) (Default = Undefined)	The two character, ISO-3166 Country Code for the nation where your organization is located.
Email Address (Default = Undefined)	An email address that can be used to contact the administrator of the certificate.
Organization (O) (Default = Undefined)	The legal name under which your company or organization is registered.
Organizational Unit (OU) (Default = Undefined)	The branch of your company that is requesting the certificate (e.g., "Tech Support" or "Human Resources".)
SAN Options (Default = Undefined)	Determines whether the SAN Certificate will be hidden or displayed. The Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with the security certificate using the subjectAltName field. These values are called "Subject Alternative Names" (SANs). Names can include: DNS names, IP addresses, Email addresses and URLs.
Show SAN	Displays additional menu options that can be used to define SAN Options.

6.3.1.8.3. Import Wildcard Certs [eth0] (SSL Certificate Import)

The Import Wildcard Certs Menu (SSL Certificate Import) is used to import a private key, a signed certificate and optionally a CA Intermediate Certificate for the Web server for the Ethernet Port (eth0]. The Import Wildcard Certs menu includes the following parameters:

Notes:

- *For instructions regarding installing SSL certificates via the CLI, please refer to the WTI.com Knowledge Base.*
- *For instructions regarding installing SSL certificates via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
Private Key	An alphanumeric key, issued by the Certification Authority.
Signed Certificate	The file that the Certification Authority returns to you, after you have submitted your Certificate Signing Request (CSR).
Show Intermediate CA Certificate	Shows or hides the Intermediate CA Certificate.

6.3.1.9. Syslog Parameters IPv4/IPv6

Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the AFS. Allows definition of IP addresses for both a primary Syslog Daemon and an optional secondary Syslog Daemon.

6.3.1.9.1. Syslog Client Parameters IPv4

Defines parameters for the Syslog Client for IPv4 communication via the Ethernet Port (eth0.) This menu can be used to define up to four Syslog Clients and to install certificates for each client

Parameter (Default)	Description
SYSLOG Address (Default = Undefined)	The external Syslog Server IP Address and corresponding UDP Syslog Server Port number.
Transport (Default = UDP)	The Transport protocol used for Syslog client.
Secure Syslog (SSL/TLS) (Default = Off)	Enables/disables Secure Syslog when TCP transport is selected.
Secure Syslog Verify Server (Default = On)	When using Secure Syslog, this parameter determines whether or not client certificates are used to verify server identity.
Install Certificate	Installs the Syslog Certificate for each of four available Syslog Clients.
Ping Syslog Servers	Pings the IP addresses for each defined Syslog Client in order to check that a valid IP address. **Note:** *In order for the Ping Syslog Servers feature to function, your network and/or firewall must be configured to allow ping commands.*

6.3.1.9.2. Syslog Server Parameters IPv4

Defines parameters for the Syslog Server for IPv4 communication via the Ethernet Port (eth0.)

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the Syslog Server function.
Port (Default = 514)	Network port used to listen for Syslog messages.
Transport (Default = UDP)	The transport protocol used for Syslog server.
Secure Syslog (SSL/TLS) (Default = Off)	Enables/disables Secure Syslog when TCP transport is selected.
Block IP 1 through 4 (Default = Undefined)	Drops Syslog messages from these IP addresses

6.3.1.10. SNMP Parameters [eth0] IPv4

This menu is used to select IPv4 format access parameters for the SNMP feature at the Ethernet Port (eth0.)

> **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the AFS unit's User Directory, control power and toggle switching and display unit status via SNMP, as described in Appendix F.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling. **Note:** *This parameter applies only to external SNMP polling of the AFS. It does not effect the ability of the AFS to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the AFS will respond to. For example, if this item is set to V3, then clients who attempt to contact the AFS using SNMPv2 will not be allowed to connect. When V3 is selected, the menu shown in Section 6.3.2.8.1 can be used to define additional parameters for SNMP.
Read Only (Default = No)	Enables/Disables the "Read Only Mode", which controls the ability to access configuration functions and invoke switching commands. When Enabled, you will not be able to change configuration parameters or invoke other commands when you contact the AFS via SNMP. Note: In order to define user names for the AFS via your SNMP client, the Read Only feature must be disabled. When the Read Only feature is enabled, you will not be able to issue configuration commands to the unit via SNMP.
System Name (Default = Undefined)	The host name of the AFS.
SNMP Contact (Default = Undefined)	The name of the administrator responsible for SNMP issues.
SNMP Location (Default = Undefined)	The location of the SNMP Server.
Read Only Community (Default = Public)	Note that this parameter is not available when the SNMP Version is set to V3.
Read/Write Community (Default = Public)	Note that this parameter is not available when the SNMP Version is set to V3.
V3 Users	When the SNMP version has been set to V3, this button can be used to access a submenu, used to define additional parameters for V3 Users as described in Section 6.3.2.8.1..

6.3.1.10.1. SNMP V3 Users (eth0 / IPv4)

When the SNMP version has been set to V3, the following parameters can be defined via the V3 Users menu.

Parameter (Default)	Description
SNMPv3 User Name (Default = Undefined)	Sets the User Name for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Authentication / **Privacy** (Default = Auth/noPriv)	Configures the Authentication and Privacy features for SNMPv3 communication. Two options are available: : • **Auth/noPriv:** An SNMPv3 username and password will be required at log in, but encryption will not be used. • **Auth/Priv:** An SNMPv3 username and password will be required at log in, and all messages will be sent using encryption. **Notes:** • *The Authentication / Privacy item is not available when the Version parameter is set to V1/V2.* • If the Version Parameter is set to V1/V2/V3 (all) and Authentication / Privacy parameter is set to "Auth/Priv", then only V3 data will be encrypted. • The AFS supports DES encryption, but does not currently support the AES protocol. • The AFS does not support "noAuth/noPriv" for SNMPv3 communication.
SNMPv3 Authentication Password (Default = Undefined)	Sets the Authentication Password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Authentication Protocol (Default = MD5)	This parameter determines which authentication protocol will be used. The AFS supports both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the AFS must match the protocol that your SNMP client will use when querying the AFS.* • *The Authentication Protocol option is not available when the Version parameter is set to V1/V2.*
SNMPv3 Privacy Password (Default = Undefined)	Sets the Privacy Password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Privacy Protocol (Default = DES)	(SNMPv3 Only) Selects AES or DES encryption support.

6.3.1.11. SNMP Trap Parameters [IPv4]

This menu is used to select parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Appendix F.

Parameter (Default)	Description
SNMP Managers 1 through 4 (Default = Undefined)	The IP Addresses for the SNMP Managers. **Note:** *In order to enable the SNMP Trap feature, you must define at least one SNMP Manager.*
Trap Community (Default = Public)	This field is used to enter the key that allows access to the AFS unit's SNMP Alarm Reporting.
Trap Version (Default = V1)	The assigned security level for SNMP traps.
V3 Trap Engine ID (Default = Undefined)	The V3 SNMP agent's unique identifier.

6.3.1.12. LDAP Parameters (Shared)

The AFS supports LDAP (Lightweight Directory Access Protocol,) which allows authentication via the Active Directory network Directory Service. When LDAP is enabled, command access rights can be granted to new users without the need to define individual new accounts at each AFS unit, and existing users can also be removed without the need to delete the account from each AFS unit. This also allows administrators to assign users to LDAP groups, and then specify which circuits the members of each group will be allowed to control at each AFS unit.

In order to apply the LDAP feature, you must first define User Names and associated Passwords and group membership via your LDAP server, and then access the AFS user interface to configure LDAP settings and define port access rights and command access rights for each group specified at the LDAP server. To access the LDAP Parameters menu, login to AFS user interface using a password that permits Administrator level commands.

The LDAP Parameters Menu allows the following parameters to be defined:

Notes:

- *The LDAP Parameters Menu defines parameters for both IPv4 and IPv6 protocols.*
- *Circuit access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each AFS unit and are specific to that AFS unit alone.*
- *When LDAP is enabled, LDAP authentication will supersede any passwords and access rights that have been defined via the AFS user directory.*
- *If no LDAP groups are defined on a given AFS, then access rights will be determined as specified by the "default" LDAP group.*
- *The "default" LDAP group cannot be deleted.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables LDAP authentication.
Primary Host IPv4 (Default = Undefined)	Defines the IP address or domain name for the primary LDAP server when IPv4 protocol is used to communicate with the AFS.
Primary Host IPv6 (Default = Undefined)	Defines the IP address or domain name for the primary LDAP server when IPv6 protocol is used to communicate with the AFS.
Secondary Host IPv4 (Default = Undefined)	Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv4 protocol is used.
Secondary Host IPv6 (Default = Undefined)	Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv6 protocol is used.
LDAP Port (Default = 389)	Defines the port that will be used to communicate with the LDAP server.
TLS/SSL (Default = Off)	Enables/Disables TLS/SSL encryption. Note that when TLS/SSL encryption is enabled, the LDAP Port should be set to 636.

Parameter (Default)	Description
Bind Type (Default = Simple)	Sets the LDAP bind request password type. Note that in the CLI, when the Bind Type is set to "Kerberos" LDAP, the menu will include additional prompts used to select Kerberos parameters.
Search Bind DN (Default = Undefined)	Selects the username that is allowed to search the LDAP directory.
Search Bind Password (Default = Undefined)	Sets the Password for the user who is allowed to search the LDAP directory.
User Search Base DN (Default = Undefined)	Sets the directory location for user searches.
User Search Filter (Default = Undefined)	Selects the attribute that lists the user name. Note that this attribute should always end with "=%S" (no quotes.)
Group Membership Attribute (Default = Undefined)	Selects the attribute that list group membership(s).
Group Membership Value Type (Default = DN)	Sets the Group Membership Value Type to either DN or Name.
Fallback (Default = Off)	Enables/Disables the LDAP fallback feature. When enabled, the AFS will revert to its own internal user directory if no defined users are found via the LDAP server. In this case, port access rights will then be granted as specified in the default LDAP group.
Debug (Default = Off)	This option is used to assist WTI Technical Support personnel with the diagnosis of LDAP issues.
Ping LDAP Hosts	Allows you to ping IP addresses or domain names that have been defined via the LDAP Parameters menus in order to check that a valid IP address or domain name has been entered. **Note:** *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
LDAP Group Setup	*Provides Access to a submenu that is used to define LDAP Groups as described in Section 6.3.1.12.2.*

6.3.1.12.1. Kerberos Parameters (Shared)

When Kerberos has been selected as the Bind Type, the following Kerberos parameters will be available:

Parameter (Default)	Description
Port (Default = 88)	The port number required for Active Directory communication and Kerberos.
Realm (Default = Undefined)	A set of managed nodes that share the same Kerberos database.
Key Distribution Centers (KDC1 through KDC5) (Default = Undefined)	A KDC is a single process that issues ticket-granting tickets (TGTs) for connection to the ticket-granting service in its own domain or in any trusted domain.
Domain Realms 1 through 5 (Default = Undefined)	The domain(s) over which a Kerberos authentication server has the authority to authenticate a user, host or service.

6.3.1.12.2. LDAP Group SetUp (Shared)

Once you have defined several users and passwords via your LDAP server, and assigned those users to LDAP Groups, you must then grant command and port access rights to each LDAP Group at each individual AFS.

The LDAP Group Setup link at the bottom of the LDAP Parameters menu allows you to Add new LDAP Groups, or View, Edit or Delete existing LDAP Groups. The LDAP Group Parameters menu provides access to the following parameters:

Parameter (Default)	Description
Group Name (Default = Undefined)	This name must match the LDAP Group names that you have assigned to users at your LDAP server.
Access Level (Default = User)	Sets the command access level to either Administrator, SuperUser, User or ViewOnly.
Service Access (Default; Serial Port = On, Telnet/SSH = On, Outbound Access = Off.)	Selects access methods for this LDAP Group. Determines whether members of this LDAP Group will be allowed to access the user interface via Serial Port, Telnet/SSH, Web and/or Outbound connections. **Note:** *The Outbound Telnet option is not available on WTI Power Control Products.*
Configure Circuit Access (Default = Undefined)	Select the circuits that members of this LDAP group will be allowed to control.
Configure Circuit Group Access (Default = Undefined)	Determines which Circuit Groups the members of this LDAP Group will be allowed to control. **Note:** *Prior to setting this parameter, you must first define at least one Circuit Group as described in Section 6.6.*

6.3.1.13. TACACS Parameters [Shared]

The TACACS Parameters [Shared] Menu is used to set TACACS parameters. The TACACS Parameters Menu includes the following options:

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the TACACS feature at the Network Port.
Primary Host/Address (Default = Undefined)	The IP address or domain name for your primary TACACS server.
Secondary Host/Address (Default = Undefined)	The IP address or domain name for your secondary, fallback TACACS server.
Secret Word (Default = Undefined)	The shared TACACS Secret Word for both TACACS servers.
Fallback Timer (Default = 15 Seconds)	Determines how long the unit will attempt to contact the primary TACACS Server before falling back to the secondary server.

Parameter (Default)	Description
Fallback Local (Default = Off)	Determines whether or not the AFS will fallback to its own username directory when authentication fails. When enabled, the unit will first attempt to authenticate the password via the TACACS Server. If this fails, the unit will then attempt to authenticate the password via its own internal username directory. This parameter offers three options: • **Off:** Fallback Local is disabled (Default) • **On (All Failures):** Fallback Local is enabled, and the unit will fallback to its own internal user directory when it cannot contact the TACACS Server, or when a password or username does not match the TACACS Server. • **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to its own internal user directory when it cannot contact the TACACS Server.
Authentication Port (Default = 49)	The port number for the TACACS function.
Account Management Module (Default = Disabled)	
Session Management Module (Default = Disabled)	
Service Name (Default = Undefined)	
Debug (Default = Off)	
Ping TACACS Servers	Pings IP addresses or domain names defined via the TACACS Parameters menu in order to make certain that a valid IP address or domain name have been entered. **Note:** *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands*
Default TACACS User Access	Defines default access parameters for new TACACS User Accounts as described in Section 6.3.1.13.1.

6.3.1.13.1. Default TACACS User Access (Shared)

When enabled, allows TACACS users to access the unit without first defining a TACACS user account on the AFS. When new TACACS users access the unit, they will inherit the default Access Level, Port Access and Service Access defined via the items listed below

Parameter (Default)	Description
Enable (Default = On)	Enables/disables the Default User Access function.
Access Level (Default = User)	Determines the default Access Level setting for new TACACS users. Sets the default access level for new TACACS users to "Administrator", "SuperUser", "User" or "ViewOnly."
Service Access (Default = Serial Port = On, Telnet/SSH = On, Web = On, Outbound Access = Off.)	Selects the default Service Access setting for new TACACS users. Determines whether each account will be able to access the user interface via Serial Port, Telnet/SSH or Web. In addition, the Service Access setting also determines whether each account will be able to employ the Outbound Access function.
Configure Port Access	Determines the default Port Access setting for new TACACS users.
Configure Circuit Access (Defaults; Administrator and SuperUser = All Circuits, User = Undefined, ViewOnly = Undefined)	Determine which circuits new TACACS users will be allowed to control by default.
Configure Circuit Group Access (Defaults; Administrator and SuperUser = All Circuit Groups On, User = Undefined, ViewOnly = Undefined)	Determines which circuit groups new TACACS users will be allowed to control by default. **Note:** *Prior to setting this parameter, you must first define at least one Circuit Group as described in Section 6.6.*

6.3.1.14. RADIUS Parameters [Shared]

The RADIUS Parameters [Shared] Menu is used to set RADIUS parameters for both IPv4 and IPv6 protocols.

Notes:

- *For information regarding setting up the AFS for RADIUS login support via CLI, please refer to the WTI.com Knowledge Base.*
- *For information on RADIUS and Two Factor Authentication, please refer to the WTI.com Knowledge Base.*

The RADIUS Configuration Menu offers the following options:

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the RADIUS feature at the Network Port(s.)
Primary Host/Address IPv4 (Default = Undefined)	The IPv4 format address or domain name for your primary RADIUS server.
Primary Host/Address IPv6 (Default = Undefined)	The IPv6 format address or domain name for your primary, RADIUS server.
Primary Secret Word (Default = Undefined)	Defines the Secret Word for the primary RADIUS server.
Secondary Host/Address IPv4 (Default = Undefined)	The IPv4 format address or domain name for your secondary, fallback RADIUS server.
Secondary Host/Address IPv6 (Default = Undefined)	The IPv6 format address or domain name for your secondary, fallback RADIUS server.
Secondary Secret Word (Default = Undefined)	Defines the Secret Word for the secondary RADIUS server.
Fallback Timer (Default = 3 Seconds)	Determines how long the AFS will continue to attempt to contact the primary RADIUS Server before falling back to the secondary RADIUS Server.
Fallback Local (Default = Off)	Determines whether or not the AFS will fallback to its own password/username directory when an authentication attempt fails. When enabled, the AFS will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the AFS will then attempt to authenticate the password by checking its own internal username directory. This parameter offers three options: • **Off:** Fallback Local is disabled. • **On (All Failures):** Fallback Local is enabled, and the unit will fallback to its own internal user directory when it cannot contact the Radius Server, or when a password or username does not match the Radius Server. • **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to its own internal user directory when it cannot contact the Radius Server.

Parameter (Default)	Description
Retries (Default = 3)	Determines how many times the AFS will attempt to contact the RADIUS server. Note that this parameter applies to both the Primary RADIUS Server and Secondary RADIUS Server.
Authentication Port (Default = 1812)	The Authentication Port number for the RADIUS function.
Accounting Port (Default = 1813)	The Accounting Port number for the RADIUS function.
OneTime Auth (Default = Off)	This feature should be enabled when using Two Factor Authentication with the One Time Password scheme enabled. When enabled, the One Time Password will be valid for the time specified under the OneTime Auth Timer parameter.
OneTime Auth Timer (Default = 5 Minutes)	When the OneTime Auth parameter is enabled, this parameter determines how long (in minutes) the One Time Password will be valid.
Session Module Type	Enables/disables queries of session parameters.
Ping RADIUS Servers	Allows you to ping IP addresses or domain names defined via the RADIUS Parameters menu in order to make certain that a valid IP address or domain name has been entered. **Note:** *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
Default RADIUS User Access	Defines default access parameters for new RADIUS User Accounts as described in Section 6.3.1.14.1.

6.3.1.14.1. Default RADIUS User Access (Shared)

When enabled, allows RADIUS users to access the unit without first defining a RADIUS user account on the AFS. When new RADIUS users access the unit, they will inherit the default Access Level, Port Access and Service Access defined via the items listed below

Parameter (Default)	Description
Enable (Default = On)	Enables/disables the Default User Access function.
Access Level (Default = User)	Determines the default Access Level setting for new RADIUS users. Sets the default access level for new RADIUS users to "Administrator", "SuperUser", "User" or "ViewOnly."
Service Access (Defaults; Serial Port = On, Telnet/SSH = On, Web = On, RESTful API = On, Outbound = Off)	Selects the default Service Access setting for new RADIUS users. Determines whether each account will be able to access the user interface via Serial Port, Telnet/SSH or Web. In addition, the Service Access setting also determines whether each account will be able to employ the Outbound Access function.
Configure Port Access	Determines the default Port Access setting for new RADIUS users.
Configure Circuit Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	Determine which circuits new RADIUS users will be allowed to control by default.
Configure Circuit Group Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	This item is used to determine which circuit groups new RADIUS users will be allowed to control by default. **Note:** *Prior to setting this parameter, you must first define at least one Circuit Group as described in Section 6.6.*

6.3.1.14.2. Dictionary Support for RADIUS

The RADIUS dictionary file can allow you to define a user and assign command access rights and port access rights from a central location.

