WTI Part No. 14527
Rev. C

WTI User's Guide

Software SetUp and Operation

Products Covered

- CPM Series - Console Server + Power Control Combos
- DSM Series - Console Servers
- NBB Series - Basic Switched PDUs - Vertical
- NPS Series - Basic Switched PDUs - Horizontal
- REM Series - Remote Edge Managers
- RPC Series - Remote DC Power Switches
- VMR Series - Outlet Metered Switched PDUs

Configuration and SetUp

Power & Console Solutions | 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

1. Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.
2. When installing 48 VDC rated equipment, it must be installed only per the following conditions:

   A. Connect the equipment to a 48 VDC supply source that is electrically isolated from the alternating current source. The 48 VDC source is to be connected to a 48 VDC SELV source.

   B. Input wiring to terminal block must be routed and secured in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.

   C. A readily accessible disconnect device, with a 3 mm minimum contact gap, shall be incorporated in the fixed 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.

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).

Up to Four Power Supply Cables

Note that some DSM series units feature two separate power inlets and a separate power supply cable for each power inlet.

In addition, some CPM-1600 series units feature four separate power inlets and a separate power supply cable for each power inlet. Make certain to disconnect all power supply cables from their power source before attempting to service or remove the unit.

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.

Restricted Access (CPM Series Only)

CPM Series units are intended for installation in Restricted Access Location.

Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT.

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

7. Configuration Options (*continued*)

Appendices:

1. Introduction

This User's Guide covers the following WTI product lines:

- DSM Series - Serial Console Servers
- CPM Series - Console Server + Power Control Combos
- VMR Series - Outlet Metered Switched PDUs
- NPS Series - Basic Horizontal Switched PDUs
- NBB Series - Basic Vertical Switched PDUs
- REM Series - Remote Edge Managers
- RPC Series - Remote DC Power Switches

All of these product lines are designed to simplify the process of remotely managing vital network elements located at distant network equipment sites and off-site facilities. WTI Console Server products provide remote access to console port command functions on faraway network elements. WTI Power Control Products provide ability to remotely control power switching and reboot functions at the remote network equipment site. WTI Combo Products provide both remote console access to console ports and remote control of power switching and reboot functions.

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.

WTI Devices provide 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 serial ports and/or plugs, 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. WTI Devices include 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:

WTI Devices can constantly monitor temperature levels, ping response and other factors. If the WTI Device 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 WTI Device 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 WTI Device can restore power to devices to return to normal operating conditions. WTI Devices also record temperature readings to a convenient log file.

In addition to the capabilities described above, some WTI Devices include current monitoring capabilities, allowing the unit to monitor and report current, power and voltage conditions at remote sites.

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 WTI Device, 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 WTI Device

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 WTI Device to an appropriate power source. Note that some WTI Devices feature two or more power inlets. When power is applied to the WTI Device, the ON LED on the instrument front panel should light, and the RDY LED should begin to flash within 90 seconds. This indicates that the unit is ready to receive commands.

2.2. Connect Your PC to the WTI Device

In the default state, communication with the WTI Device via Telnet, HTTP and HTTPS are disabled. Although communication via Telnet, HTTP and/or HTTPS can be enabled as described in this User's Guide, during this bench test procedure, the WTI Device will be controlled via the Command Line Interface (CLI) using a local PC, connected to either the Mini USB Port, Serial SetUp Port or Network Port:

- **Mini USB Port:** 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 WTI Device. 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 WTI Device 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 WTI Device, please refer to Hardware Guide.*

2.3. Communicating with the WTI Device

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 WTI Device 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 WTI Device from a node on the same subnet.*
- *When connecting only a single network cable to a WTI Device 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]**. 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 WTI Device will display either the Main Menu (Web Browser Interface) or the Port Status Screen (Text Interface.)

2.4. Connecting Ports and Switching Outlets

If you wish to verify that the WTI Device is operating properly before deploying the unit in a working network environment, proceed as follows to connect ports and switch outlets:

1. **Review the Help Menu:** At the Text Interface command prompt, type **/H** and press **[Enter]** to display the Help Menu.