The RADIUS dictionary file, “dictionary.wti” can be found under the “downloads” tab on the product information page at wti.com. To install the dictionary file on your RADIUS server, please refer to the documentation provided with your server; some servers will require the dictionary file to reside in a specific directory location, others will require the dictionary file to be appended to an existing RADIUS dictionary file.

> **Note:** *For information regarding installing the WTI RADIUS Dictionary to FreeRadius, please refer to the WTI.com Knowledge Base.*

The WTI RADIUS dictionary file provides the following commands:

- **`WTI-Super`** - Sets the command access level for the user. This command provides the following arguments:
  - `0` = ViewOnly
  - `1` = User
  - `2` = SuperUser
  - `3` = Administrator

  For example, in order to set command access level to “SuperUser”, the command line would be:

  ```
  WTI-Super=”2”
  ```

- **`WTI-Port-Access`** - Determines which port(s) the user will be allowed to access. This command provides an argument that consists of an 8 character string, with one character for each Serial Port. The following options are available for each port:
  - `0` = Off (Deny Access)
  - `1` = On (Allow Access)

  For example, to allow access to Serial Ports 1, 2, 3, 5 and 8, the command line would be:

  ```
  WTI-Port-Access=”11101001”
  ```

6.3.1.15. Ping Parameters (Ping Access) [eth0] IPv4

Configures the AFS unit's response to ping commands at the Ethernet Port (eth0.)

Note: *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

Parameter (Default)	Description
Ping Access (Default = Allow All)	This parameter offers three options: • **Allow All Pings:** • **Block All Pings:** • **Limited:** Blocks all pings, except for up to four permitted IP addresses, defined via the "Allowed" parameters.
Allowed IP Addresses 1 through 4 (Default = Undefined)	When "Limited" Ping Access is selected, these four parameters are used to determine which IP addresses will be allowed to ping the AFS.

6.3.1.16. Email Messaging [IPv4]

The Email Messaging (IPv4) menu is used to define IPv4 parameters that will be used for email communication sent from the Ethernet Port (eth0). The AFS can be configured to automatically send email to notify administrators when alarms are generated, and also when other events occur. The Email Messaging (IPv4) menu offers the following options:

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables the Email Messaging feature. When disabled, the AFS will not be able to send email messages when an alarm is generated.
SMTP Server (Default = Undefined)	Defines the address of your SMTP Email server.
Port Number (Default = 25)	Selects the TCP/IP port number that will be used for email connections.
Use TLS (Default = On)	Enables/disables Transport Level Security (TLS) and selects either UseTLS or UseSTARTTLS.
Domain (Default = Undefined)	The domain name for your email server. **Note:** *In order to use domain names, you must first define Domain Name Server parameters as described in Section 7.3.1.6.1.*
Auth Type (Default = None)	The Authentication type; the AFS allows you to select None, Plain, Login, or CRAM-MD5 Authentication.
User Name (Default = Undefined)	The User Name that will be entered when logging into your email server.
Password (Default = Undefined)	The password that will be used when logging into your email server.
From Name (Default = Undefined)	The name that will appear in the “From” field in email sent by the AFS.
From Address (Default = Undefined)	The email address that will appear in the “From” field in email sent by the AFS.
To Address (Default = Undefined)	These prompts are used to defined up to three address that will receive email messages generated by the AFS. When Alarm Configuration parameters are selected, you may then designate these addresses as recipients for email messages generated by alarms.
Send Test Email	Sends a test email, using the parameters currently defined for the Email configuration menu.

6.3.2. Network Configuration [eth0] IPv6 Menus

The Network Configuration [eth0] IPv6 Menus are used to define network communication parameters that apply only to IPv6 protocol access to the Ethernet Port (eth0.)

6.3.2.1. Network Parameters [eth0] IPv6

This menu is used to assign the IP Address, Subnet Mask and other IPv6 parameters for the Ethernet Port (eth0).

Parameter (Default)	Description
IP Address (Default = Undefined)	The IPv6 format address for the Ethernet Port, eth0. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the AFS via the CLI.*
Subnet Prefix (Default = Undefined)	Defines the IPv6 Subnet Prefix.
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the Ethernet Port, eth0. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must use the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol. When enabled, the AFS will perform a DHCP request. In the CLI, the MAC address is listed on the Network Status Screen. **Notes:** • *Prior to configuring this feature, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the AFS.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the AFS via the CLI.*

6.3.2.2. IP Tables IPv6

The IP Tables menu allow the AFS to restrict unauthorized IP addresses from establishing inbound connections to the unit. If you wish to restrict access to the AFS, you can employ the IP Tables menu to define a firewall that determines which IP addresses will be allowed to access the user interface and which IP addresses will be denied.

To define the firewall, use Linux syntax routing commands to determine which IP address(es) will be allowed access and which IP address(es) will be denied. In most cases, the IP Tables should allow access to administrators and deny access to everybody else.

> **Note:** *For instructions regarding setting up IP Tables, please refer to the WTI.com Knowledge Base.*

6.3.2.3. Static Route [eth0] IPv6

The Static Route menu allows you to define Linux routing commands that will be automatically executed each time that a user accesses the user interface via the Ethernet Port (eth0.)

6.3.2.4. DNS Selection Menu [eth0 / IPv6]

The DNS Selection option provides access to two submenus that are used to define DNS and DDNS parameters.

6.3.2.4.1. DNS Servers (Shared)

The DNS Parameters menu is used to select IP addresses for Domain Name Servers for the Ethernet Port [eth0]. When web and network addresses are entered, the Domain Name Server interprets domain names (e.g., www.wti.com), and translates them into IP addresses. Note that if you don't define at least one DNS server, then IP addresses must be used, rather than domain names.

The Domain Name Server menu includes a Ping Test feature that allows you to ping the IP addresses for each user-defined domain name server.

> **Note:** *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

6.3.2.4.2. DDNS Parameters [eth0] IPv6

The DDNS Parameters menu is used to select parameters and define hosts for Dynamic DNS services for IPv6 communication via the Ethernet Port (eth0.) The DDNS Parameters menu includes the following parameters:

Parameter (Default)	Description
Services (Default = None)	Sets the service type to either Dyn or None.
Host Name (Default = Undefined)	The IP Address for the DDNS Service.
Username (Default = Undefined)	The Username for your DDNS Account.
Password (Default = Undefined)	The Password for your DDNS Account.
Maximum Update Times (Default = Every 1 Hour)	Determines how often the AFS will ping the DDNS host address.

6.3.2.5. Negotiation [eth0] IPv4/IPv6

This parameter can be used to solve synchronization problems when the AFS negotiates IPv6 communication parameters with another device via the Ethernet Port (eth0.).

Notes:

- *If the other device is set for automatic negotiation, then the AFS unit's Negotiation parameter should also be set to Auto.*
- *If the other device is not set for automatic negotiation, then the AFS unit's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*

6.3.2.6. Web Selection [eth0] IPv4/IPv6

This link provides access to the Web Access Menu, SSL Certificates Menu and Import Wildcard Certs Menu for both IPv4 and IPv6 access via the Ethernet Port (eth0.)

6.3.2.6.1. Web Access [eth0] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the Ethernet Port (eth0.)

> **Note:** *For further information regarding web security, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
HTTP Access (Default = Off)	Enables/disables the Web Browser Interface. When disabled, users will not be allowed communicate with the unit via the Web Browser Interface.
HTTP Port (Default = 80)	Selects the TCP/IP port number used for HTTP connections.
HTTPS Access (Default = Off)	Enables/disables HTTPS communication.
HTTPS Port (Default = 443)	Selects the TCP/IP port number that will be used for HTTPS connections.
Harden Web Security (Default = Medium)	Offers three different Web Security settings: • **Off:** All SSL protocols are enabled. (Allows compatibility with older browsers.) • **Medium:** Only SSLv3/TLS1.x Protocols and MEDIUM/HIGH ciphers are enabled. • **High:** Only TLS1.x Protocol and HIGH ciphers enabled.
TLS Mode (Default = TLSv1.1/TLSv1.2)	Selects the TLS version that will be used. This parameter can select either TLSv1 only, both TLSv1.1 and TLSv1.2 or TLSv1.2 Only.
Trace Method (Default = Off)	Enables/disables the Web Trace Method.
OCSP Stapling (Default = Off)	Enables/disables Online Certificate Status Protocol (OCSP) Stapling (also known as the TLS Certificate Status Request.)

6.3.2.6.2. SSL Certificates [eth0]

Defines SSL Certificate parameters for the Ethernet Port (eth0.)

Notes:

- *For instructions regarding installing SSL certificates via the CLI, please refer to the WTI.com Knowledge Base.*
- *For instructions regarding installing SSL certificates via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
Common Name (CN) (Default = Undefined)	The Common Name is typically composed of Host + Domain Name (e.g., "www.yoursite.com".) SSL Certificates are specific to the Common Name to which they have been issued at Host level. The Common Name must be the same as the Web address you will access when connecting to the secure site.
State or Province (S) (Default = Undefined)	The full name of the State or Province where your organization is registered to operate by national, state or local authorities.
Locality (L) (Default = Undefined)	The name of the town or city where your organization is located.
Country Code (C) (Default = Undefined)	The two character, ISO-3166 Country Code for the nation where your organization is located.
Email Address (Default = Undefined)	An email address that can be used to contact the administrator of the certificate.
Organization (O) (Default = Undefined)	The legal name under which your company or organization is registered.
Organizational Unit (OU) (Default = Undefined)	The branch of your company that is requesting the certificate (e.g., "Tech Support" or "Human Resources".)
SAN Options (Default = Undefined)	Determines whether the SAN Certificate will be hidden or displayed. The Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with the security certificate using the subjectAltName field. These values are called "Subject Alternative Names" (SANs). Names can include: DNS names, IP addresses, Email addresses and URLs.

6.3.2.6.3. Import Wildcard Certs [eth0] (SSL Certificate Import)

The Import Wildcard Certs Menu (SSL Certificate Import) is used to import a private key, a signed certificate and optionally a CA Intermediate Certificate for the Web server for the Ethernet Port (eth0]. The Import Wildcard Certs menu includes the following parameters:

Notes:

- *For instructions regarding installing SSL certificates via the CLI, please refer to the WTI.com Knowledge Base.*
- *For instructions regarding installing SSL certificates via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*

Parameter (Default)	Description
Private Key	An alphanumeric key, issued by the Certification Authority.
Signed Certificate	The file that the Certification Authority returns to you, after you have submitted your Certificate Signing Request (CSR).
Show Intermediate CA Certificate	Shows or hides the Intermediate CA Certificate.

6.3.2.7. Syslog Parameters IPv6

Defines parameters for the Syslog Client for IPv6 communication. This menu can be used to define up to four Syslog Clients and to install certificates for each client

Parameter (Default)	Description
SYSLOG Address (Default = Undefined)	The external Syslog Server IP Address and corresponding UDP Syslog Server Port number.
Transport (Default = UDP)	The transport protocol used for the Syslog server.
Secure Syslog (SSL/TLS) (Default = Off)	Enables/disables Secure Syslog when TCP transport is selected.
Secure Syslog Verify Server (Default = On)	
Install Certificate	Installs the Syslog Certificate for each of four available Syslog Clients.
Ping Syslog Servers	Pings the IP addresses for each defined Syslog Client in order to check that a valid IP address. **Note:** *In order for the Ping Syslog Servers feature to function, your network and/or firewall must be configured to allow ping commands.*

6.3.2.8. SNMP Parameters [eth0] IPv6

This menu is used to select IPv6 format access parameters for the SNMP feature at the Ethernet Port (eth0.)

> **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the AFS unit's User Directory, control power and toggle switching and display unit status via SNMP, as described in Appendix G.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling at the Ethernet Port (eth0.). **Note:** *This parameter applies only to external SNMP polling of the AFS. It does not effect the ability of the AFS to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the Ethernet Port (eth0) will respond to. For example, if this item is set to V3, then clients who attempt to contact the AFS via eth0 using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the Ethernet Port (eth0.) This controls the ability to access configuration functions and invoke switching commands. When Enabled, you will not be able to change configuration parameters or invoke other commands when you contact the AFS unit's Ethernet Port (eth0) via SNMP. **Note:** *In order to define user names for the AFS via your SNMP client, the Read Only feature must be disabled. When the Read Only feature is enabled, you will not be able to issue configuration commands to the unit via SNMP.*
System Name (Default = Undefined)	The host name of the AFS.
SNMP Contact (Default = Undefined)	The name of the administrator responsible for SNMP issues.
SNMP Location (Default = Undefined)	The location of the SNMP Server.
Read Only Community (Default = Public)	Note that this parameter is not available when the SNMP Version is set to V3.
Read/Write Community (Default = Public)	Note that this parameter is not available when the SNMP Version is set to V3.

6.3.2.8.1. SNMP V3 Users (eth0 / IPv6)

When the SNMP version has been set to V3, the following parameters can be defined via the V3 Users menu.

Parameter (Default)	Description
SNMPv3 User Name (Default = Undefined)	Sets the User Name for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Authentication / **Privacy** (Default = Auth/noPriv)	Configures the Authentication and Privacy features for SNMPv3 communication. Two options are available: : • **Auth/noPriv:** An SNMPv3 username and password will be required at log in, but encryption will not be used. • **Auth/Priv:** An SNMPv3 username and password will be required at log in, and all messages will be sent using encryption. **Notes:** • *The Authentication / Privacy item is not available when the Version parameter is set to V1/V2.* • If the Version Parameter is set to V1/V2/V3 (all) and Authentication / Privacy parameter is set to "Auth/Priv", then only V3 data will be encrypted. • The AFS supports DES encryption, but does not currently support the AES protocol. • The AFS does not support "noAuth/noPriv" for SNMPv3 communication.
SNMPv3 Authentication Password (Default = Undefined)	Sets the Authentication Password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Authentication Protocol (Default = MD5)	This parameter determines which authentication protocol will be used. AFS units support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the AFS must match the protocol that your SNMP client will use when querying the AFS.* • *The Authentication Protocol option is not available when the Version parameter is set to V1/V2.*
SNMPv3 Privacy Password (Default = Undefined)	Sets the Privacy Password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2.
Privacy Protocol (Default = DES)	(SNMPv3 Only) Selects AES or DES encryption support.

6.3.2.9. SNMP Trap Parameters [IPv6]

This menu is used to select IPv6 parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Appendix F.

Parameter (Default)	Description
SNMP Managers 1 through 4 (Default = Undefined)	The IPv6 Addresses for the SNMP Managers. **Note:** *In order to enable the SNMP Trap feature, you must define at least one SNMP Manager.*
Trap Community (Default = Public)	This field is used to enter the key that allows access to the AFS unit's SNMP Alarm Reporting.
Trap Version (Default = V1)	The assigned security level for SNMP traps.
V3 Trap Engine ID (Default = Undefined)	The V3 SNMP agent's unique identifier.

6.3.2.10. Ping Parameters (Ping Access) [eth0] IPv6

Configures the AFS unit's response to ping commands at the Ethernet Port (eth0.)

> **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

Parameter (Default)	Description
Ping Access (Default = Allow All)	This parameter offers three options: • **Allow All Pings:** • **Block All Pings:** • **Limited:** Blocks all pings, except for up to four permitted IP addresses, defined via the "Allowed" parameters.
Allowed IP Addresses 1 through 4 (Default = Undefined)	When "Limited" Ping Access is selected, these four parameters are used to determine which IP addresses will be allowed to ping the AFS.

6.3.2.11. Email Messaging [IPv6]

The Email Messaging (IPv6) menu is used to define IPv6 parameters that will be used for email communication sent from the Ethernet Port (eth0). The AFS can be configured to automatically send email to notify administrators when alarms are generated, and also when other events occur. The Email Messaging (IPv4) menu offers the following options:

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables the Email Messaging feature. When disabled, the AFS will not be able to send email messages when an alarm is generated.
SMTP Server (Default = Undefined)	Defines the address of your SMTP Email server.
Port Number (Default = 25)	Selects the TCP/IP port number that will be used for email connections.
Use TLS (Default = On)	Enables/disables Transport Level Security (TLS) and selects either UseTLS or UseSTARTTLS.
Domain (Default = Undefined)	The domain name for your email server. **Note:** *In order to use domain names, you must first define Domain Name Server parameters.*
Auth Type (Default = None)	The Authentication type; the AFS allows you to select None, Plain, Login, or CRAM-MD5 Authentication.
User Name (Default = Undefined)	The User Name that will be entered when logging into your email server.
Password (Default = Undefined)	The password that will be used when logging into your email server.
From Name (Default = Undefined)	The name that will appear in the “From” field in email sent by the AFS.
From Address (Default = Undefined)	The email address that will appear in the “From” field in email sent by the AFS.
To Address (Default = Undefined)	These prompts are used to defined up to three address that will receive email messages generated by the AFS. When Alarm Configuration parameters are selected, you may then designate these addresses as recipients for email messages generated by alarms.
Send Test Email	Sends a test email, using the parameters currently defined for the Email configuration menu.

6.4. User Configuration

In addition to providing basic log-in security, User Accounts also limit the features and capabilities that each user is allowed to access. The privileges assigned to each User Account can limit access to configuration functions, service access and determine which circuits the user will be allowed to control. The User Configuration menu allows administrators to create new user accounts, edit or review existing user accounts and delete user accounts that are no longer needed.

6.4.1. Access Levels

The Access Level assigned to each User Account provides a simple means to control each account's access to configuration and command functions. The AFS offers four different Access Levels for User Accounts:

- **Administrator:**Administrator accounts are allowed to invoke all configuration and operation commands, view all status screens, and control all circuits present on the AFS.
- **SuperUser:** SuperUser accounts are allowed to invoke all switching commands and view all status screens. SuperUser accounts can view configuration menus, but are not allowed to change parameters. SuperUsers are granted access to all circuits present on the AFS.
- **User:** User accounts are not allowed to access configuration menus, and are only allowed to control circuits that are specifically permitted by the account.
- **ViewOnly:** ViewOnly accounts are allowed to view Status Menus, but are not allowed to invoke circuit switching commands, view configurations menus or change parameters. ViewOnly accounts can display the Circuit Status screen, but can only view the status of circuits allowed by the account.

Section 10.3 summarizes command access for all four access levels.

In the default state, the AFS includes one predefined account that provides access to Administrator commands and allows to control of all switched circuits. The default username for this account is super (lowercase), and the password for the account is also super.