2. **Creating Connections Between Ports:** (WTI Console Server products and WTI Console Server + Power Control Combo products only.) Commands issued at the SetUp port can be used to create a connection between two other ports.

   a) To connect Port 3 to Port 4, type **/C 3 4 [Enter]**.

   b) While Ports 3 and 4 are connected, your resident port will still recognize commands. Type **/S [Enter]** to display the Status Screen. The "STATUS" column should now list Ports 3 and 4 as connected and other ports as "Free".

   c) Issue a Disconnect command; type **/D 3 [Enter]**. The unit will display the, "Are you Sure (y/n)?" prompt. Type **y** and press **[Enter]** to disconnect.

   d) Type **/S [Enter]** to display the Status Screen. The "STATUS" column should now list Ports 3 and 4 as "Free".

3. **Controlling Outlets:** (WTI Power Control products and WTI Console Server + Power Control Combo products only.) You may wish to perform the following tests in order to make certain that the switched outlets are functioning properly.

   a) **Reboot Outlet:** At the command prompt, type **/BOOT 1** and press **[Enter]**. The status indicator for Plug 1 should go Off, pause for a moment and then go back On, indicating that the boot cycle has been successfully completed.

   b) **Switch Outlet Off:** At the command prompt, type **/OFF 1** and then press **[Enter]**. The status indicator for Plug 1 should go Off, indicating that the command has been successfully completed. Leave Plug 1 in the "Off" state, and then proceed to the next step.

   c) **Switch Outlet On:** At the command prompt, type **/ON 1** and press **[Enter]**. The status indicator for Plug 1 should then go back On, indicating that the command has been successfully completed.

4. **Exit from User Interface:** To exit the user interface, type **/X** and press **[Enter]**.

3. The User Interface

WTI Devices 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 WTI Devices automatically.

  Note: *WTI Devices 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 WTI Device

In the default state, communication with the WTI Device via Telnet, HTTP and HTTPS are disabled. When connecting your PC or Laptop to the WTI Device 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 WTI Device. 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 WTI Device 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 WTI Device, 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, disconnect serial ports and perform power switching and reboot operations.

Notes:

- *When communicating with the WTI Device 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 WTI Device 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 WTI Device 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 WTI Device'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 WTI Device 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 WTI Device will display the Status Screen.

3.3.1. Enabling Web Access and Telnet Access

Once you have accessed the WTI Device'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 WTI Device 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 WTI Device 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:** WTI Devices 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 WTI Device'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 WTI Device:**

   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 WTI Device 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 WTI Device'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 WTI Device's IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Dial-Up Modem:** If your WTI Device unit includes the optional external modem or if you have installed a modem at one of the WTI Device'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 WTI Device 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 WTI Device, including current alarm states, selected configuration parameters, port status, plug 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 12.4.1.*

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 WTI Device.

> **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 WTI Device'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 Port Status Screens (/SD)

The Port Status Screens are used to list conditions at the Serial Ports as well as the currently defined IP Alias for the Serial Ports.

Notes:

- *The Port Status Screens are only available on WTI Console Server products and WTI Console Server + Power Control Combo products.*
- *When Port Status Screens are viewed by an account with "Administrator" or "SuperUser" command access, all Serial Ports are listed.*
- *When Port Status Screens are viewed by an account with "User" or "ViewOnly" command access, then the screen will list only the Serial Ports that are allowed by that account.*
- *When WTI Console Server + Power Control Combo products are accessed via the Command Line Interface, the /S command can be used to display both the Port Status Screen and Plug Status Screen.*

4.3.1. Serial Port Status

The Serial Port Status screen shows the status of the Serial Ports, including the user-defined port name and port mode for each Serial Port, as well as the buffer count, connection status and the names of any users currently accessing these ports. In addition to listing conditions at the Serial Ports, the Serial Port Status Screen will also list the ambient rack temperature.

Note: *On some WTI Devices, the Serial Port Status Screen will also include a line that indicates whether or not power is connected to the available power inlets.*

4.3.2. Alias Status

The Alias Status Screen displays much of the same information provided by the Serial Port Status Screen, but also lists user-defined IP aliases for each serial port.