Notes:

- *It is recommended that when initially setting up the unit, a new user account with Administrator access should be created, and the default "super" account should then be deleted.*
- *If the AFS is reset to default parameters, all User Accounts will be cleared, and the default "super" account will be restored.*

6.4.2. Adding Accounts

The "Add User" option allows you to create new accounts. Note that the Add User option is only available when you have accessed the user interface using a password that permits Administrator Level commands. The Add User Menu can define the following parameters for each new account:

Parameter (Default)	Description
User Name (Default = Undefined)	Up to 32 characters long, and cannot include spaces or non-printable characters. Duplicate usernames are not allowed.
Password (Default = Undefined)	Five to 16 characters long, and cannot include spaces or non-printable characters. Note that passwords are case sensitive.
Access Level	Determines which functions and capabilities this account will be allowed to access. This Access Level can be set to "Administrator", "SuperUser", "User" or "ViewOnly."
Service Access (Default = User)	Determines whether this account will be able to access the user interface via Serial Port, Telnet/SSH, Web or RESTful API. Note: *The Service Access Parameter is only used to select permitted access services for an individual user account. To separately enable/disable all SSH/Telnet Access for the AFS, please refer to Appendix D.*
Callback Phone Numbers (Default = Undefined)	Assigns up to five phone numbers that can be called when this account attempts to access the user interface via dial-up modem, and the Callback Security Function has been enabled . **Notes:** • *If a Callback Phone Number is not defined, then Callbacks will not be performed for this user.* • *If a Callback Phone Number is not defined for a given user, and the Callback Security feature is configured to use either of the "On - Callback" options, then this user will be granted immediate access to the user interface via modem.* • *If a Callback Phone Number is not defined for a given user, and the Callback Security feature is configured to use the "On - Callback ONLY" option, then this user will not be able to access the user interface via Modem.* • *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback phone number will be allowed to access the user interface without callback verification.*
Authorized Keys (Default = Undefined)	Assigns SSH Authorization Key(s) and associated key name(s) to the user account. When a valid authorization key is assigned the user will be able to access the user interface without entering a password.

Parameter (Default)	Description
Configure Port Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	Determines whether or not this account will be allowed to access the Serial Setup Port. **Notes:** • *Administrator and SuperUser level accounts will always provide access to the Serial Setup Port.* • *The Port Access parameter is also used to grant or deny user access to the internal modem port (if present.)*
Configure Circuit Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	Determines which circuit(s) this account will be allowed to control. **Notes:** • *Administrator and SuperUser level accounts will always have access to all circuits.* • *ViewOnly accounts are allowed to display the On/Off status of circuits, but are limited to the circuits specified by the account. ViewOnly accounts are not allowed to invoke circuit switching commands.*
Configure Circuit Group Access (Defaults; Administrator & SuperUser = All Groups On, User = Undefined, ViewOnly = Undefined)	Determines which Circuit Groups this account will be allowed to control. **Notes:** • *In order to use this feature, Circuit Groups must first be defined as described in Section 6.6.* • *Administrator and SuperUser level accounts will always have access to all circuit groups.* • *ViewOnly accounts are allowed to display the On/Off status of circuit groups, but are limited to the circuit groups specified by the account. ViewOnly accounts are not allowed to invoke switching and toggle commands.*

6.4.3. Viewing User Accounts

The “View User” option allows you to view details about each account. The View User function is only available when you have accessed the user interface using a password that permits Administrator Level commands. The View User option will not display account user passwords.

6.4.4. Modifying User Accounts

The “Modify User” function allows you to edit existing user accounts. Note that the Modify User function is only available when you have accessed the user interface using a password that permits Administrator Level commands.

6.4.5. Deleting User Accounts

This “Delete User” function can be employed to delete individual user accounts. Note that the Delete User function is only available when you have accessed the user interface using a password that permits Administrator Level commands.

Notes:

- *Deleted accounts cannot be automatically restored.*
- *The AFS allows you to delete the default “super” account, which is included to permit initial access to the user interface. Before deleting the “super” account, make certain to create another account that permits Administrator Access. If you do not retain at least one account with Administrator Access, you will not be able to invoke Administrator level commands.*

6.5. VPN Options

The VPN Options menu is used to set up Site-to-Site communication via IPsec (Client Site-to-Site), OpenVPN (Client Site-to-Site) or IPSec Server (Client Site-to-Site.)

6.5.1. IPsec (Client Site-to-Site) Options

To set IPsec (Client Site-to-Site) Parameters, click on IPsec (Client Site-to-Site), select the desired Tunnel IPsec Client from the resulting submenu, then click on Choose Tunnel to define the following parameters. For more information, please refer to the WTI.com Knowledge Base.

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables communication via IPsec Client Site-to-Site.
Tunnel Name (Default = TUNNEL_IPSEC_CLIENT_1)	Displays the name of the currently selected Tunnel IPsec Client.
Security (Default = PKI (X.509 Certificates))	Sets Security to PKI (X.509 Certificates) or Pre-Shared Secret (Static Key File.)
Authentication Type (Default = ESP)	Sets the Authentication Type to either ESP or AH.
Left Address (Default = Undefined)	
Left ID (Default = Undefined)	
Left Subnet (Default = Undefined)	
Right Address (Default = Undefined)	
Right ID (Default = Undefined)	
Right Subnet (Default = Undefined)	
Tunnel Options	Tunnel Options 1 - 15.
EAP Users	EAP Users 1 - 4.
Server Certificate (Default = Undefined)	
Client Certificate (Default = Undefined)	
Client Key File (Default = Undefined)	
Server CA Certificate (Default = Undefined)	

6.5.2. OpenVPN (Client Site-to-Site) Options

To set OpenVPN (Client Site-to-Site) Parameters, click on OpenVPN (Client Site-to-Site), select the desired Tunnel OpenVPN Client from the resulting submenu, then click on Choose Tunnel to define the following parameters. For more information, please refer to the WTI.com Knowledge Base.

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables communication via OpenVPN Client Site-to-Site.
Tunnel Name (Default = TUNNEL_ OPENVPN_CLIENT_1)	Displays the name of the currently selected Tunnel OpenVPN Client.
Security (Default = PKI (X.509 Certificates))	Sets Security to PKI (X.509 Certificates,) Pre-Shared Secret (Static Key File) or Unified OpenVPN Profile (Custom Configuration.)
Driver (Default = TUN-IP)	Sets the Driver to either TUN-IP or TAP-IP.
Protocol (Default = UDP)	Sets the Protocol to either UDP or TCP.
Compression (Default = Enable LZO Compression)	Enables/disables LZO Compression.
Primary Host/Address (Default = Undefined)	The Primary Host computer with the other side of the Open VPN connection
Primary Host Port (Default = Undefined)	The Primary Host computer Port with the other side of the Open VPN connection
Secondary Host/Address (Default = Undefined)	The Secondary Host computer Port with the other side of the Open VPN connection
Secondary Host Port (Default = Undefined)	The Secondary Host computer Port with the other side of the Open VPN connection
Tunnel Options	
EAP Users	
Server Certificate (Default = Undefined)	
Client Certificate (Default = Undefined)	
Client Key File (Default = Undefined)	

6.5.3. IPSec Server (Client Site-to-Site) Options.

To set IPsec Server (Client Site-to-Site) Parameters, click on IPsec Server (Client Site-to-Site), select the desired Tunnel IPsec Server from the resulting submenu, then click on Choose Tunnel to define the following parameters. For more information, please refer to the WTI.com Knowledge Base.

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables communication via IPsec Server Client Site-to-Site.
Tunnel Name (Default = TUNNEL_IPSEC_SERVER_1)	Displays the name of the currently selected Tunnel IPsec Server.
Security (Default = PKI (X.509 Certificates))	Sets Security to PKI (X.509 Certificates) or Pre-Shared Secret (Static Key File.)
Authentication Type (Default = ESP)	Sets the Authentication Type to either ESP or AH.
Left Address: (Default = Undefined)	
Left ID (Default = Undefined)	
Left Subnet (Default = Undefined)	
Right Address (Default = Undefined)	
Right ID (Default = Undefined)	
Right Subnet (Default = Undefined)	
Tunnel Options	
EAP Users	
Server Certificate (Default = Undefined)	
Client Certificate (Default = Undefined)	
Server CA Certificate (Default = Undefined)	

6.6. The Circuit Group Directory

The Circuit Group Directory allows you to designate groups of circuits that are dedicated to a similar function, and will most likely be switched all at the same time or controlled by the same user or department. When two or more switched circuits are assigned to a Circuit Group, this allows you to direct commands to all circuits in the group, without addressing each circuit individually.

The Circuit Group Directory is only available when you have logged into the user interface using an account that permits Administrator commands. The Circuit Group Directory allows administrators to create/add new Circuit Groups, display or edit existing Circuit Groups, or delete Circuit Groups that are not needed.

6.6.1. Adding Circuit Groups

The “Add Circuit Group” option allows you to create new Circuit Groups and assign circuit access rights to each group. Note that the Add Circuit Group function is only available when you have accessed the user interface using a password that permits Administrator Level commands. The Add Circuit Group Menu can be used to define the following parameters:

Parameter (Default)	Description
Circuit Group Name (Default = Undefined)	Assigns a descriptive name to the Circuit Group.
Circuit Access (Default = Undefined)	Determines which circuits will be included in this Circuit Group.

6.6.2. Viewing Circuit Groups

The “View Circuit Group” option allows you to view the configuration of each Circuit Group. Note that the View Circuit Group function is only available when you have accessed the user interface using a password that permits Administrator Level commands.

6.6.3. Modifying Circuit Groups

The “Modify Circuit Group” function allows you to edit existing Circuit Groups. Note that this function is only available when you have accessed the user interface using a password that permits Administrator Level commands.

6.6.4. Deleting Circuit Groups

This function is used to delete individual Circuit Groups. Note that this function is only available when you have accessed the user interface using a password that permits Administrator Level commands.

Note: *Deleted Circuit Groups cannot be automatically restored.*

6.7. Circuit Parameters

The Circuit Parameters Menu is used to define Circuit Names and other parameters for each of the Switched Circuits. Note that this function is only available when you have accessed the user interface using a password that permits Administrator Level commands. The Circuit Parameters Menu allows you to define the following:

Parameter (Default)	Description
Name (Common)	This item can be used to assign a descriptive name to each switched circuit.
Name (A)	
Name (B)	
Default (Default = A)	The Default A/B setting for each circuit.

6.8. Ping No Answer Configuration

The Ping-No-Answer function can be used to automatically switch one or more circuit modules when an attached device fails to respond to a Ping Command. In addition, the Ping-No-Answer function can also be configured to send an email, text message, Syslog Message or SNMP Trap to notify you whenever a Ping-No-Answer Action occurs.

To set up a Ping-No-Answer Profile, you must access command mode using a password that permits Administrator level commands. In the Text Interface, type **/PNA** and press **[Enter]** to access the Ping-No-Answer Configuration menu and then select the desired option from the resulting submenu. In the Web Browser Interface, the Ping-No-Answer Configuration menu is accessed via the Configuration link on the left hand side of the screen.

The Ping-No-Answer Configuration menu allows you to create new Ping-No-Answer triggers, edit or view existing Ping-No-Answer triggers, or delete existing Ping-No-Answer triggers.

> **Note:** *In order for the Ping-No-Answer feature to work properly, your network and/or firewall as well as the device at the target IP address must be configured to allow ping commands.*

6.8.1. Adding Ping-No-Answer Triggers

Up to 54 Ping-No-Answer Triggers can be defined. The Add Ping-No-Answer menu offers the following parameters:

Parameter (Default)	Description
IP Address or Domain Name (Default = Undefined)	The IP address or Domain Name for the device that you wish to Ping. When the device at this address fails to respond to the Ping command, the AFS will switch the selected Circuit(s). **Note:** *In order to use domain names, DNS Server parameters must first be defined as described in Section6.3.1.6.1.*
Protocol (Default = IPv4)	Selects an IPv4 format IP Address or an IPv6 format IP Address. Both an IPv4 and an IPv6 format IP Address may be defined.
Ping Interval (Default = 60 Seconds)	Determines how often the Ping command will be sent to the selected IP Address. The Ping Interval can be any whole number, from 1 to 3,600 seconds. **Note:** *If the Ping Interval is set lower than 20 seconds, it is recommended to define the "IP Address or Domain Name" parameter using an IP Address rather than a Domain Name. This ensures more reliable results in the event that the Domain Name Server is unavailable.*
Interval After Failed Ping (Default = 10 Seconds)	Determines how often the Ping command will be sent after a previous Ping command receives no response.
Ping Delay After PNA Action (Default = 15 Minutes)	Determines how long the AFS will wait to send additional Ping commands, after Ping-No-Answer Switching has been initiated. This option is used to allow time for a device to fully "wake up" after Ping-No-Answer Switching before attempting to Ping the device again.

Parameter (Default)	Description
Consecutive Failures (Default = 5)	Determines how many consecutive failures to respond to a Ping command must be detected in order to initiate Ping-No-Answer Switching.
Toggle (Default = No)	Enables/Disables the Ping-No-Answer Switching function for the specified IP address. When disabled, the AFS will not switch the specified circuit(s) or circuit group(s) when a Ping-No-Answer event is detected. However, the AFS will continue to notify you via Email, Syslog Message and/or SNMP Trap, providing that parameters for these functions have been defined and the Ping-No-Answer alarm has been enabled. **Notes:** • *In order for Email/Text Message Notification to function, you must first define Email/Text Message parameters.* • *In order for Syslog Message Notification to function, you must first define a Syslog Address* • *In order for SNMP Trap Notification to function, you must first define SNMP parameters.*
PNA Action (Default = Continuous Alarm))	Determines how the AFS will react when the IP address fails to respond to a ping: • **Continuous:** The AFS will continuously switch the specified circuit(s) and send notification until the IP address responds and the Ping-No-Answer is cleared • **Single:** The AFS will switch the specified circuit(s) or circuit group(s) and send notification only once each time Ping-No-Answer Switching is initially triggered.) • **Recover:** If the target device fails to respond, the AFS will continue to ping the target device. If the target device eventually responds, the AFS will then switch the specified circuit(s) or group(s) to their original A/B status.
Select Circuits (Default = Undefined)	Determines which circuit(s) will be switched when the IP address for this Ping-No-Answer operation does not respond to a Ping command.
Select Circuit Groups (Defaults = Undefined)	Determines which Circuit Group(s) will be switched when the IP address for this Ping-No-Answer operation does not respond to a Ping command. **Note:** *Prior to setting this parameter, you must first define at least one Circuit Group as described in Section 6.6.*

6.8.1.1. Viewing Ping-No-Answer Profiles

After you have defined one or more Ping-No-Answer profiles, you can review the parameters selected for each profile using the View Ping-No-Answer function. In order to view the configuration of an existing Ping-No-Answer profile, you must access the user interface using a password that allows Administrator level commands.

6.8.1.2. Modifying Ping-No-Answer Profiles

After you have defined a Ping-No-Answer profile, you can modify the configuration of the profile using the Modify Ping-No-Answer feature. In order to modify the configuration of an existing Ping-No-Answer profile, you must access the user interface using a password that allows Administrator level commands.

6.8.1.3. Deleting Ping-No-Answer Profiles

After you have defined one or more Ping-No-Answer profiles, you can delete profiles that are no longer needed using the Delete Ping-No-Answer feature. In order to delete an existing Ping-No-Answer profile, you must access the user interface using a password that allows Administrator level commands.

6.9. Alarm Configuration

When properly configured, the AFS can monitor temperature readings, ping response and a number of other factors at installation sites and log this information for future review. When any monitored condition exceeds user-defined trigger levels, the AFS can also notify support personnel via Email, Syslog Message or SNMP trap.

Notes:

- *In order to send alarm notification via email, email addresses and parameters must first be defined as described in Section 6.3.1.16. Email alarm notification can be sent for any Alarm that is properly configured and enabled.*
- *In order to send alarm notification via Syslog Message, a Syslog address must first be defined as described in Section 6.3.1.9. Once the Syslog address has been defined, Syslog Messages can be sent for any Alarm that is properly configured and enabled.*
- *In order to send alarm notification via SNMP Trap, SNMP Trap parameters must first be defined as described in Section 6.3.1.11. Once SNMP Trap Parameters have been defined, SNMP Traps can be sent for any Alarm that is properly configured and enabled.*
- *In order to access the Alarm Configuration Menus, your User Account must allow Administrator level command access.*

6.9.1. The Output Contacts

In addition to providing notification when an alarm is generated, the Over Temperature Alarms, Ping-No-Answer Alarm, Invalid Access Lockout Alarm and Monitor Input Alarm all offer the option to switch the output contacts on the Control Module AUX Connector when an alarm is triggered. The output contacts can then be used to activate an audible alarm or other device in response to these alarms.

When the Contact Output Enable parameter is enabled for any of these alarms, the Common line will be switched from the Normally Closed contact to the Normally Open contact in order to drive an attached device. Figure 6.1 below shows the location of the Normally Closed, Common and Normally Open contacts on the Control Module AUX Connector.

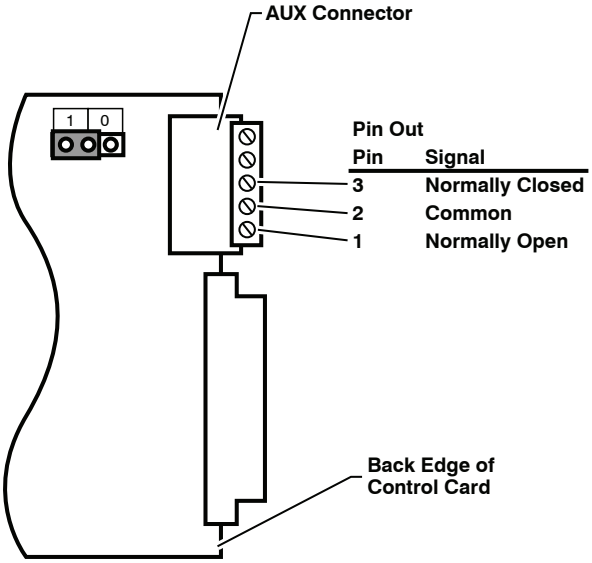

Figure 6.1: Control Module AUX Connector - Output Contacts

6.9.2. The Over Temperature Alarms

The Over Temperature Alarms can inform you when temperatures inside your equipment rack reach or exceed user specified trigger levels. There are two separate Over Temperature Alarms; the Initial Threshold alarm and the Critical Threshold Alarm.

Typically, the Initial Threshold alarm is used to provide notification when temperatures reach a point where you might want to investigate, whereas the Critical Threshold alarm is used to provide notification when temperatures approach a level that may harm equipment or inhibit performance. The trigger for the Initial Threshold alarm is generally set lower than the Critical Threshold alarm.

Notes:

- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined as described in Section 6.3.1.16.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 6.3.1.9.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 6.3.1.11.*

Both the Over Temperature (Initial Threshold) alarm and the Over Temperature (Critical Threshold) alarm offer the following parameters:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.* • *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Alarm Set Threshold (Defaults: Initial Threshold = 110°F or 43°C, Critical Threshold = 120°F or 49°C)	The trigger level for this alarm. When temperature exceeds the Alarm Set Threshold, the AFS can send an alarm (if enabled.) **Note:** *The Alarm Set Threshold value must be greater than the Alarm Clear Threshold value. The AFS will not allow you to define an Alarm Clear Threshold value that is higher than the Alarm Set Threshold.*

Parameter (Default)	Description
Alarm Clear Threshold (Defaults; Initial Threshold = 100°F or 38°C, Critical Threshold = 110°F or 43°C)	Determines how low the temperature must drop in order for the Alarm condition to be cancelled and for Auto Recovery (if enabled) to occur. **Note:** *The System Parameters menu is used to set the temperature format for the AFS to either Fahrenheit or Celsius.*
Resend Delay (Default = 60 Minutes)	Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt was unsuccessful.
Notify Upon Clear (Default = On)	When enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected.
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses, defined via the “Email Messaging” menu, will receive email alarm notification messages generated by this alarm. **Note:** *If Email addresses have been previously defined, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = “Alarm: Over Temperature (Initial)” or “Alarm: Over Temperature (Critical)”)	Defines the text that will appear in the “Subject” field for all email notification messages generated by this alarm.
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The severity level used to generate Syslog Messages for Alarm Log Events.
Contact Output Enable (Default = On)	Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to “On”, the Common line will be switched from the Normally Closed contact to the Normally Open contact when an Over-Temperature Alarm is generated. **Note:** *For more information on the Output Contacts, please refer to Section 6.9.1.*

6.9.3. The Ping-No-Answer Alarm

The Ping-No-Answer Alarm can provide notification when a device at a target IP address fails to respond to a ping command. When properly configured and enabled, the Ping-No-Answer Alarm can notify network administrators and support personnel when a target device appears to have malfunctioned, allowing prompt response to equipment problems that could potentially interfere with network communication.

6.9.3.1. Ping No Answer Alarm

The Ping-No-Answer Alarm can provide notification when one of the IP addresses defined via the Ping No Answer feature fails to respond to a Ping command. If the Ping No Answer alarm is triggered, the AFS can provide notification via Email, Syslog Message or SNMP Trap and also automatically switch user specified circuits.

Notes:

- *In order for the Ping-No-Answer Alarm to function, your network and/or firewall as well as the devices at the target IP addresses must be configured to allow ping commands.*
- *Prior to configuring and enabling this alarm, at least one target IP Addresses for the Ping-No-Answer Alarm must be defined.*
- *When a Ping-No-Answer condition is detected, the AFS can still switch user-selected circuit(s), and can also send an email, Syslog Message and/or SNMP trap if configured as described in this section.*
- *In order for the AFS to provide Email alarm notification, communication parameters must first be defined as described in Section 6.3.1.16.*
- *In order for the AFS to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 6.3.1.9.*
- *In order for the AFS to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled.*

To configure the Ping-No-Answer Alarm, you must access the user interface using a password that permits Administrator Level commands. Up to 54 Ping-No-Answer IP Addresses can be defined. The Add Ping-No-Answer menu allows the following parameters to be defined for each new Ping-No-Answer IP Address:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined.* • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.* • *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Power Control unit will wait to resend an email message generated by this alarm, when the initial attempt was unsuccessful.
Notify Upon Clear (Default = On)	When enabled, the WTI Power Control unit will send additional notification when the situation that caused the alarm has been corrected.
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses, (defined via the "Email Messaging" menu,) will receive the email alarm notification messages generated by this alarm. **Note:** *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Ping-No-Answer")	Defines the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm.
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The Severity level used to generate Syslog Messages for Alarm Log Events.
Contact Output Enable (Default = On)	Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated. **Note:** *For more information on the Output Contacts, please refer to Section 6.9.1.*

6.9.4. The Serial Port Invalid Access Lockout Alarm

The Serial Port Invalid Access Lockout Alarm can provide notification when the AFS has locked serial ports due to repeated, invalid attempts to access the user interface via serial port. Although the Invalid Access Lockout feature can lock the serial ports when the unit detects that the threshold for invalid access attempts has been exceeded, the Serial Port Invalid Access Lockout Alarm expands on this capability by providing notification via Email, SYSLOG message or SNMP Trap when a serial port lockout occurs.

Notes:

- *In order for this alarm to function, the Serial Setup Port must be set to "Normal" mode and Invalid Access Lockout parameters must be configured and enabled.*
- *The AFS can also be configured to count Invalid Access attempts at the Serial Setup Port, and provide notification when the counter exceeds the user defined trigger level, without actually locking the serial ports. To do this, enable the Invalid Access Lockout Alarm as described here, but when you configure Invalid Access Lockout parameters, set the Lockout Attempts and Lockout Duration as you would normally, and then set the "Serial Port Lockout" parameter to "Off."*
- *In order for the AFS to provide Email alarm notification, communication parameters must first be defined as described in Section 6.3.1.16.*
- *In order for the AFS to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 6.3.1.9.*
- *In order for the AFS to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 6.3.1.10.*

To configure the Serial Port Invalid Access Lockout Alarm, access the user interface using a password that permits Administrator Level commands. The Serial Port Invalid Access Lockout Alarm configuration menu offers the following parameters:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.* • *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Resend Delay (Default = 60 Minutes)	Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful.
Notify Upon Clear (Default = On)	When enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected.
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses defined via the "Email Messaging" menu will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. **Note:** *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Invalid Access Lockout")	Defines the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm.
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The Severity level used to generate Syslog Messages for Alarm Log Events.
Contact Output Enable (Default = On)	Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated. **Note:** *For more information on the Output Contacts, please refer to Section 6.9.1.*

6.9.5. The Power Cycle Alarm

The Power Cycle Alarm can provide notification when input power to the AFS unit is lost and then restored. When the Power Cycle Alarm is triggered, the AFS can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined as described in Section 6.3.1.16.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 6.3.1.9.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 6.3.1.11.*

To configure the Power Cycle Alarm, access the user interface using a password that permits Administrator Level commands. The Power Cycle Alarm configuration menu offers the following parameters:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.* • *The Trigger Enable, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses, (defined via the "Email Messaging",) menu will receive the email alarm notification messages generated by this alarm. **Note:** *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Power Cycle")	Defines the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm.
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The Severity level used to generate Syslog Messages for Alarm Log Events.

6.9.6. The Alarm Input Alarm

The Alarm Input Alarm can be used to monitor dry contacts that have been connected to the Alarm Inputs. Typically, the Alarm Input Alarm is used to detect open doors and other situations where a dry contact has been opened or closed.

To configure the Alarm Input Alarm, you must first connect a dry contact relay to the alarm inputs and then access the AFS using a password that permits Administrator Level commands. The Alarm Input Alarm configuration menu offers the following parameters:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.* • *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Alarm Input Level (Default = Low)	Determines whether a high or low signal at the Monitor Input contact (Pin 4 on the Control Module's AUX Connector) will generate an alarm. For example, if the Monitor/Alarm Input Level is set at "Low", then an alarm will be triggered when a low signal is detected at Pin 4. Note that the Monitor/Alarm Input Level is always set to compliment the setting for the Monitor Input Level Jumper as described in Section 6.9.6.2.
Alarm Input Delay (Default = 0.5 Secs)	Determines how long the signal at the Monitor Input Contact must remain high/low in order to generate an alarm.
Resend Delay (Default = 60 Minutes)	Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful.
Notify Upon Clear (Default = On)	When enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected.
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses defined via the "Email Messaging" menu (see Section 6.3.1.16,) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. **Note:** *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Power Cycle")	Defines the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm.

Parameter (Default)	Description
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The Severity level used to generate Syslog Messages for Alarm Log Events.
Contact Output Enable (Default = On)	Activates/deactivates the Output Contacts on the Control Module AUX Connector. When this parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact.
Circuits to Switch	Provides access to a submenu that is used to select the circuits that will be switched when an Alarm Input Alarm is generated.

6.9.6.1. The Alarm Input Alarm - Circuits to Switch

This submenu is used to select the circuits that will be switched when the Alarm Input Alarm is triggered. The Alarm Input Parameters submenu offers the following configuration options:

Parameter (Default)	Description
Enable (Default = Enable)	Enables/disables A/B switching in response to the Alarm Input Alarm.
Circuit State (Default = B)	Determines whether selected circuits will be switched to the "A" position or "B" position when the Alarm Input Alarm is triggered.
Return (Default = Off)	When enabled, the AFS will return the selected circuit(s) to their original position when the Alarm Input Alarm is cleared.
Select Circuits (Default = Undefined)	Selects the circuits that will be switched when an Alarm Input Alarm is triggered.
Select Circuit Groups (Default = Undefined)	Selects the circuits groups that will be switched when an Alarm Input Alarm is triggered.

6.9.6.2. Monitor Input Level Settings

When the Monitor/Alarm Input feature is properly configured, the AFS can trigger an alarm and/or perform A/B switching operations when the signal at Pin 4 (Monitor Input) on the Control Module AUX connector goes high or low.

When setting up this feature, you must first use the Control Card Jumper to select the non-active (non-alarm) state, and then use the Monitor/Alarm Input configuration menu to select the active/alarm state (the signal level that will trigger an alarm) as described in the figures below and the Sections that follow.

Notes:

- *The Monitor Input signal (Pin 4) is always measured relative to the signal at the common ground (Pin 5).*
- *A "Low" signal should be between Zero (0) Volts and -48 Volts and a "High" signal should be between +5 Volts and +48 Volts.*

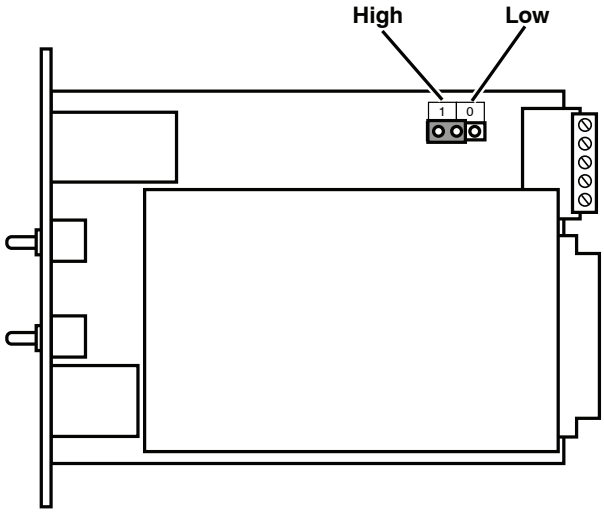

Figure 6.2: Control Module Jumper

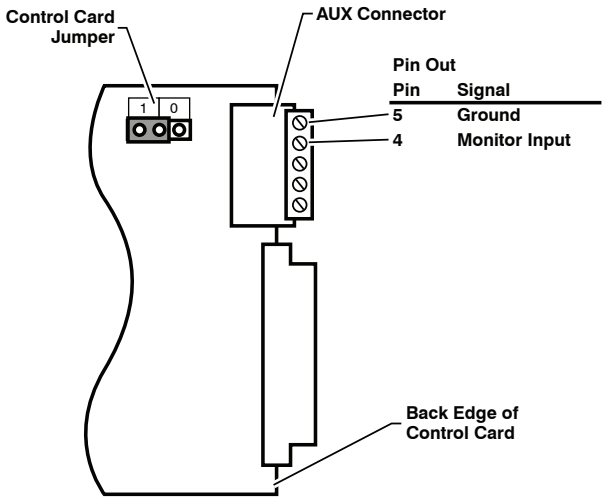

Figure 6.3: Control Module AUX Connector - Monitor Input and Ground

6.9.6.2.1. Monitor Input Signal - Trigger When Low

To set up the Monitor/Alarm Input feature to trigger an alarm when the signal at AUX connector pin 4 (the Monitor Input) goes Low, configure the AFS as follows:

1. **Control Card Jumper Setting:** Set the Jumper to the "1" position (default.) This will set the non-active, non-alarm signal state to "High".
2. **Monitor/Alarm Input Level:** Use the Monitor/Alarm Input configuration menu to set the Monitor Alarm Input Level to "Low". This will configure the Monitor/Alarm Input feature to generate an alarm when the Monitor Input signal goes Low.
3. **Set the Remaining Parameters:** Use the Monitor/Alarm Input configuration menu to select the remaining parameters.
4. **Connect Monitor Input:** Connect the signal line that you wish to monitor to Pin 4 (Monitor Input) on the Control Module AUX Connector as shown in Figure 6.3.

6.9.6.2.2. Monitor Input Signal - Trigger When High

To set up the Monitor/Alarm Input feature to trigger an alarm when the signal at AUX Connector pin 4 (the Monitor Input) goes High, configure the AFS as follows:

1. **Control Card Jumper Setting:** Set the Jumper to the "0" position. This will set the non-active, non-alarm signal state to "Low" as shown in Figure 6.2.
2. **Monitor/Alarm Input Level:** Use the Monitor/Alarm Input configuration menu to set the Monitor Alarm Input Level to "High". This will configure the Monitor/Alarm Input feature to generate an alarm when the Monitor Input signal goes High.
3. **Set the Remaining Parameters:** Use the Monitor/Alarm Input configuration menu to select the remaining parameters.
4. **Connect Monitor Input:** Connect the signal line that you wish to monitor to Pin 4 (Monitor Input) on the Control Module AUX Connector as shown in Figure 6.3. Connect your ground line to the Ground Connector (Pin 5).

6.9.7. The No Dialtone Alarm

The No Dialtone Alarm allows the AFS to monitor a telephone line connected to an external modem installed at the AFS unit's Setup Port, and then provide notification if the phone line is dead or no dialtone is present. When the No Dialtone Alarm is enabled the AFS will monitor the phone line checking for a dialtone.

Notes:

- *In order for this alarm to function, the Reset/No Dialtone Interval and the Reset/No Dialtone Scaler must both be set to a value from 1 to 99.*
- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled.*

The No Dialtone Alarm Menu allows the following parameters to be defined:

Parameter (Default)	Description
Trigger Enable (Default = On)	Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. **Notes:** • *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.* • *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all alarms.*
Resend Delay (Default = 60 Minutes)	Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt was unsuccessful.
Notify Upon Clear (Default = On)	When enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected.
Email Message (Default = On)	Enables/Disables email notification for this alarm.
Address 1, 2, and 3 (Default = All On)	These parameters are used to select which of the three email addresses defined via the "Email Messaging" menu will receive the email alarm notification messages generated by this alarm. **Note:** *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: No Dial Tone")	Defines the text that will appear in the "Subject" field for all email notification messages generated by this alarm.
Facility (Default = 0)	The Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	The Severity level used to generate Syslog Messages for Alarm Log Events.
Contact Output Enable (Default = On)	Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated.

6.10. Telemetry Options

The Telemetry Options button can be used to access the Continuous (Streaming Data) configuration menu and the Event Based (One Shot Data) menu.

6.10.1. Continuous (Streaming Data) Telemetry Menu

When Continuous (Streaming Data) is selected, the AFS will display a menu that allows you to select the Telemetry Name. Use the drop down menu to select the desired Telemetry Name and then click on the Choose Telemetry Option button. The Continuous (Streaming Data) Telemetry Menu will be displayed.

The Continuous (Streaming Data) Telemetry Menu allows the following parameters to be defined.

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables Continuous Details Telemetry.
Name (Default = Undefined)	
Password (Default = Undefined)	
Shared Secret (Default = Undefined)	
Dataset (Default = Temperature)	
Frequency (Default = 3600)	
Timeout (Default = 10)	
Retries (Default = 2)	
Command (Default = Undefined)	

6.10.2. Event Based (One Shot Data) Telemetry Menu

When Event Based (One Shot Data) is selected, the AFS will display a menu that allows you to select the Telemetry Name. Use the drop down menu to select the desired Telemetry Name and then click on the Choose Telemetry Option button. The Event Based (One Shot Data) Telemetry Menu will be displayed.

The Event Based (One Shot Data) Telemetry Menu allows the following parameters to be defined.

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables Continuous Details Telemetry.
Name (Default = Undefined)	
Password (Default = Undefined)	
Shared Secret (Default = Undefined)	
Dataset (Default = Alert Data)	
Timeout (Default = 10)	
Retries (Default = 2)	
Command (Default = Undefined)	

6.11. Download Unit Configuration

Once the AFS is properly configured, parameters can be downloaded and saved. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to automatically reconfigure the unit without the need to manually reassign each parameter. Saved parameters can also be uploaded to other identical AFS units, allowing rapid set-up when several identical units will be configured with similar parameters.

The AFS unit's Download Unit Configuration option can be used to save configuration parameters to an XML format file on your PC or laptop. To save parameters via the Web Browser Interface, proceed as follows:

Notes:

- *Although AFS parameters can be saved to a file via either the CLI or Web Browser Interface, saved parameters can only be restored via the CLI. The Restore Parameters function is not available via the Web Browser Interface.*
- *For further instructions regarding downloading parameters via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*
- *This procedure may differ slightly, depending on the operating system and browser used. In some cases, your system may perform a security scan before proceeding with the download.*

6.11.1. Restoring Saved Configuration Parameters

This section describes the procedure for using your terminal emulation program to send saved parameters to the AFS.

Note: *The Restore Parameters feature is only available via the CLI.*

1. Start your terminal emulation program (e.g. PuTTy, TeraTerm©, etc.) and access the CLI using an account that permits Administrator level commands.
2. Configure your terminal emulation program to upload an XML format file.
3. Upload the XML with the saved AFS parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the XML file to the AFS. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the AFS detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.*

5. If the parameter upload is successful, the AFS will send a confirmation message, and then return to the command prompt. Type /S and press [Enter], the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

6.12. Firmware Upgrade

The Firmware Upgrade feature allows you to review recent Firmware Release Notes, check for new Firmware Upgrades and select and install Firmware Upgrades as described in Section 9.

6.13. The Test Menu

The Test Menu can be used to check to make certain that SNMP Trap Managers and Syslog communication are configured correctly. In addition, the Test Menu can also be used to Ping AFS units and other network elements to make certain that they are responsive. The Test Menu offers the following functions:

Parameter (Default)	Description
SNMP Trap Test Manager 1 through 4	Sends a test SNMP Trap to the SNMP Managers that were defined as described in Section 6.3.1.11.
Syslog Test	Sends a test Syslog Message to the Syslog Manager that was defined as described in Section 6.3.1.9.
Ping Test	Pings the IP address currently entered in the IPS Address field, just above the Ping Test Button. In addition, the Ping Test also offers the ability to send the test ping via either the Ethernet Port (eth0.)

7. Creating Web Certificates

There are two different types of HTTPS security certificates: “Self Signed” certificates and “Signed” certificates.

Self Signed certificates can be created by the AFS, without the need to go to an outside service. The principal disadvantage of Self Signed certificates, is that when you access the AFS via the Web Browser Interface, the browser will display a message which warns that the connection might be unsafe. Note however, that even though this message is displayed, communication will still be encrypted, and the message is merely a warning that the AFS is not recognized and that you may not be connecting to the site that you intended.

Signed certificates must be created via an outside certificate authority (e.g., VeriSign®, Thawte™, etc.) and then uploaded to the AFS to verify the unit’s identity. Once a signed certificate has been set up, you will then be able to access the user interface without seeing the warning message that is displayed for a Self Signed certificate access.

7.1. Creating a Self Signed Certificate

To create a Self Signed certificate, access the CLI, using a password that permits access to Administrator level commands and proceed as follows:

1. Type **/N 0** and press **[Enter]** to display the eth0/IPv4 (Shared) Network Parameters menu.
2. At the eth0/IPv4 Network Parameters menu, type 23 and press [Enter] to display the Web Access menu. Type 3 and press [Enter] and then use the resulting submenu to enable HTTPS access.
3. Press **[Esc]** to return to the Web Access menu and then define the following parameters.