4.3.3. USB Console Port Status (/SDU)

If your WTI Device includes USB Console Port(s) the status from these ports can be displayed via the Port Status Screen in the Web Browser Interface, or by issuing the `/SDU` command via the Command Line Interface.

4.4. The Plug Status Screen (Circuit Status Screen) (/S)

The Plug Status Screen lists the On/Off status of each switched outlet or circuit, along with user-defined Plug Names, default On/Off settings, Boot Sequence Delay Periods and Plug Priority values. In addition, the Plug Status Screen also lists the current ambient rack temperature.

Notes:

- *The Plug Status Screen is not available on WTI Console Server products.*
- *On WTI Console Server + Power Control Combo products, the Serial Port Status Screen will also include a line that indicates whether or not power is connected to the available power inlets.*
- *On RPC Series DC Power Control units, the Plug Status Screen is referred to as the Circuit Status Screen.*
- *On WTI Devices that include current monitoring capabilities, the Plug Status Screen will also display the Amps consumed by each switched outlet.*
- *When WTI Console Server + Power Control Combo products are accessed via the Command Line Interface, the /S command can be used to display both the Port Status Screen and Plug Status Screen.*

4.5. The Plug Group Status Screen (Circuit Group Status Screen) (/SG)

On WTI Power Control products and WTI Console Server + Power Control Combo products, the Plug Group Status screen can be used to show configuration details and On/Off status for user-defined Plug Groups.

Notes:

- *In order to display the Plug Group Status screen, you must first define at least one Plug Group as described in Section 7.7.*
- *The Plug Group Status Screen is not available on WTI Console Server products.*
- *When the Plug Group Status Screen is viewed by an account with Administrator or SuperUser command access, all plugs and plug groups can be shown. When the Plug Status Screen is viewed by an account with User or ViewOnly command access, then the unit will only display the plugs and plug groups that are allowed by that account.*
- *On RPC Series DC Power Control units, the Plug Group Status Screen is referred to as the Circuit Group Status Screen and instead of displaying conditions of switched outlets groups, the Circuit Group Status Screen shows the status of each switched DC Power Circuit Group.*
- *On WTI Devices that include current monitoring capabilities, the Plug Group Status Screen will also display the Amps consumed by each switched outlet.*

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" for alarms that are active or "No" for alarms that are not active.

4.7. The Cell Modem Status Screen (/CELL)

The Cell Modem Status Screen displays information regarding the status and configuration of the optional internal Cellular Modem. In addition to showing the Cell Phone Number, Device ID, SIM Number, Software Revision, Network Carrier, Public IP Address and other device and configuration related information, the Cell Modem Status Screen also shows whether or not a PPP Session is currently established and ranks the Cell Signal Quality.

> **Note:** *The Cell Modem Status Screen is only present on WTI Devices that include the Cellular Modem option.*

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 WTI Device, including user account logins and logouts, port connection, outlet 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 WTI Device. 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 7.10.

5. Control Functions

This section describes the procedures for connecting and disconnecting Serial Ports and controlling power switching and reboot functions.

5.1. The Port Control Menu

In the Web Browser Interface, the Port Control Menu can be used to disconnect Serial Ports on WTI Console Server products and WTI Console Server + Power Control Combo products. Although the Web Browser Interface can be used to disconnect ports, port connections are created using the Command Line Interface (CLI.)

Notes:

- *Serial Port connection and disconnection features are only available on WTI Console Server products and WTI Console Server plus Power Control Combo products.*
- *The Serial Port Configuration Menus offer a wide variety of configuration parameters that can be used to adapt Serial Port behavior to fit your specific application. For more information, please refer to Section 7.2.*

5.1.1. Connecting and Disconnecting Serial Ports Using the CLI

Two different types of connections can be made between serial ports; Resident Connections and Third Party Connections WTI Console Server products and WTI Console Server + Power Control Combo products allow communication between devices without the requirement that both ports use the same communication parameters.

- **Resident Connections:** Your resident port issues a /C command to connect to a second port. For example, Port 4 issues the /C command to connect to Port 5.
- **Third Party Connections:** (Administrator and SuperUser Mode Accounts Only) Your resident port issues a /C command to create a connection between two other ports. For example, Port 1 is your resident port, and Port 1 issues a command to connect Port 2 to Port 3.