Notes:

- *When configuring the AFS, make certain to define all of the following parameters. Although most SSL/TLS applications require only the Common Name, in the case of the AFS all of the following parameters are mandatory.*
- *If desired, any random text sequence can be entered in each of these fields.*

- **5. Common Name:** A domain name that will be used to identify the AFS. If you will use a Self Signed certificate, then this name can be any name that you choose, and there is no need to set up your domain name server to recognize this name. However, if you will use a Signed certificate, then your domain name server must be set up to recognize this name (e.g., service.yourcompanyname.com.)
- **6. State or Province:** The name of the state or province where the AFS will be located (e.g., California.)
- **7. Locality:** The city or town where the AFS will be located (e.g., Irvine.)
- **8. Country Code:** The two character country code for the nation where the AFS will be located (e.g., US.)
- **9. Email Address:** An email address, that can be used to contact the person responsible for the AFS (e.g., jsmith@yourcompany.com.)
- **10. Organization:** The name of your company or organization (e.g., Yourcompanyname, Inc.)
- **11. Organizational Unit:** The name of your department or division.

4. After you have defined parameters 5 through 11, type `13` and press **[Enter]** to access the CSR Commands menu. From the CSR Commands Menu, type `1` and press **[Enter]** to generate a Certificate Signing Request. This will overwrite any existing certificate, and create a new Self Signed certificate.

   a) The AFS will prompt you to create a password. Key in the desired password and then press **[Enter]**. When the AFS prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the AFS will return to the Web Access Menu, indicating that the CSR has been successfully created.

   b) When the Web Access Menu is re-displayed, press **[Esc]** several times until you exit from the Network Parameters menu and the "Saving Configuration" message is displayed.

5. After the new configuration has been saved, test the Self Signed certificate by accessing the AFS via the Web Interface, using an HTTPS connection.

   a) Before the connection is established, the AFS should display the warning message described previously. This indicates that the Self Signed certificate has been successfully created and saved.

   b) The AFS will prompt you to enter a user name and password. After keying in your password, the main menu should be displayed, indicating that you have successfully accessed the user interface.

7.2. Creating a Signed Certificate

To create a Signed certificate, and eliminate the warning message, first set up your domain name server to recognize the Common Name (item 5) that you will assign to the unit. Next, complete steps one through five as described in Section 10.1 and then proceed as follows:

1. **Capture the Newly Created Certificate:** Type `13` and press **[Enter]** to access the CSR Commands submenu.

   a) At the CSR Commands submenu, type `2` and press **[Enter]** to select the Display CSR Key option.

   b) The AFS will prompt you to configure your communications program to receive the certificate. Set up your communications program to receive a binary file, and then press **[Enter]** to capture the file and save it. This is the Code Signing Request that you will send to the outside security service (e.g., VeriSign, Thawte, etc.) in order to have them sign and activate the certificate.

2. **Obtain the Signed Certificate:** Send the captured certificate to the outside security service. Refer to the security service's web page for further instructions.

3. **Upload the Signed Certificate to the AFS:** After the signed certificate is returned from the certificate authority, return to the Web Access menu.

   a) Access the AFS via the CLI using an account that permits Administrator level commands as described previously, then type **`/N`** and press **[Enter]** to display the eth0/IPv4 (Shared) Network Parameters menu.

   b) At the eth0/IPv4 (Shared) Network Parameters, type **`23`** and press **[Enter]** to display the Web Access menu.

   c) From the Web Access menu, type **`13`** and press **[Enter]** to display the CRT Commands submenu.

   d) At the CRT Commands submenu, type **`1`** and press **[Enter]** to select the Upload Signed CRT Certificate option.

   e) Use your communications program to send the binary format Signed Certificate to the AFS. When the upload is complete, press **[Esc]** to exit from the CRT Commands submenu.

   f) After you exit from the CRT Server Key submenu, press **[Esc]** several times until you have exited from the Network Parameters menu and the "Saving Configuration" message is displayed.

4. After the configuration has been saved, test the signed certificate by accessing the AFS via the Web Browser Interface, using an HTTPS connection. For example, if the common name has been defined as "service.wti.com", then you would enter "**`https://service.wti.com`**" in your web browser's address field. If the Signed Certificate has been properly created and uploaded, the warning message should no longer be displayed.

7.3. Downloading the Server Private Key

When configuring the AFS's SSL/TLS encryption feature (or setting up other security/authentication features), it is recommended to download and save the Server Private Key. To download the Server Private Key, access the CLI using a password that permits access to Administrator level commands and then proceed as follows:

1. Type `/N 0` and press **[Enter]** to display the eth0/IPv4 (Shared) Network Parameters menu.
2. At the eth0/IPv4 (Shared) Network Parameters menu, type `23` and press **[Enter]** to display the Web Access menu.
    a) To download the Server Private Key from the AFS, make certain that SSL/TLS parameters have been defined, then type `13` and press **[Enter]** to display the CRT Commands submenu.
    b) At the CRT Commands submenu, type `2` and press **[Enter]** to display the Signed CRT Certificate Copy the resulting CRT certificate to a text file and save the text file on your hard drive.
3. To upload a previously saved CRT Certificate to the AFS, make certain that SSL/TLS parameters have been defined, return to the Web Access menu as described in Steps 1 and 2 above, then type `13` and press **[Enter]** to display the CRT Commands Submenu.
    a) At the CRT Commands submenu, type `1` and press **[Enter]** to select the Upload Signed CRT Certificate option.
    b) Use your communications program to send the binary format Signed Certificate to the AFS. When the upload is complete, press **[Esc]** to exit from the CRT Commands submenu.
    c) After you exit from the CRT Server Key submenu, press **[Esc]** several times until you have exited from the Network Parameters menu and the "Saving Configuration" message is displayed.

7.4. Harden Web Security

In the Web Access Menu, the Harden Web Security option allows you to disable SSLv3 and MEDIUM ciphers for in coming web connections.

7.5. TLS Mode

The TLS Mode parameter in the Web Access menu selects the TLS version(s) that the web server will accept from incoming web connections.

8. Saving and Restoring Configuration Parameters

Once the AFS is properly configured, parameters can be downloaded and saved. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to quickly restore configuration parameters without the need to manually assign each parameter.

Saved parameters can also be uploaded to other identical AFS units, allowing rapid set-up when several identical units will be configured with similar parameters.

The "Save Parameters" procedure can be performed from any terminal emulation program (e.g. PuTTy, TeraTerm©, etc.), that allows downloading.

> **Note:** *Configuration parameters can be downloaded and saved via either the Web Browser Interface or Command Line Interface (CLI). Saved configuration parameters can only be uploaded to the AFS via the CLI.*

8.1. Sending Parameters to a File

8.1.1. Downloading & Saving Parameters via CLI

1. Access the CLI, using an account that permits Administrator level commands.
2. When the command prompt appears, type `/DF` and press **[Enter]**.
   a) The AFS will prompt you to select a file transfer protocol. Key in the number for the desired protocol, and press **[Enter]**.
   b) The AFS will prompt you to configure your terminal emulation program to receive an ASCII download.
      i. Set your terminal emulation program to receive an ASCII file, and then specify a name for a file that will receive the saved parameters (e.g., WTI.PAR).
      ii. Disable the Line Wrap function for your terminal emulation program. This will prevent command lines from being broken in two during transmission.
   3. When the terminal emulation program is ready to receive the file, return to the AFS's Save Parameter File menu, and press **[Enter]** to proceed. AFS parameters will be saved on your hard drive in the file specified in Step 2 above.
   4. The AFS will send a series of command lines which specify currently selected parameters. When the download is complete, press **[Enter]** to return to the command prompt.

8.1.2. Downloading & Saving Parameters via Web Browser Interface

The Web Browser Interface also includes a download function that can be used to save AFS parameters to an XML format file on your PC or laptop. To save parameters via the Web Browser Interface, proceed as follows:

Notes:

- *Although AFS parameters can be saved to a file via either the CLI or Web Browser Interface, saved parameters can only be restored via the CLI. The Restore Parameters function is not available via the Web Browser Interface.*
- *For further instructions regarding downloading parameters via the Web Browser Interface, please refer to the WTI.com Knowledge Base.*
- *This procedure may differ slightly, depending on the operating system and browser used. In some cases, your system may perform a security scan before proceeding with the download.*

1. Access the Web Browser Interface using an account that permits Administrator level commands.
2. When the Web Browser Interface appears, click on the “Download Unit Configuration” button on the left hand side of the screen.
3. After a brief pause, your browser may display a prompt asking if you want to open or save the downloaded file. At this point, you can either select the “Save” option to save the parameters file to the download folder on your PC, or select “Save As” to pick a different location and/or filename for the saved parameters file.

8.2. Restoring Downloaded Parameters

This section describes the procedure for using your terminal emulation program to send saved parameters to the AFS.

Note: *The Restore Parameters feature is only available via the CLI.*

1. Start your terminal emulation program and access the AFS's CLI using an account that permits Administrator level commands.
2. Configure your terminal emulation program to upload an ASCII file.
3. Upload the ASCII text file with the saved AFS parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the AFS. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the AFS detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.*

5. If the parameter upload is successful, the AFS will send a confirmation message, and then return to the command prompt. Type `/s` and press **[Enter]**, the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

8.3. Restoring Recently Saved Parameters

If you make a mistake while configuring the AFS, and wish to return to the previously saved parameters, the CLI's "Reboot System" command (/I) offers the option to reinitialize the AFS using previously backed up parameters. This allows you to reset the unit to previously saved parameters, even after you have changed parameters and saved them.

Notes:

- *The AFS will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved AFS parameters, and will be overwritten by the next night's daily backup.*
- *When the /I command is invoked, a submenu will be displayed which offers several Reboot options. Option 4 is used to restore the configuration backup file. The date shown next to option 4 indicates the date that you last changed and saved unit parameters.*
- *If the daily automatic configuration backup has been triggered since the configuration error was made, and the previously saved configuration has been overwritten by newer, incorrect parameters, then this function will not be able to restore the previously saved (correct) parameters.*

To restore the previously saved configuration, proceed as follows:

1. Access the CLI, using a username/password that permits access to Administrator level commands.
2. At the command prompt, type `/I` and press **[Enter]**. The AFS will display a submenu that offers several different reboot options.
3. At the submenu, select Item 4 (Reboot & Restore Last Known Working Configuration,) type **`4`**, and then press **[Enter]**.
4. The AFS will reboot and previously saved parameters will be restored.

9. Upgrading Software

When new, improved versions of WTI software become available, either the WMU Enterprise Management Software (recommended,) the Web Browser Interface's Firmware Upgrade option, or the CLI's "Upgrade Software" function can be used to update the unit. This section describes the procedures for updating the AFS.

9.1. WMU Enterprise Management Software (Recommended)

The WMU Enterprise Management Software provides the preferred method for updating AFS units. The WMU software allows you to manage software updates for multiple AFS units from a single centralized interface. The WMU program can be downloaded from WTI at:

ftp://ftp.wti.com/pub/TechSupport/WMU/WTIManagementUtilityInstall.exe

For a description of the procedure for managing software updates using the WMU, please refer to the WMU user's guide, which can be downloaded from the User Manual archive at WTI.com.

Note that in order to use the WMU, the software version for the AFS must be at least v6.23 or higher. When upgrading older AFS units that feature pre v6.23 software, it is recommended to use the WTI Software Upgrade Utility.

9.2. The Firmware Upgrade Function (Web Browser Interface)

The Firmware Upgrade function provides a method for updating the AFS via the Web Browser Interface. A zip file that contains the installation files and other documentation for the WTI Software Upgrade Utility can be downloaded from WTI's FTP server at:

ftp://wtiftp.wti.com/pub/TechSupport/Firmware/Upgrade_Utility/

Notes:

- *All other ports will remain active during the software upgrade procedure.*
- *If the upgrade includes new parameters or features not included in the previous software version, these new parameters will be set to their default values.*
- *The upgrade procedure will require approximately 15 minutes.*

1. Obtain the update file. Software modifications can be downloaded from WTI. Copy the update file to your hard drive.
2. Access the Web Browser Interface for the desired AFS, using an account and port that permit Administrator level commands.
3. When the Home Menu appears, click on the Firmware button on the left hand side of the screen. The AFS will display the Firmware Upgrade menu.
4. At the Firmware Upgrade menu, click on the "Choose File" button, and then select the Firmware Upgrade file that was copied to your hard drive in Step 1 above.
6. To proceed with the upgrade, click on the "Submit" button to begin the upgrade.

Notes:

- *The upgrade will require approximately five minutes. If you exit from the Firmware Upgrade Menu before the upgrade is complete, the upgrade will be cancelled.*
- *Do not power down the AFS while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

9.3. The Upgrade Software Function (Command Line Interface)

The Upgrade Software function provides an alternative method for updating the AFS software. A zip file that contains the installation files and other documentation for the WTI Software Upgrade Utility can be downloaded from WTI's FTP server at:

ftp://wtiftp.wti.com/pub/TechSupport/Software/Upgrade_Utility/

Updates can be uploaded via FTP or SFTP protocols.

Notes:

- *The FTP/SFTP servers can only be started via the Command Line Interface (CLI).*
- *All other ports will remain active during the software upgrade procedure.*
- *If the upgrade includes new parameters or features not included in the previous software version, these new parameters will be set to their default values.*
- *The upgrade procedure will require approximately 15 minutes.*

1. Obtain the update file. Software modifications can be downloaded from WTI. Copy the update file to your hard drive.
2. Access the CLI via Serial Port, using an account and port that permit Administrator level commands.
3. When the command prompt appears, type /UFW and then press [Enter]. The AFS will display a screen which offers the following options:

   a) **Start FTP/SFTP Servers Only (Do NOT default parameters):** Upgrade and retain user-defined parameters. All existing parameter settings will be restored when the upgrade is complete.

   b) **Start FTP/SFTP Servers & Default (Keep IP parameters & SSH Keys):** Upgrade and reset all parameters (except for the IP Parameters and SSH Keys) to default values. When the upgrade is complete, all parameter settings except the IP Parameters and SSH Keys will be reset to factory defaults.

   c) **Start FTP/SFTP Servers & Default (Default ALL parameters):** Upgrade and reset all parameters to default settings. When the upgrade is complete, all parameters will be set to default values.

   d) **Start FTP/SFTP Servers for Slip Stream Upgrade:** Upgrade only the WTI Management Utility, without updating the AFS's operating software.

   Note that after any of the above options is selected, the AFS will start the receiving servers and wait for an FTP/SFTP client to make a connection and upload a valid software binary image.

4. To proceed with the upgrade, select either option 1 or option 2. The AFS will display a message that indicates that the unit is waiting for data. Leave the current SSH/Telnet client session connected at this time.

5. Open your FTP/SFTP application and (if you have not already done so,) login to the AFS, using an account and port that permit access to Administrator Level commands.

6. Transfer the md5 format upgrade file to the AFS.

7. After the file transfer is complete, the AFS will install the upgrade file and then reboot itself and break all port connections. Note that it will take approximately 10 minutes to complete the installation process. The unit will remain accessible until it reboots.

   a) Some FTP/SFTP applications may not automatically close when the file transfer is complete. If this is the case, you may close your FTP/SFTP client manually after it indicates that the file has been successfully transferred.

   b) When the upgrade process is complete, the AFS will send a message to all currently connected network sessions, indicating that the AFS is going down for a reboot.

   Note: *Do not power down the AFS while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

8. If you have accessed the AFS via the Network Port, in order to start the FTP/SFTP servers, the AFS will break the network connection when the system is reinitialized.

   - If you initially selected "Start FTP/SFTP Servers and Save Parameters", you may then reestablish a connection with the AFS using your former IP address.

   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the AFS's default IP address (Default = 192.168.168.168) or access the user interface via Serial Port 1 or via Modem.

When software upgrades are available, WTI will provide the necessary files. At that time, an updated Configuration Guide or addendum will also be available.

10. The Command Line Interface (Scripting)

In addition to the Web Browser Interface and WMU Enterprise Management Software, the AFS also includes a Command Line Interface (or CLI) that allows the unit to be controlled and configured using simple, ASCII commands.

In addition to providing simple, direct, real-time control of the AFS, the CLI also allows Administrators to create custom scripts, which can be used to automate port connection, power switching and configuration operations, and provide compatibility with third party enterprise management solutions.

10.1. Accessing the Command Line Interface (CLI)

The CLI consists of a an array of commands and text menus, which allow you to set options and configuration parameters.

Since the Web Browser Interface and Telnet accessibility are both disabled in the default state, you will need to use the CLI to contact the AFS via Local PC or SSH connection when setting up the unit for the first time. After you have accessed the CLI, you can then enable Web Access and Telnet Access, if desired, allowing future communication with the unit via Web Browser or Telnet.

Once access is enabled, you will then be able to use the CLI to communicate with the AFS via local PC, Telnet or SSH connection. You can also access the CLI via dial-up or cellular modem, providing that the dial-up modem option or cellular modem option are present.

- **Access via Network:** The AFS must be connected to your TCP/IP Network, and your PC must include a communications program (such as TeraTerm or PuTTy.)
- **Access via Dial-Up Modem:** If desired a dial-up modem can be installed at the AFS Setup Port.
- **Access via Local PC:** Your PC must be connected to the AFS Serial SetUp Port, the SetUp Port must be configured for Normal Mode, (default port Mode for the SetUp Port,) and your PC must include a communications program (Such as Tera Term or PuTTY.)

To access the Command Line Interface (CLI), proceed as follows:

Note: *When communicating with the unit for the first time, you will not be able to contact the unit via Telnet until you have accessed the user interface, via Local PC or SSH Client, and used the Network Parameters Menu to enable Telnet as described in Section 3.3.1.*

1. Contact the AFS:

   a) **Via Local PC:** Start your communications program and press **[Enter]**. Wait for the connect message, then proceed to Step 2. Note that when viewed by a PC running Windows XP or later, the Serial COM Port menu will list the USB Mini Port (if present) as, "USB to Serial."

   b) **Via Network:** The AFS includes a default IPv4 format IP address (192.168.168.168) and a default IPv4 format subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit.

      i. **Via SSH Client:** Start your SSH client, and enter the AFS IP Address. Invoke the connect command, wait for the connect message, then proceed to Step 2.

      ii. **Via Telnet:** If you have enabled Telnet as described in Section 3.3.1, start your Telnet Client, and then Telnet to the AFS IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Dial-Up Modem:** If you have installed an external modem at the AFS Setup Port, you can then use your communications program to dial the number for the phone line that you have connected to the modem.

2. **Login** / **Password Prompt:** A message will be displayed, which prompts you to enter a username (login name) and password. The default username is super (all lower case,) and the default password is also super.

10.2. Command Conventions

Most CLI commands described conform to the following conventions:

- **Apply Command to All Circuits:** When an asterisk is entered as the argument of the **/T** (Toggle), **/TA** (Toggle to A) or **/TB** commands (Toggle to B) the command will be applied to all circuits. For example, to switch all circuits to "A", type **/TA * [Enter]**.
- **Circuit Name Wild Card:** It is not always necessary to enter the entire circuit name. Circuit names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (*****). For example, a circuit named "**SERVER**" could be specified as "**S***". Note however, that this command would also be applied to any other circuit name that begins with an "S".
- **Command Queues:** If a toggle command is directed to a circuit that is already being switched by a previous command, then the new command will be placed into a queue until the circuit is ready to receive additional commands.
- **"Busy" Circuit:** If the "Status" column in the Circuit Status Screen includes an asterisk, this means that the circuit is currently busy, and is in the process of completing a previously issued command. If a new command is issued to a busy circuit, then the new command will placed into a queue to be executed later.
- **Suppress Command Confirmation Prompt:** When any command that normally requires confirmation is invoked, the "**,Y**" option can be included to override the Command Confirmation ("Sure?") prompt. For example, to switch Circuit 4 to the "B" position wihout displaying the Sure prompt, type **/TB 4,Y [Enter]**.

10.3. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Circuit Status	**/S [Enter]**	X❶	X❶	X❶	X❶
Serial Setup Port Diagnostics	**/SD [Enter]**	X❶	X❶	X❶	X❶
Serial Port Parameters (Who)	**/W [n] [Enter]**	X	X	X	X
Circuit Group Status	**/SG [Enter]**	X❶	X❶	X❶	X❶
Network Status	**/SN [Enter]**	X	X	X	X
Network Configuration Summary	**/RN [Enter]**	X	X	X	X
IP Alias Status	**/SA [Enter]**	X	X	X	X
Alarm Status	**/AS [alarm] [Enter]**	X			
Help Menu	**/H [Enter]**	X❷	X❷	X❷	X❷
Log Functions	**/L [Enter]**	X	X		
Site ID / Unit Information	**/J [*] [Enter]**	X	X	X	X
Control					
Exit CLI	/X [Enter]	X	X	X	X
Connect - Local <Remote>	**/C <n> [n] [Enter]**	X	X	X❸	
Switch Circuit *C* to Position A	**/TA <*C*>[,Y] [Enter]❹**	X	X	X	
Switch Circuit *C* to Position B	**/TB <*C*>[,Y] [Enter]❹**	X	X	X	
Switch Circuit *C* to Position *P*	**/T <*C*>,<*P*>[,Y] [Enter]❹**	X	X	X	
Default All Circuits ❺	**/DC[,Y] [Enter]❹**	X	X	X	
Download Parameter File	**/DF [ztp] [Enter]**	X			
Send Parameter File	**/U [Enter]**	X			
Unlock Invalid Access	**/UL [Enter]**	X			
Outbound Telnet	**/TELNET <ip> [port] [raw] [Enter]**	X❻	X❻	X❻	
Outbound SSH	**/SSH <ip> -l <username> [Enter]**	X❻	X❻	X❻	
Test Network Configuration	**/TEST [Enter]**	X			
Configuration					
System Parameters	**/F [Enter]**	X	❼		
Serial Port Parameters	**/P [Enter]**	X	❼		
Circuit Parameters	**/PC <n> [Enter]**	X	❼		
Circuit Group Parameters	**/G [Enter]**	X	❼		
Network Configuration - Eth0/IPv4	**/N [Enter]**	X	❼		
Network Configuration - IPv0/IPv6	**/N6 [Enter]**	X	❼		
Ping No Answer Configuration	**/PNA [Enter]**	X	❼		
Alarm Configuration	**/AC [Enter]**	X	❼		
Reboot System	**/I [Enter]**	X	X		
Upgrade Software	**/UFW [Enter]**	X			
VPN Configuration	**/VPN [Enter]**	X			

❶ In Administrator and SuperUser mode, all circuits and circuit groups are displayed. In User and ViewOnly mode, the screen will only display circuits and circuit groups allowed by the account.

❷ In Administrator Mode, Help Menus will list all commands. In SuperUser, User and ViewOnly modes, Help Menus will only list the commands allowed by the access level.

❸ User Mode accounts are only allowed to connect to the Serial Port if Serial Access is enabled for the account.

❹ The ",Y" argument can be included to suppress the command confirmation prompt.

❺ The "Default All Circuits" command will only be applied to the Circuits that are allowed by the account.

❻ In order to invoke this command, Outbound Telnet/SSH and Outbound Service Access must be enabled for your account.

❼ In SuperUser mode, configuration menus can be displayed, but parameters cannot be changed.

10.4. Command Set

This section provides information on all Command Line Interface (CLI) commands, sorted by functionality

10.4.1. Display Commands

/S Display Status Screen

Displays the Main Status Screen, which lists the current status of all AFS circuits.

> **Note:** *In Administrator Mode and SuperUser Mode, all AFS circuits are displayed. In User Mode and ViewOnly Mode, the Port and Circuit Status Screen will only include the circuits allowed by the account.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/S`** **[Enter]**

/SD Display Port Diagnostics

Provides detailed information regarding the status of the Serial Setup Port.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/SD`** **[Enter]**

Response: Displays Port Diagnostics Screen.

/W Display Port Parameters (Who)

Displays configuration information regarding the Serial Setup Port, but does not allow parameters to be changed.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/W [x]`** [Enter]

Where **`x`** is the port number or name. To display parameters for the Network Port, enter an "**`N`**". If the "**`x`**" argument is omitted, parameters for your resident port will be displayed.

Example: To display parameters for a port named "SERVER", access the CLI via a port and account that permit Administrator level commands, and type **`/W SERVER`** **[Enter]**.

/SG Display Circuit Group Status Screen

Displays the Circuit Group Status Screen, which lists all user-defined Circuit Groups, the Circuits included in each group, the current A/B status and other information.

> **Note:** *In Administrator Mode all user defined Circuit Groups are displayed. In SuperUser Mode, User Mode and ViewOnly Mode, the Circuit Group Status Screen will only include the Circuit Groups allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/S`** **[Enter]**

/SN Display Network Status

Displays the Network Status Screen, which lists current network connections to the AFS Network Port.

Availability: Administrator, SuperUser, User, ViewOnly
Format: **`/SN`** **[Enter]**

/RN Network Configuration Summary

Displays a screen that lists currently selected communication settings, LDAP status, RADIUS status, Email Messaging status, NTP status, PPP status and other information.

Availability: Administrator, SuperUser, User ViewOnly
Format: **`/RN`** **[Enter]**

/SA IP Alias Status

Displays the Alias Status Screen, which lists currently selected port name, alias IP address and Direct Connect status for the AFS serial port.

> **Note:** *When the Alias Status Screen is displayed by an Administrator or SuperUser level account, the screen will display the status of all ports. If the Alias Status Screen is displayed by a User or ViewOnly level account, the screen will only display the status of the ports specifically allowed by the account.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: **`/SA`** **[Enter]**

/H Help

Displays a Help Screen, which lists most available Command Line Interface (CLI) commands along with a brief description of each command.

> **Note:** *In the Administrator Mode, the Help Screen will list most available AFS commands. In SuperUser Mode, User Mode and ViewOnly Mode, the Help Screen will only list the commands allowed for that Access Level.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: **`/H`** **[Enter]**

/L Log Functions

Provides access to a menu which allows you to display, download or erase the Audit Log, Alarm Log and Temperature Log. For more information on Log Functions, please refer to Section 4.8.

Availability: Administrator, SuperUser
Format: **`/L`** **[Enter]**

/AS Alarm Status Screen

Lists all available alarms and indicates whether or not an alarm has been triggered. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm as shown in the table below:

Alarm Name	Alarm Argument
Over Temperature (Initial)	OTI
Over Temperature (Critical)	OTC
Ping No Answer	PNA
Serial Port Invalid Access Lockout	LO
Power Cycle (Cold Boot)	CB
Alarm Input Alarm	AI
No Dialtone	ND

Availability: Administrator

Format: **`/AS [alarm]`** **[Enter]**

Where alarm is an optional argument, which can be used to display the status of an individual alarm as shown in the table above.

/J Display Site ID / Unit Information

Displays the user-defined Site I.D. message. If the optional asterisk (*) argument is included, the command can also display the model number, serial number, software version and other information regarding the AFS.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/J [*]`** **[Enter]**

Where **`*`** is an optional argument, which can be included in the command line to display the exact model number and software version of the AFS.

10.4.2. Control Commands

/X Exit CLI

Exits the user interface. When issued at the Network Port, also ends the session.

> **Note:** *If the /X command is invoked from within a configuration menu, recently defined parameters may not be saved. In order to make certain that parameters are saved, always press the **[Esc]** key to exit from all configuration menus and then wait until "Saving Configuration" message has been displayed and the cursor has returned to the command prompt before issuing the /X command.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: **`/X`** **[Enter]**

/C Connect

This command can be used to establish a bidirectional connection between the Serial Setup Port and the Network Port.

Notes:

- *User level accounts can only connect to the ports that are specifically permitted by the account.*
- *To terminate the connection, press **[Ctrl]**+**[X]** (`^x`) and then press **[Enter]**.*

Availability: Administrator, SuperUser, User
Format: **`/C 1 [x]`** **[Enter]**

/TA Toggle to "A" Position

Toggles a Circuit or a Circuit Group to the "A" position.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User
Format: **`/TA <c>[,Y]`** **[Enter]**

Where:

`c`	The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch to the "A" position. To apply the command to several Circuits, enter a plus sign (+) between each Circuit number. To apply the command to a range of Circuits, enter the numbers for the first and last Circuits in the range, separated by a colon character (:). To apply the command to all Circuits allowed by your account, enter an asterisk character (*).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "A" position without displaying the optional command confirmation prompt, invoke the following command line:

`/TA 2+3,Y` **[Enter]**

/TB Toggle to "B" Position

Toggles a Circuit or a Circuit Group to the "B" position.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/TB <c>[,Y]`** **[Enter]**

Where:

- **`c`** The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch to the "B" position. To apply the command to several Circuits, enter a plus sign (+) between each Circuit number. To apply the command to a range of Circuits, enter the numbers for the first and last Circuits in the range, separated by a colon character (:). To apply the command to all Circuits allowed by your account, enter an asterisk (**`*`**).
- **`,Y`** (Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "B" position without displaying the optional command confirmation prompt, invoke the following command line:

`/TB 2+3,Y` **[Enter]**

/T Toggle Command

This command can be used to toggle any Circuit or Circuit Group to either the "A" position or the "B: position.

> **`Note:`** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/T <c>,<p>[,Y]`** **[Enter]**

Where:

- **`c`** The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch. To apply the command to several Circuits, enter a plus sign (**+**) between each Circuit number. To apply the command to all Circuits allowed by your account, enter an asterisk character (**`*`**).
- **`p`** The desired switch position. Enter an "A" to switch specified circuits to the "A" position or a "B" to switch circuits to the "B" position.
- **`,Y`** (Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "A" position without displaying the optional command confirmation prompt, invoke the following command line:

`/T 2+3,A,Y` **[Enter]**

/DC Set All Circuits to Default States

Sets all Circuit Modules to their user-defined default state.

> **Note:** *When this command is invoked in Administrator Mode and SuperUser Mode, it will be applied to all AFS circuits. When invoked in User Mode, the command will only be applied to the Circuits that are allowed by your account.*

Availability: Administrator, SuperUser, User

Format: **`/DC[,Y]`** **[Enter]**

Where **`,Y`** is an optional command argument, which can be included to suppress the command confirmation prompt.

/DF Download Parameters to File

Sends all configuration parameters to a file on your server or system as described in Section 8.1.1. Saved configuration data can be transferred via serial port, FTP, SCP or TFTP.

Availability: Administrator

Format: **`/DF [ztp]`** **[Enter]**

/UL Unlock Port (Invalid Access Lockout)

Manually cancels the Invalid Access Lockout feature. When a series of failed login attempts are detected, the Invalid Access Lockout feature can shut down the effected port or protocol for a user specified time period in order to prevent further access attempts. When the /UL command is invoked, the AFS will immediately unlock all ports and protocols that are currently in the locked state.

Availability: Administrator

Format: /UL **[Enter]**

/TELNET Outbound Telnet

Creates an outbound Telnet connection.

Notes:

- *In order for the /TELNET command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 6.4. In addition, Telnet Access and Outbound Access must also be enabled via the Network Configuration menu, as described in Section 6.3.1.1.*
- *If you have logged in via the Network Port, the /TELNET command will not function.*

Availability: Administrator, SuperUser, User

Format: **`/TELNET <ip> [port] [raw]`** **[Enter]**

Where:

`ip`	Is the target IP address, in either IPv4 or IPv6 format.
`port`	Is an optional argument which can be included to indicate the target port at the IP address.
`raw`	Is an optional argument which can be included to indicate a raw socket connection. In order to create a raw socket connection, the command line must end with the text "**`raw`**".

/SSH Outbound SSH

Creates an outbound SSH connection.

Notes:

- *In order for the /SSH command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 6.4. In addition, SSH Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 6.3.1.1.*
- *If you have logged in via the Network Port, the /SSH command will not function.*

Availability: Administrator, SuperUser, User

Format: /SSH <ip> -l <username> **[Enter]**

Where:

ip	Is the target IP address, entered in either IPv4 or IPv6 format.
-l	(Lowercase letter "L") Indicates that the next argument will be the log on name.
username	Is the username that you wish to use to log in to the target device.

10.4.3. Configuration Commands

/F System Parameters

Displays a menu used to define general system parameters for the AFS. The System Parameters menu offers the following configuration options:

Parameter (Default)	Description
User Directory (Default = Undefined)	Provides access to a submenu which is used to create, view, edit and delete user accounts.
Site ID (Default = Undefined)	A text field, generally used to note the installation site or name for the AFS.
Real Time Clock (Default = Undefined)	Provides access to a submenu which is used to set and configure the Real Time Clock.
Invalid Access Lockout (Default = Off)	Provides access to a submenu which is used to set up the Invalid Access Lockout function.
Temperature Settings (Default = Undefined)	Provides access to a submenu which is used to select the Temperature Format and calibrate the temperature sensor.
Log Configuration	Provides access to a submenu which is used to enable/disable and configure the Audit Log, Alarm Log and Temperature Log.
Callback Security	Provides access to a submenu which is used to enable/disable and configure the Callback Security function as described in Section 6.1.4.
Control Card A/B Switch (Default = On)	Enables/disables the Manual A/B Selector Switch on the Control Card.
Control Card Reset Switch (Default = On)	Enables/disables the Manual Reset Switch on the Control Card.
Analog Modem Phone No. (Default = Undefined)	If the AFS includes the optional internal dial-up modem, this parameter can be used to record the phone number. When the AFS is used in conjunction with the WMU Enterprise Management Solution, the WMU will retrieve the phone defined here for use when contacting the unit via dial-up.
Scripting Options	Provides access to a submenu which is used to select Scripting Options as described in Section 6.1.5.
Asset Tag (Default = Undefined)	Allows a descriptive tag or tracking number to be assigned to the AFS. Once defined, the Asset Tag can be displayed via the Product Status Screen.
Location (Default = Undefined)	If desired, the physical location of the WTI unit can be noted here. When defined, the location will be displayed when the unit is queried via API calls and is also sent with Syslog / Splunk messages when the option is enabled.

Parameter (Default)	Description
Login Banner (Default = Undefined)	(Not present in Web Browser Interface) Allows definition of a banner message that is displayed after successful log in. The Login Banner can be used to post legal warnings or to display other user-defined information or instructions. **Notes:** • *Although the Login Banner will be displayed when the AFS is accessed via both the Text Interface and Web Browser Interface, the Login Banner can only be defined via the Text Interface.* • *The Login Banner can be up to 1024 characters long.* • *The Login Banner text must begin with the <banner> command and end with the </banner> command.* • *Banner text can be copied and pasted from a text editor, or sent from a file.* • *For best results, the individual text lines in the Login Banner should be less than 80 characters wide.*

Availability: Administrator

Format: **`/F`** **[Enter]**

/P Serial Setup Port Configuration

Displays a menu used to select parameters for the Serial Setup port. The Serial Setup Port Parameters menu offers the following configuration options:

Parameter (Default)	Description
Communication Settings	
Baud Rate (Default = 9600 bps)	Any standard rate from 300 bps to 230.4 kbps.
Bits/Parity (Default = 8-None)	The Data Bits and Parity settings for the Serial Port.
Stop Bits (Default = 1)	The Stop Bits setting for the Serial Port.
Handshake Mode (Default = None)	XON/XOFF, RTS/CTS (hardware), Both, or None.
General Parameters	
Administrator Mode (Default = Permit)	Permits/denies Setup Port access to Administrator level commands. When enabled (Permit), the port will be allowed to invoke Administrator level commands, providing they are issued by an account that permits them. If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access the CLI via this port. **Note:** *Administrator Mode cannot be disabled at the Setup Port.*
Logoff Character (Default = ^X)	Defines the CLI Logoff Character. In the CLI, the Logoff Character determines the command(s) or character(s) that must be issued at the Setup Port in order to disconnect.
Sequence Disconnect (Default = One Character)	Enables/Disables and configures the Resident Disconnect command in the CLI interface. This option allows users to disable the CLI Sequence Disconnect, select a one character format or a three character format.
Inactivity Timeout (Default = 5 Minutes)	Enables and selects the Timeout Period for the Setup Port. If enabled, the Setupl Port will disconnect when no additional data activity is detected for the duration of the timeout period.
Command Echo (Default = On)	Enables/Disables command echo for the CLI at the Setup Port. When disabled, commands sent to the Serial Port will still be invoked, but the keystrokes will not be displayed on your monitor.
Accept Break (Default = On)	Determines whether the Setup Port will accept breaks received from the attached device. When enabled, breaks received at the port will be passed to any port this port is connected to. When disabled, breaks will be refused at this port.

Parameter (Default)	Description
Port Mode Parameters	
Port Name (Default = Undefined)	Assigns a descriptive name to the Setup Port.
Port Mode (Default = Normal)	The operation mode for this port; Normal Mode, Modem Mode or Modem PPP Mode. For more information, please refer to Section 6.2.1.
DTR Output (Default = Pulse)	Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high.
Modem Parameters	(Modem Mode and Modem PPP Mode Only) Provides access to a submenu which is used to define the parameters described in the "Modem Mode Parameters" section of this table.
Modem Mode Parameters	
Modem Reset String (Default = ATZ)	(Modem Mode and Modem PPP Mode Only) Redefines the modem reset string. The Reset String can be sent prior to the Initialization string.
Modem Initialization String (Default = `AT&C1&D2S0=1&B1&H1&R2`)	(Modem Mode and Modem PPP Mode Only) Defines a command string that can be sent to initialize a modem to settings required by your application.
Modem Hang-Up String (Default = Undefined)	(Modem Mode and Modem PPP Mode Only) Although the AFS will pulse the DTR line to hang-up an attached modem, the Hang-Up string can be used for controlling modems that do not use the DTR line.
Reset/No Dialtone Interval (Default = 15 Minutes)	(Modem Mode and Modem PPP Mode Only) Defines the Periodic Modem reset duration, (which determines how often the Reset String will be sent to a modem at this port) and also sets the trigger value for the No Dialtone Alarm. If this value is set to "0," then the No Dialtone Alarm will not function.
No Dialtone Alarm Enable (Default = Off)	(Modem Mode and Modem PPP Mode Only) Enables/Disables the No Dialtone Alarm. This item must be enabled in order for the No Dialtone Alarm to function.
Reset/No Dialtone Scaler (Default = 15 Minutes)	(Modem Mode and Modem PPP Mode Only) Determines the number of Periodic Modem Reset sequences that must occur in order to initiate a No Dialtone Check. If set to "0," then the No Dialtone Alarm will not function. When both this parameter and the Reset/No Dialtone Interval are set to a value from 1 to 99 and the No Dialtone Alarm is enabled, the AFS will initiate a No Dialtone Check after a time period equal to the defined Reset/No Dialtone Interval value multiplied by the Reset/No Dialtone Scaler value.