Notes:

- *Third Party Connections can only be initiated by accounts and ports that permit Administrator or SuperUser level commands.*
- *The serial ports cannot employ the /C command to initiate a connection to the Network Port.*
- *User level accounts are only allowed to connect to ports that are specifically allowed by the account. Administrator and SuperUser level are allowed to connect to all serial ports.*

To connect ports using the CLI, proceed as follows:

1. Access the CLI (for instructions, see Section 3.3.)

2. Invoke the /C command to connect the desired ports.

   a) **Resident Connect:** To connect your resident port to another port, type **`/C xx`** **[Enter]**. Where xx is the number or name of the port you want to connect.

      Example: To connect your resident port to Port 8, type **`/C 8`** **[Enter]**.

   b) **Third Party Connect:** (Administrator and SuperUser Mode Only) To connect any two ports (other than your resident port), type **`/C xx XX`** **[Enter]**. Where **`xx`** and **`XX`** are two port names or numbers.

      Example: To connect Port 5 to Port 6, access the CLI at a third port that permits Administrator level commands (using an account that also permits Administrator or SuperUser level commands), and invoke the following command: **`/C 5 6`** **[Enter]**.

   c) **Connecting to a USB Console Port:** If your WTI Device includes USB Console ports, issue the /C command as follows to connect to USB format console ports.

      i. To connect your resident port to USB port 1, type **`/C U1`** **[Enter]**.

      ii. To connect your resident port to USB port 2, type **`/C U2`** **[Enter]**.

   Note: *While you're connected to USB port 1, the REM will not recognize commands issued at your resident port, with the exception of the Resident Disconnect Sequence.*

      iii. If you've connected a 4-Port USB Hub to the USB Console Port(s) on your WTI Device, type **`/C ux.y`** and press **[Enter]**. Where **`x`** is the USB Port number, and **`y`** is the number of desired USB port on the Hub. For example, to connect to the first port on a USB Hub installed at USB Port U2, type **`/C U2.1`** **[Enter]**.

      iv. To disconnect, issue the Resident Disconnect Sequence (Logoff Sequence); type ^X (press [Ctrl] and [X] at the same time).

3. To disconnect ports via the CLI, invoke the /D command from either the Network Port, Modem Port or any free Serial Port: type **`/D xx`** **[Enter]**. Where **`xx`** is the name or number of one of the two connected ports.

Notes:

- *When the /C or /D commands are invoked, the WTI Device will display a confirmation prompt before implementing the command. If needed, the confirmation prompt can be disabled as described in Section 7.1.5.*
- *When the /C command or /D command specifies the port name, it is only necessary to enter enough letters to differentiate the desired port from other ports. Type an asterisk (*) to represent the remaining characters in the port name. For example, to connect your resident port to a port named "SALES", the connect command can be invoked as /C S*, providing no other port names begin with the letter "S".*

5.1.2. Disconnecting Ports Using the Web Browser Interface

To disconnect ports using the Port Control Menu, proceed as follows:

1. Access the Web Browser Interface as described in Section 3.2.
2. Click on the Control link on the left hand side of the screen to display the Control Submenu, then Click on Port Control to display the Port Control Menu.
3. When the Port Control Menu appears, click the down arrow in the Action column for the desired serial port(s), select the Disconnect option from the dropdown menu and then click on the Confirm Port Actions button.
4. When the Confirm Port Actions button is pressed, the WTI Device will display a screen which lists the selected action(s) and asks for confirmation before proceeding. To implement the selected port action(s), click on Execute Port Actions.

   Notes: *If needed, the command confirmation prompt can be disabled, as described in Section 7.1.5.*
5. After a brief pause, the WTI Device will display the Port Status Screen, confirming that the selected ports have been disconnected.

Notes:

- *Port connections cannot be created via the Web Browser Interface. To connect ports, please refer to Section 5.1.1.*
- *When the Port Control Screen is displayed by an account that permits Administrator or SuperUser command access, all Serial Ports will be displayed.*
- *When the Port Control Screen is displayed by an account that permits User or ViewOnly level commands, the screen will only include the Serial Ports that are allowed by the account.*

5.2. The Plug Control Menu (Circuit Control)

The Plug Control Screen lists the On/Off status of the Switched Outlets or Circuits and is used to control switching and rebooting. To invoke power switching commands, proceed as follows:

Notes:

- *On RPC Series DC Power Control units, the Plug Control menu is referred to as the Circuit Control menu.*
- *Power switching and reboot functions are not available on WTI Console Server products.*
- *WTI Power Control products and WTI Console Server + Power Control Combo products offer a wide variety of configuration parameters that can be used to adapt outlet switching behavior to better fit your specific application. For more information, please refer to Section 7.8.*

1. Access the Web Browser Interface as described in Section 3.2.
2. Click on the Control link on the left hand side of the screen. When the menu expands, click on Plug Control. The Plug Control Menu will be displayed.
3. From the Plug Control Menu, click on the down arrow in the Action column for the row for the desired plug(s). When the flyout menu appears, select the desired action (On, Off, Boot or Default) and then click on the Confirm Actions button.
4. The WTI Device will display a menu that allows you to confirm that the selected action(s) should be executed. Click on the Execute Actions button to proceed.

   Note: *If needed, the command confirmation prompt can be disabled, as described in Section 7.1.5.*

5. The WTI Device will execute the selected power switching/reboot actions, and then display the Plug Status screen to show the updated plug status.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 7.8.*
- *If a switching or reboot command is directed to a plug that is already in the process of being switched or rebooted, then the new command will be placed in a queue until the plug is ready to receive additional commands.*
- *If the Status column in the Plug Control Menu includes an asterisk, this means that the outlet is busy completing a previously invoked command.*
- *When the Plug Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched outlets will be shown.*
- *When the Plug Control Screen is displayed by an account that permits User or ViewOnly command access, the screen will only include the switched outlets that are specifically allowed by the account.*
- *On RPC DC Power Control products, the Plug Control Menu will also list the status of the RPC's four Alarm Inputs.*

5.3. The Plug Group Control Menu (Circuit Group Control)

The Plug Group Control Screen is used to send switching and reboot commands to the user-defined Plug Groups. As described in Section 7.7, Plug Groups allow you to specify a group of outlets that are dedicated to a similar purpose or client, and then direct switching commands to the group, rather than switching one plug at a time.

Notes:

- *On RPC Series DC Power Control units, the Plug Group Control menu is referred to as the Circuit Group Control menu.*
- *Power switching and reboot functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products. WTI Console Servers products do not support power control functions.*

To apply power switching commands to Plug Groups, first access the Web Browser Interface, proceed as follows:

1. Access the Web Browser Interface.
2. Click on the Control link on the left hand side of the screen. When the menu expands, click on Plug Group Control. The Plug Group Control Menu will be displayed.

   Note: *In order to use the Plug Group Control Menu, you must first define at least one Plug Group, as described in Section 7.7.1.*
3. From the Plug Group Control Menu, click on the down arrow in the Action column for the row for the desired Plug Group(s). When the flyout menu appears, select the desired action (On, Off, Boot or Default) and then click on the Confirm Actions button.
4. The WTI Device will display a menu that allows you to confirm that the selected action(s) should be executed. Click on the Execute Actions button to proceed.

   Note: *If needed, the command confirmation prompt can be disabled, as described in Section 7.1.5.*
5. The WTI Device will execute the selected power switching/reboot actions, and then display the Plug Status screen to show the updated plug status.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times and user-defined Plug Priority values will be applied as described in Section 7.8.*
- *If a switching or reboot command is directed to a plug that is already in the process of being switched or rebooted by a previous command, then the new command will be placed in queue until the plug is ready to receive additional commands.*
- *When the Plug Group Control Screen is displayed by an account that permits Administrator or SuperUser command access, all user-defined Plug Groups will be displayed.*
- *When the Plug Control Screen is displayed by an account that permits User or ViewOnly level commands, the screen will only include the Plug Groups that are allowed by the account.*

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 WTI Device.

5.5. Logging Out of the User Interface

When you have finished communicating with the WTI Device 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 WTI Device has completely exited from the user interface, and is not waiting for the inactivity timeout period to elapse before allowing additional connections.