Parameter (Default)	Description
Modem PPP Mode Parameters	
Modem Reset String (Default = ATZ)	(Modem Mode and Modem PPP Mode Only) Redefines the modem reset string. The Reset String can be sent prior to the Initialization string.
Modem Initialization String (Default = `ATQ0V1E1S0=0&C1&D2`)	(Modem Mode and Modem PPP Mode Only) Defines a command string that can be sent to initialize a modem to settings required by your application.
Modem Hang-Up String (Default = Undefined)	(Modem Mode and Modem PPP Mode Only) Although the AFS will pulse the DTR line to hang-up an attached modem, the Hang-Up string can be used for controlling modems that do not use the DTR line.
Reset/No Dialtone Interval (Default = 15 Minutes)	(Modem Mode and Modem PPP Mode Only) Defines the Periodic Modem reset duration, (which determines how often the Reset String will be sent to a modem at this port) and also sets the trigger value for the No Dialtone Alarm. If this value is set to "0," then the No Dialtone Alarm will not function. .
No Dialtone Alarm Enable (Default = Off)	(Modem Mode and Modem PPP Mode Only) Enables/Disables the No Dialtone Alarm. This item must be enabled in order for the No Dialtone Alarm to function.
Reset/No Dialtone Scaler (Default = 16 Minutes)	(Modem Mode and Modem PPP Mode Only) Determines the number of Periodic Modem Reset sequences that must occur in order to initiate a No Dialtone Check. If set to "0," then the No Dialtone Alarm will not function. When both this parameter and the Reset/No Dialtone Interval are set to a value from 1 to 99 and the No Dialtone Alarm is enabled, the AFS will initiate a No Dialtone Check after a time period equal to the defined Reset/No Dialtone Interval value multiplied by the Reset/No Dialtone Scaler value.
Periodic Reset Location (Default = Undefined)	(Modem PPP Mode Only) The IP address or URL for the website that will be used to keep the PPP connection alive when not in use. The AFS will regularly ping the selected IP address or URL to keep the connection alive. **Notes:** • *In order to select a domain name as the Periodic Reset Location, you must first define the Domain Name Servers as described in Section 6.3.1.6.1.* • *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication is started.*
PPP Phone Number (Default = Undefined)	(Modem PPP Mode Only) The phone number for the line that will be used for PPP communication.
Username (Default = Undefined)	(Modem PPP Mode Only) The username for the ISP account that will be used for PPP communication.
Password (Default = Undefined)	(Modem PPP Mode Only) The password for the ISP account that will be used for PPP communication.

Parameter (Default)	Description
Modem PPP Mode Parameters (*continued*)	
IP Address (Default = Undefined)	(Modem PPP Mode Only) The temporary IP address assigned to the PPP communication session by the ISP. This item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is initiated.
P-t-P (Default = Undefined)	(Modem PPP Mode Only) Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started.
Subnet Mask (Default = Undefined)	(Modem PPP Mode Only) Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started.

Availability: Administrator

Format: **`/P`** **[Enter]**

Where **<n>** is the number or name of the desired serial port.

/PC Set Circuit Parameters

Displays a menu that is used to assign names and select default status for the AFS's switched circuits. The Set Circuit Parametes Menu allows you to define a name for each circuit, and also assign a name to the default status for each circuit. All functions provided by the /PC command are also available via the Web Browser Interface.

Availability: Administrator

Format: **`/PC`** **[Enter]**

/G Circuit Group Parameters

Displays a menu that is used to View, Add, Modify or Delete Circuit Groups. When Circuit Groups are created, this menu is used to name each Circuit Group and assign circuits to be included in each group.For more information on Circuit Groups, please refer to Section 6.6. The Add Circuit Group menu offers the following configuration options:

Parameter (Default)	Description
Circuit Group Name (Default = Undefined)	Assigns a descriptive name to the Circuit Group.
Circuit Access (Default = Undefined)	Determines which switched circuits will be included in this Circuit Group.

Availability: Administrator

Format: **`/G`** **[Enter]**

/N* Network Selection Menus Selection - IPv4/IPv6

Displays a the Network Selection menu, which is used to access the configuration menus for the Network Port for IPv4 and IPv6 protocols. Network Selection Menu offers access to two network port configuration menus:

- **[eth0] IPv4:** Network Port, IPv4 and Shared Parameters
- **[eth0] IPv6:** Network Port, IPv6 Parameters

Availability: Administrator

Format: **/N* [Enter]**

The **/N*** command provides access to the following submenus:

Network Parameters [eth0] IPv4 (Shared)

This menu is used to define IPv4 communication parameters for the Ethernet Port (eth0) plus Shared parameters. The eth0, Shared menu offers the following options:

Parameter (Default)	Description
Communication Settings	
IP Address (Default = 192.168.168.168)	The IPv4 format address for the Ethernet Port, eth0. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the AFS via the CLI as described in Section 3.3.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the Ethernet Port, eth0. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the AFS via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the Ethernet Port, eth0. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the AFS via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol, defines the DHCP Host Name and Lease Time, enables/disables the ability to automatically Obtain DNS addresses, enables/disables DNS Server Update and enables/disables the Default Gateway. When DHCP is enabled, the AFS will perform a DHCP request. In the CLI, the MAC address is listed on the Network Status Screen. **Notes:** • *Prior to configuring this feature, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the AFS.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the AFS via the CLI.*

Parameter (Default)	Description
Communication Settings (*continued*)	
IP Tables (Default = Undefined)	Allows the AFS to restrict unauthorized IP addresses from establishing inbound connections as described in Section 6.1.3.4.
Static Route (Default = Undefined)	Allows definition of Linux routing commands that will be automatically executed each time a user accesses the user interface via this Ethernet Port.
DNS Services (Default = Undefined)	This option is used to define DNS and DDNS parameters. In the [eth0] IPv4 menu, the DNS option is used to access either the DNS Parameters menu or the DDNS parameters menu. For more information, please refer to Section 6.3.1.6.
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the AFS negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the AFS's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the AFS's Negotiation parameter should be set to match the other device* (e.g., "100/Full.)
General Parameters	
Administrator Mode (Default = Permit)	Permits/denies access to the Ethernet Port by accounts that allow Administrator level commands. When enabled (Permit), the Administrator Mode accounts will be allowed to access the user interface via the Ethernet Port. If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access the user interface via the Ethernet Port.
Logoff Character (Default = ^X ([Ctrl]+[X]))	Defines the CLI Logoff Character for the Ethernet Port. This determines the command that must be issued at this port in order to disconnect from a second port. **Note:** The Sequence Disconnect parameter can be used to pick a one character or a three character logoff sequence.
Sequence Disconnect (Default = One Character)	Enables/Disables and configures the Resident Disconnect command for the CLI. Offers the option to either disable the Sequence Disconnect, or select a one character, or three character command format. **Notes:** • *The One Character Disconnect is intended for situations where the destination port should not receive the disconnect command. When the Three Character format is selected, the disconnect sequence will pass through to the destination port prior to breaking the connection.* • *When the Three Character format is selected, the Resident Disconnect uses the format "**[Enter]**`LLL`**[Enter]**", where* `L` *is the selected Logoff Character.*

Parameter (Default)	Description
General Parameters (*continued*)	
Inactivity Timeout (Default = 5 Minutes)	Enables and selects the Inactivity Timeout period for the Ethernet Port. If enabled, and the port does not receive or transmit data for the specified time period, the port will disconnect.
Command Echo (Default = On)	Enables or Disables command echo for the Ethernet Port.
Accept Break (Default = On <ASCII 28>)	Determines how the Ethernet Port will handle breaks received from the attached device. When disabled, all break codes are ignored and passed through untouched to the serial port. When enabled, ASCII 28 and/or IETF/RFC4335 SSH break sequences are stripped and a 'break' sequence is initiated on the connected serial port.
Servers and Clients	
Telnet Access (Default = Off)	Enables/disables Telnet access to the Ethernet Port, sets the Telnet Port Number and determines the maximum number of sessions that will be allowed per user MAC address. **Notes:** • *When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the Ethernet Port(s) or initiate outbound Telnet connections.* • *After changing the "Per Source" parameter, you must log out of all pre-existing sessions in order for the new maximum value to be applied.*
SSH Access (Default = On)	Enables/disables SSH communication at the Ethernet Port, selects the SSH Port Number, sets the SSH Security Level, enables/disables the SSH View Port function and SSH View Port Bidirectional function.
Web Access (Default = Off)	Provides access to the Web Access and SSL Certificates menu. Enables/disables/configures HTTP access and HTTPS access.
SYSLOG Address (Default = Undefined)	Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the AFS.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the Ethernet Port (eth0.) For more information, please refer to Section 6.3.1.10. **Note:** *After you have configured SNMP Access Parameters, control circcuit switching and display unit status via SNMP, as described in Appendix G.*
SNMP Traps (Default = Undefined)	Selects parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Section 6.3.1.11.
LDAP (Default = Off)	Provides access to a submenu that is used to define parameters for LDAP and Kerberos authentication protocols and LDAP Group Setup. Please refer to Section 6.3.1.12.

Parameter (Default)	Description
Servers and Clients (*continued*)	
TACACS (Default = Off)	Provides access to a submenu that is used to define TACACS parameters and Default TACACS User Access as described in Section 6.3.1.13.
RADIUS (Default = Off)	Provides access to a submenu that is used to define parameters for RADIUS authentication per Section 6.3.1.14.
Ping Access (Default = Allow All Pings)	Configures the AFS's response to ping commands at the Ethernet Port (eth0). **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*
Multiple Logins (Default = On)	Enables/disables multiple logins.
Email Messaging (Default = Off)	Provides access to a submenu that is used to defined parameters for Email notifications.
Raw Socket Access (Default = Off)	Enables/Disables Raw Socket Protocol access to the Ethernet Port(s) via Direct Connect and selects either port 3001 or 23 for Raw Socket Access.

Network Parameters [eth0] IPv6

This menu is used to define IPv6 communication parameters for the Ethernet Port (eth0.) The eth0, Shared menu offers the following options:

Parameter (Default)	Description
Communication Settings	
IP Address (Default = Undefined)	The IPv6 format address for the Ethernet Port, eth0. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the AFS via the CLI.*
Subnet Prefix (Default = Undefined)	The IPv6 Subnet Prefix for the Ethernet Port, eth0. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the AFS via the CLI.*
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the Ethernet Port, eth0. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the AFS via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol, defines the Host Name, defines the Lease Time, enables/disables the ability to automatically Obtain DNS addresses, enables/disables DNS Server Update and enables/disables the Default Gateway. When DHCP is enabled, the AFS will perform a DHCP request. **Notes:** • *Prior to configuring this feature, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the AFS.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the AFS via the CLI.*
IP Tables (Default = Undefined)	Allows the AFS to restrict unauthorized IP addresses from establishing inbound connections as described in Section 6.3.2.2.
Static Route (Default = Undefined)	Allows definition of Linux routing commands that will be automatically executed each time a user accesses the user interface via the Ethernet Port.
DNS Services (Default = Undefined)	This option is used to define DNS parameters. For more information, please refer to Section 6.3.2.4.
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the AFS negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the AFS's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the AFS's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*

Parameter (Default)	Description
Servers & Clients	
Web Access (Default = Off)	Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access. .
SYSLOG Address (Default = Off)	Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the AFS.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv6 format access parameters for the SNMP feature at the Ethernet Port (eth0.) For more information, please refer to Section 6.3.2.8. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the AFS's User Directory, control circuit switching and display unit status via SNMP, as described in Appendix G.*
SNMP Traps (Default = Off)	Selects parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Section 6.3.2.9.
Ping Access (Default = Allow)	Configures the AFS's response to ping commands at the Ethernet Port (eth0). **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm*.
Email Messaging (Default = Off)	Provides access to a submenu that is used to defined parameters for Email notifications.

/PNA Ping No Answer Configuration Parameters

Displays a menu used to define Ping No Answer parameters. The Ping No Answer menu allows you to add, delete, modify or view Ping No Answer operations. When Ping No Answer IP addresses have been defined and the Ping No Answer Alarm has been enabled, the AFS can ping those IP addresses and notify you when those IP addresses fail to respond to ping commands. For more information, please refer to Section 6.9.3.

The Add Ping No Answer menu offers the following configuration options:

Parameter (Default)	Description
IP Address or Domain Name (Default = Undefined)	The IP address or Domain Name that you wish to Ping. **Note:** *In order to use domain names, DNS Server parameters must first be defined per Section 6.3.1.6.*
Ping Interval (Default = 60 Seconds)	Determines how often the Ping command will be sent. Can be any whole number, from 1 to 3,600 seconds. **Note:** *If the Ping Interval is set lower than 20 seconds, it is recommended to define the "IP Address or Domain Name" parameter using an IP Address rather than a Domain Name. This ensures more reliable results in the event that the Domain Name Server is unavailable.*
Interval After Failed Ping (Default = 10 Seconds)	Determines the delay period between failed Ping attempts.
Ping Delay After PNA Action (Default = 15 Minutes)	Determines how long the AFS will wait to send additional Ping commands, after a Ping-No-Answer action has been initiated. Typically, this option is used to allow time for a device to fully "wake up" after a Ping-No-Answer action attempting to Ping the device again.
Consecutive Failures (Default = 5)	Determines how many consecutive failures to respond to a Ping command must be detected in order to initiate a Ping-No-Answer action.
PNA Action (Default = Continuous Alarm)	Determines how the AFS will react when the IP address fails to respond to a ping.
Ping Test	Pings the Address specified in the "IP Address or Domain Name" Field.

Availability: Administrator

Format: **`/PNA`** **[Enter]**

/AC Alarm Configuration Parameters

Displays a menu used to configure and enable the AFS's monitoring and alarm functions. When properly configured and enabled, these Alarm Functions can provide notification when numerous conditions are detected by the AFS. For more information on Alarm Configuration, please refer to Section 6.9. The Alarm Configuration Menu allows the following alarms to be defined:

Alarm Name (Default)	Description
Over Temperature (Initial) (Default = On - 110 Degrees F)	Provides notification when the temperature level reaches a point that might indicate a potential problem.
Over Temperature (Critical) (Default = On - 120 Degrees F)	Provides notification when the temperature level reaches a point that indicates a hazardous condition.
Ping No Answer (Default = On)	Provides notification when a device at a target IP address fails to respond to a ping command.
Serial Port Invalid Access Lockout (Default = On)	Provides notification when the AFS has locked serial ports due to repeated, invalid attempts to access the user interface via serial port.
Power Cycle (Cold Boot) (Default = On)	Provides notification when all input power to the AFS unit is lost and then restored.
Alarm Input Alarm (Default = On)	Monitors pin 4 on the Control Module's AUX connector.
No Dialtone (Default = On)	Monitors a telephone line connected to an external modem installed at the AFS's Setup Port, and then provides notification if the phone line is dead or no dialtone is present.

Availability: Administrator

Format: `/AC` **[Enter]**

/I Reboot System (Default)

Re-initializes the AFS and offers the option to either retain user-defined parameters or reset to default parameters. As described in Section 8.3, the /I command can also be used to restore the unit to previously saved parameters. When the /I command is invoked, the unit will offer four reboot options:

- Reboot Only (Do NOT default parameters)
- Reboot & Default (Keep IP Parameters & SSH Keys; Default all other parameters)
- Reboot & Default (Default ALL parameters)
- Reboot & Restore Last Known Working Configuration

Availability: Administrator

Format: `/I` **[Enter]**

/UFW Upgrade Software

When new versions of the AFS software become available, this command can be used to update existing software as described in Section 9.2.

Notes:

- *The WMU Enterprise Management Utility is the preferred method for managing AFS software upgrades. The /UFW command is intended to provide an alternative to the WMU. For more information, please refer to Section 9.1.*
- *When a software upgrade is performed, the AFS will require 15 minutes for the upgrade procedure.*

The Upgrade Software menu offers four options:

1. **Servers:** Enables/disables FTP, SFTP and TFTP Servers.
2. **Upload Software:** Provides access to a submenu used to initiate uploading of the MD5 format Software Update File.
3. **Upload Parameters:** Provides access to a submenu used to initiate uploading of the XML format Saved Parameters File.
4. **Incremental Upgrade Options:** This option is used when installing partial upgrades, such as security patches.

Availability: Administrator
Format: **`/UFW`** **[Enter]**

/TEST Test Network Parameters

Displays a menu which is used to test configuration of the Syslog and SNMP Trap functions and can also be used to ping a user-selected IP address.

Notes:

- *In order for a ping test to function properly, your network and/or firewall and the target device must be configured to allow ping commands.*
- *In order for the ping command to function with domain names, Domain Name Server parameters must be defined as described in Section 6.3.1.6.1.*
- *The Test Menu's Ping command is not effected by the status of the Network Parameters Menu's Ping Access function.*

Availability: Administrator
Format: **`/TEST`** **[Enter]**

/VPN VPN Configuration

Provides a menu used to defined parameters for IPSec and OpenVPN.

Availability: Administrator
Format: **`/VPN`** **[Enter]**

Appendix A. Customer Service

Customer Service hours are from 8:00 AM to 5:00 PM, PST, Monday through Friday. When calling, please be prepared to give the name and make of the unit, its serial number and a description of its symptoms. If the unit should need to be returned for factory repair it must be accompanied by a Return Authorization number from Customer Service.

WTI Customer Service
5 Sterling
Irvine, California 92618

Local Phone: (949) 586-9950
Toll Free Service Line: 1-888-280-7227
Service Fax: (949) 583-9514

Email: service@wti.com

Appendix B. Automation

AFS units support both Ansible 2.7 and RESTful API.

- For more information regarding Ansible 2.7, please refer to the WTI.com Knowledge Base.
- For more information regarding RESTful API, please refer to the WTI.com Knowledge Base.

Appendix C. Zero Touch Provisioning (ZTP)

Zero Touch Provisioning (ZTP) provides network administrators with an automated solution for configuring newly added network elements without the need to have a network engineer present at the installation site. ZTP works with your DHCP server to automatically assign vital configuration parameters to newly installed devices without user intervention. This drastically reduces downtime due to user configuration errors, cuts the time required to configure new devices and eliminates the delays and expenses associated with a physical service call to the remote network equipment site.

For more information regarding the ZTP capabilities provided by the AFS, please refer to the WTI.com Knowledge Base.

Appendix D. SSH & Telnet Functions

D.1. Network Port Numbers

Whenever an inbound SSH or Telnet session connects to the serial port on the AFS, the Port Status Screen and Port Diagnostics Screen will indicate that the serial port is presently connected to Port “Nn” (where “N” indicates a network connection, and “n” is a number that lists the logical Network Port being used; for example, “N11”.) This “Nn” number is referred to as the logical Network Port Number.

D.2. SSH Encryption

The AFS supports SSH connections, which provide secure, encrypted access via network. In order to communicate with the AFS using SSH protocol, your network node must include an appropriate SSH client.

Note that in the Command Line Interface (CLI,) when the /K (Send SSH Key) command is invoked, the AFS can also provide you with a public SSH key, which can be used to streamline connection when using SSH protocol.

Although you can establish an SSH connection to the unit without the public key, the public key provides validation for the AFS, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the AFS is not a recognized user when the client attempts to establish a connection.

In the CLI, the /K command uses the following format:

`/K <k>` [Enter]

Where **`k`** is an argument that determines which type of public key will be displayed. The **`k`** argument offers the following options:

1. SSH1
2. SSH2 RSA
3. SSH2 DSA

For example, to obtain the public SSH key for an SSH2 RSA client, type **`/K 2`** and then press **[Enter]**.

Notes:

- *Although the AFS does not support SSH1, the /K 1 command will still return a key for SSH1.*
- *For instructions regarding setting up SSH Public Key Authentication, please refer to the WTI.com Knowledge Base.*
- *For information regarding RSA SecurID Ready Implementation, please refer to* the *WTI.com Knowledge Base.*

Appendix E. Syslog Messages

The Syslog feature can create log records of each Alarm Event. As these event records are created, they are sent to a Syslog Daemon, located at an IP address defined via the Network Parameters menu.

E.1. Configuration

In order to employ this feature, you must set the real-time clock and calendar via the System Parameters Menu, and define the IP address for the Syslog Daemon via the Network Port Configuration menu.

To configure the Syslog function, please proceed as follows:

1. **Access the User Interface:** Note that the following configuration menus are only available to accounts that permit Administrator level commands.

2. **System Parameters Menu:** Access the System Parameters Menu, then set the following parameters:

   a) **Set Clock and Calendar:** Set the Real Time Clock and Calendar and/or configure and enable the NTP server feature.

3. **Network Parameters Menu:** Access the Syslog Parameters Menu and set the following parameters:

   a) **Syslog IP Address:** Determine the IP address for the device that will run the Syslog Daemon, then use the Network Port Configuration menu to define the IP address for the Syslog Daemon.

   Notes:

   - *The Network Parameters Menu allows the definition of IP addresses for both a primary Syslog Daemon and an optional secondary Syslog Daemon.*
   - *The Syslog Address submenu in the Command Line Interface (CLI) includes a Ping Test function that can be used to ping the user-selected Syslog IP Address to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

4. **Syslog Daemon:** In order to capture messages sent by the AFS, a computer must be running a Syslog Daemon (set to UDP Port 514) at the IP address(es) specified in Step 3 above.

Once the Syslog Address is defined, Syslog messages will be generated whenever one of the alarms discussed in Section 6.9 is triggered.

Appendix F. SNMP Traps

The SNMP Trap function allows the AFS to send Alarm Notification messages to two different SNMP managers, each time one of the Alarms discussed in Section 6.9 is triggered.

Note:

- *To enable the SNMP Trap feature, you must define at least one SNMP Manager. SNMP Traps are automatically enabled when at least one SNMP Manager has been defined.*
- *The SNMP feature cannot be configured via the SNMP Manager.*
- *SNMP reading ability is limited to the System Group.*
- *The SNMP feature includes the ability to be polled by an SNMP Manager.*
- *Once SNMP Trap Parameters have been defined, SNMP Traps will be sent each time an Alarm is triggered.*

F.1. Alarm Notification via SNMP Traps

For most of the available AFS alarm functions, all that is needed in order to enable notification via SNMP Trap, is to access the user interface using an account that allows Administrator level commands and then use the Network Configuration menu's SNMP Traps submenu to define the following parameters:

1. **SNMP Managers 1 through 4:** The address(es) that will receive SNMP Traps generated by the alarms. Consult your network administrator to determine the IP address(es) for the SNMP Manager(s), then use the SNMP Trap menu to set the IP address for each SNMP Manager. Note that it is not necessary to define both SNMP Managers.

   Notes:

   - *The SNMP Trap submenu includes a Ping Test function that can be used to ping the user-selected SNMP Managers to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
   - *There are separate submenus for defining IPv4 and IPv6 SNMP Managers.*

2. **Trap Community:** Consult your network administrator, and then use the Network Parameters menus to set the Trap Community.

Once SNMP Trap parameters have been defined, the AFS will send an SNMP Trap each time an alarm is triggered.

Appendix G. Operation via SNMP

If SNMP Access Parameters have been defined as described in Section 6.3.1.10, then you will be able to manage user accounts and switching and display unit status via SNMP. This section describes SNMP communication with the AFS, and lists some common commands that can be employed to manage users, control switching and display unit status.

G.1. AFS SNMP Agent

The AFS SNMP Agent supports various configuration, control, status and event notification capabilities. Managed objects are described in the wti-afs-mib.txt file, which is available via the Downloads page at **https://www.wti.com**. The MIB document can be compiled for use with your SNMP client.

Notes:

- *The AFS SNMP Agent provides compatibility with a wide variety of Device Center Information Management Packages (DCIM.) For more information, please refer to the remainder of this section, and the WTI.com Knowledge Base.*
- *For information regarding the procedure for Importing WTI Alert Definitions into Solarwinds Orion NPM, please refer to the WTI.com Knowledge Base.*

G.2. SNMPv3 Authentication and Encryption

The major limitations of SNMPv2 were the failure to include proper username/password login credentials (v2 only used a password type of login, i.e., community name) and the exclusion of encryption for data moving over the internet. SNMPv3 addresses both of these shortcomings.

For SNMPv3, the AFS supports two forms of Authentication/Privacy: Auth/noPriv which requires a username/password, but does not encrypt data going over the internet and Auth/Priv which requires a username/password AND encrypts the data going over the internet using DES (AES is not supported at this time). For the Password protocol, the AFS supports either MD5 or SHA1.

G.3. Configuration via SNMP

AFS User accounts can be viewed, created, modified, and deleted via SNMP. User accounts are arranged in a table of 128 rows, and indexed 1-128. User account parameters, as seen through the SNMP, are summarized below.

- **`userTable::userName`** – 32 character username
- **`userTable::userPasswd`** – 16 character password
- **`userTable::userAccessLevel`** – Account access level.
  `0` – View Only Access
  `1` – User Access
  `2` – SuperUser Access
  `3` – Administrator Access
- **`userTable::userPlugAccess`** – A string of up to 16 characters, with one character for each of the 16 possible circuits on the AFS. A '`0`' indicates that the account does not have access to the circuit, and a '`1`' indicates that the user does have access to the circuit.
- **`userTable::userPortAccess`** – A '`0`' indicates that the account does not have access to the Serial Port, and a '`1`' indicates that the user does have access to the port.
- **`userTable::userGroupAccess`** – A string of 54 characters, with one character for each of the 54 possible circuit groups in the system. A '`0`' indicates that the account does not have access to the circuit group, and a '`1`' indicates that the user does have access to the circuit group.
- **`userTable::userSerialAccess`** – Access to the serial interface
  `0` – No access
  `1` – Access
- **`userTable::userTelnetSshAccess`** – Access to the Telnet/SSH interface
  `0` – No access
  `1` - Access
- **`userTable::userOutboundTelSshAccess`** – Access to Outbound Telnet/SSH
  `0` – No access
  `1` - Access
- **`userTable::userWebAccess`** – Access to the Web interface
  `0` – No access
  `1` - Access

- **`userTable::userCallbackNum1`** – The first 32 character callback number for this account
- **userTable::userCallbackNum2** – The second 32 character callback number for this account
- **`userTable::userCallbackNum3`** – The third 32 character callback number for this account
- **`userTable::userCallbackNum4`** – The fourth 32 character callback number for this account
- **`userTable::userCallbackNum5`** – The fifth 32 character callback number for this account
- **`userTable::userSubmit`** – Set to 1 to submit changes.

G.3.1. Viewing Users

To view users, issue a GET request on any of the user parameters for the index corresponding to the desired user.

G.3.2. Adding Users

For an empty index, issue a SET request on the desired parameters. Minimum requirement is a username and password to create a user, all other parameters will be set to defaults if not specified. To create the user, issue a SET request on the userSubmit object.

G.3.3. Modifying Users

For the index corresponding to the user you wish to modify, issue a SET request on the desired parameters to be modified. Once complete, issue a SET request on the userSubmit object.

G.3.4. Deleting Users

For the index corresponding to the user you wish to delete, issue a SET request on the username with a blank string. Once complete, issue a SET request on the userSubmit object.

G.4. Circuit Control via SNMP

G.4.1. Controlling Circuits

ON, OFF, BOOT, and DEFAULT commands can be issued for plugs/circuits via SNMP. Plugs or circuits are arranged in a table of N rows, where N is the number of plugs/circuits in the system. Plug/circuit parameters are described below.

- **`plugTable::plugID`** – String indicating the circuit's ID
- **`plugTable::plugName`** - String indicating the circuit's user-defined name.
- **`plugTable::plugStatus`** – Current state of the circuit
  - **`0`** – Circuit is OFF
  - **`1`** – Circuit is ON
- **`plugTable::plugAction`** – Action to be taken on circuit
  - **`1`** – Mark to turn ON (does not execute)
  - **`2`** – Mark to turn OFF (does not execute)
  - **`3`** – Mark to BOOT (does not execute)
  - **`4`** – Mark to DEFAULT (does not execute)
  - **`5`** – Mark to turn ON and execute plug/circuit actions
  - **`6`** - Mark to turn OFF and execute plug/circuit actions
  - **`7`** - Mark to BOOT and execute plug/circuit actions
  - **`8`** - Mark to DEFAULT and execute plug/circuit actions

Set **`plugTable::plugAction`** to desired action, as specified by values 1-4 above, for each plug/circuit index the action is to be applied to. For the last plug/circuit you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

G.4.2. Controlling Circuit Groups

ON, OFF, BOOT, and DEFAULT commands can be issued for circuit groups via SNMP. Circuit Groups are arranged in a table of 54 rows, one row for each circuit group in the system. Circuit Group parameters are described below.

- **`plugGroupTable::plugGroupName`** – String indicating the plug/circuit group's name
- **`plugGroupTable::plugGroupAction`** – Action to be taken on plug/circuit group
  - **`1`** – Mark to turn ON (does not execute)
  - **`2`** – Mark to turn OFF (does not execute)
  - **`3`** – Mark to BOOT (does not execute)
  - **`4`** – Mark to DEFAULT (does not execute)
  - **`5`** – Mark to turn ON and execute plug/circuit group actions
  - **`6`** - Mark to turn OFF and execute plug/circuit group actions
  - **`7`** - Mark to BOOT and execute plug/circuit group actions
  - **`8`** - Mark to DEFAULT and execute plug/circuit group actions

Set **`plugGroupTable::plugGroupAction`** to desired action, as specified by values 1-4 above, for each plug/circuit group index the action is to be applied to. For the last plug/circuit group you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

G.5. Configuring Serial Ports

Commands can be issued to set certain serial port configuration parameters via SNMP. Ports are arranged in a table of up to 41 rows, with one row for each possible serial port. Serial port parameters are described below.

- **`portTable::portID`** – String indicating the serial port's ID
- **`portTable::portThreshold`** – An integer that sets the serial port's Buffer Threshold value. If this value is set between 1 and 32,757, then the SNMP trap function is enabled and traps will be sent to the SNMP Managers whenever the buffer for this port reaches the specified level. If set to "0" (zero), then SNMP Traps related to the Buffer Threshold will be disabled at this port.
- **`portTable::portStatus`** - Shows the connection status of each port. If a port is connected, the portStatus object will return the number of the other port in the connection pair.
- **`free`** - Disconnect port.

G.6. Viewing Unit Status via SNMP

Status of various components of the AFS can be retrieved via SNMP. Circuit Status, and Environmental Status are currently supported.

G.6.1. System Status - Ethernet Port MAC Addresses

The MAC Address for Ethernet Port 0 (eth0) can be displayed using the command below:

- **`environmentUnitTable::environmentMacEth0`** - The MAC Address for Ethernet Port 0 (eth0.)

G.6.2. Power Input Status

The status of each power inlet can be displayed using the command below:

- **`environmentUnitTable::environmentInputPower1`** - Status of the first power input

G.6.3. Circuit Status

Note: *The power control functions described here are only available on WTI Power Control products and WTI Console Server + Power Control products.*

The status of each plug/circuit in the system can be retrieved using the command below.

- **`plugTable::plugStatus`** – The status of the plug (or circuit.)
  `0` – Plug/circuit is OFF
  `1` – Plug/circuit is ON

G.6.4. Unit Temperature Status

The temperature status can be retrieved for various variables for the AFS. The environmentUnitTable contains one row.

- **`environmentUnitTable::environmentUnitTemperature`** – The temperature of the AFS.
- **`environmentUnitTable::environmentUnitName`** – Returns the specific model number for the AFS.

G.6.5. Serial Number

Displays the serial number of the AFS.

- **`environmentUnitTable::environmentSerialNumber`** - The serial number of the AFS.

G.6.6. Alarm Status

The status of the AFS's alarm functions can be retrieved and displayed using the following commands:

Notes:

- *When an alarm status command returns a zero (0), this indicates that the alarm is inactive.*
- *When an alarm status command returns a one (1), this indicates that the alarm is active (triggered.)*

- **`alarmTables::alarmOverCurrentInitial`** - (Products with Current Monitoring Capabilities Only) Displays the status of the Over Current (Initial) Line Alarm.
- **`alarmTables::alarmOverCurrentCritical`** - (Products with Current Monitoring Capabilities Only) Displays the status of the Over Current (Critical) Line Alarm.
- **`alarmTables::alarmOverTemperatureInitial`** - Displays the status of the Over Temperature (Initial) Alarm.
- **`alarmTables::alarmOverTemperatureCritical`** - Displays the status of the Over Temperature (Critical) Alarm.
- **`alarmTables::alarmCircuitBreakerOpen`** - (Breakered Units Only) Displays the status of the Circuit Breaker Open Alarm.
- **`alarmTables::alarmCommLoss`** - Displays the status of the Lost Communication Alarm.
- **`alarmTables::alarmPingNoAnswer`** - Displays the status of the Ping-No-Answer Alarm.
- **`alarmTables::alarmInvalidAccessLockout`** - Displays the status of the Serial Port Invalid Access Lockout Alarm.
- **`alarmTables::alarmPowerCycle`** - Displays the status of the Power Cycle Alarm.

- **`alarmTables::alarmBufferThreshold`** - Displays the status of the Buffer Threshold Alarm.
- **`alarmTables::alarmPlugCurrent`** - (Products with Current Monitoring Capabilities Only) Displays the status of the Plug Current Alarm.
- **`alarmTables::alarmLostOptoVoltage`** - (Units with Two or More Power Inlets Only) Displays the status of the Lost Voltage Alarm.
- **`alarmTables::alarmEmergencyShutoff`** - (WTI Power Control products and WTI Console Server + Power Control Combo products Only) Displays the status of the Emergency Shut Off feature. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at **service@wti.com**.
- **`alarmTables::alarmNoDialtone`** - Displays the status of the No Dialtone Alarm.
- **`alarmTables::alarmWakeupOnFailure`** - Displays the status of the Wakeup on Failure Alarm.

G.7. Sending Traps via SNMP

Traps that report various unit conditions can be sent to an SNMP Management Station from the AFS. The following traps are currently supported.

- **`WarmStart`** Trap – Trap indicating a warm start
- **`ColdStart`** Trap – Trap indicating a cold start
- **`Test`** Trap – Test trap invoked by user via the Command Line Interface (CLI)

The AFS can send an SNMP trap to notify you when any of the available AFS alarm functions have been triggered. In all cases except the Power Cycle Alarm, there will be one trap sent when the alarm is triggered, and a second trap sent when the alarm is cleared. For more information on alarm functions, please refer to Section 6.9.

- **`Alarm Trap`** – Trap indicating an alarm condition. A trap with a unique enterprise OID is defined for the Invalid Access Lockout Alarm, under which specific trap-types are defined to indicate the setting or clearing of that particular alarm condition. There are separate traps for the Invalid Access Lockout Alarm. The Alarm includes a "Set Trap," which indicates that the alarm has been triggered, and a "Clear Trap," which indicates that the alarm has been cleared.
- **`overCurrentInitialSetTrap`** - (Products with Current Monitoring Capabilities Only) Indicates that the Over Current (Initial) Alarm has been triggered.
- **`overCurrentInitialClearTrap`** - (Products with Current Monitoring Capabilities Only) Indicates that the Over Current (Initial) Alarm has been cleared.
- **`overCurrentCriticalSetTrap`** - (Products with Current Monitoring Capabilities Only) Indicates that the Over Current (Critical) Alarm has been triggered.
- **`overCurrentCriticalClearTrap`** - (Products with Current Monitoring Capabilities Only) Indicates that the Over Current (Critical) Alarm has been cleared.
- **`overTemperatureInitialSetTrap`** - Indicates that the Over Temperature (Initial) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **`overTemperatureInitialClearTrap`** - Indicates that the Over Temperature (Initial) Alarm has been cleared.
- **`overTemperatureCriticalSetTrap`** - Indicates that the Over Temperature (Critical) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **`overTemperatureCriticalClearTrap`** - Indicates that the Over Temperature (Critical) Alarm has been cleared.
- **`lostCommSetTrap`** - Indicates that the Lost Communication Alarm has been triggered.
- **`lostCommClearTrap`** - Indicates that the Lost Communication Alarm has been cleared.

- **`pingNoAnswerSetTrap`** - Indicates that the Ping No Answer Alarm has been triggered. The trap will also include a numerical value that indicates the IP address of the device that failed to respond to the ping command.
- **`pingNoAnswerClearTrap`** - Indicates that the Ping No Answer Alarm has been cleared.
- **`lockoutSetTrap`** - Indicates that the Invalid Access Lockout Alarm has been triggered. The trap will also include a numerical value that indicates the number of the serial port where the lockout occurred.
- **`lockoutClearTrap`** - Indicates that the Invalid Access Lockout Alarm has been cleared.
- **`powercycleSetTrap`** - Indicates that the Power Cycle Alarm has been triggered (Note that there is no corresponding Clear Trap for the Power Cycle Alarm.)
- **`bufferThresholdCrossedSetTrap`** - Indicates that the amount of data in the serial port buffer has exceeded the currently defined Buffer Threshold value. The trap will also include a the number of the port where the Buffer Threshold Alarm was generated, and a numerical value that indicates the amount of data currently stored in the port buffer.
- **`bufferThresholdCrossedClearTrap`** - Indicates that the data in the port buffer has either been read or erased and that the Buffer Threshold Alarm has been cleared.

- **`emergencyShutoffSetTrap`** - (WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Indicates that an emergency shut off has been implemented. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at service@wti.com.
- **`emergencyShutoffClearTrap`** - (WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Indicates that an emergency shut off has been cleared. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at service@wti.com.
- **`noDialtoneSetTrap`** - Indicates that the No Dialtone Alarm has been triggered.
- **`noDialtoneClearTrap`** - Indicates that the No Dialtone Alarm has been cleared.
- **`wakeupOnFailureSetTrap`** - Indicates that the Wakeup On Failure Alarm has been triggered.
- **`wakeupOnFailureClearTrap`** - Indicates that the Wakeup On Failure Alarm has been cleared.

Trademark and Copyright Information

WTI and Western Telematic are trademarks of Western Telematic Inc.. All other product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

Information and descriptions contained herein are the property of Western Telematic Inc.. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Western Telematic Inc..

August 2021
Part Number: 14527, Revision: H

Trademarks and Copyrights Used in this Manual

All trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.