5.6. Emergency Shut Off Function

WTI Power Control products and WTI Console Server + Power Control Combo products also include an Emergency Shut Off function, that can be used to immediately shut off all power outlets in the event of an emergency. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at **service@wti.com**.

6. The Metering Menus

The Metering Menus can be used to display live readings of current and power consumption and ambient rack temperature. In addition, the Metering Menus can also provide a means to review current, power and temperature history over a user-selected period of time in graph format. Current, Power and Temperature data can either be viewed live or downloaded.

The Metering link on the left hand side of the Web Browser Interface provides access to the Current Metering Menu, Power Metering Menu and Temperature Metering menu.

6.1. Current Metering

The Current Metering link provides access to the Current Metering Status menu, Current Range menu and Current History menu:

Note: *Current Metering functions are only available on WTI Devices that include the Current Metering Option.*

- **Current Metering Status:** Displays Current, Voltage and Power consumption data for all available line inputs, plus Current and Temperature Alarm settings and other data.
- **Current Range:** Displays Current Range data for user specified plugs, plug groups and/or input lines in graph format.
- **Current History:** Displays current usage history for user specified plugs, plug groups and/or input lines in graph format, and allows current history data to be downloaded in ASCII, CSV or XML format.

6.2. Power Metering

The Power Metering link provides access to the Power Range menu and Power History menu:

Note: *Power Metering functions are only available on WTI Devices that include the Current Metering Option.*

- **Power Range:** Displays power consumption data for user specified plugs, plug groups and/or input lines in graph format.
- **Power History:** Displays power usage history for user specified plugs, plug groups and/or input lines in graph format, and allows power history data to be downloaded in ASCII, CSV or XML format.

6.3. Temperature

The Temperature Metering link provides access to the Temperature Range Menu and the Temperature History Menu:

- **Temperature Range:** Displays ambient Temperature data for a user specified time range in graph format.
- **Temperature History:** Displays temperature history in graph format, and allows temperature history data to be downloaded in ASCII, CSV or XML format.

7. Configuration Options

This section describes the basic configuration procedure for all WTI Console Server products, WTI Power Control Products and WTI Console Server + Power Control Combo products. 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 12.

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 3.1.*
- *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.*

7.1. 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.

7.1.1. System Parameters

The System Parameters Menu is used to define the Site ID tag for the WTI Device, 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 WTI Device. **Note:** *The Site I.D. will be cleared if the WTI Device 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 reboot activity at the WTI Device, including reboots and switching caused by Load Shedding, Load Shedding Recovery, Ping No Answer Reboots and Scheduled Reboots.
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
Syslog Server Format (Default = Standard)	The format used in Syslog Server Log.
Current Metering Log (Default = On)	(WTI Devices with Current Metering Option Only) Enables/disables the Current Metering Log.
Front Panel Buttons (Default = On)	Enables/disables control functions for the front panel buttons

Parameter (Default)	Description
Analog Modem Phone No. (Default = Undefined)	If the WTI Device includes the optional internal dial-up modem, this parameter can be used to record the phone number. When the WTI Device 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.
Voltage Calibration (Default = Undefined)	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Calibrates the voltage readout. To calibrate the voltage, first determine the approximate voltage and then select the Voltage Calibration option and key in the correct voltage.
Power Configuration (Default = Undefined)	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Used to define the Power Factor parameter and Power Efficiency parameter. For more information, please refer to Section 7.1.1.1.
Asset Tag (Default = Undefined)	Allows a descriptive tag or tracking number to be assigned to the WTI Device. Once defined, the Asset Tag can be displayed via the Product Status Screen

7.1.1.1. Power Configuration

Note: *Current and Power Metering functions are only available on WTI Devices that include the Current Metering option.*

The Power Configuration menu allows you to adjust power measurements in order to obtain a more accurate determination of how much “real power” is being used by devices connected to the -C Series unit. Real Power is determined by the following equation:

$$\text{Real Power} = \frac{(\text{Voltage} * \text{Amps}) * \text{Power Factor}}{\text{Power Efficiency}}$$

To define Power Configuration parameters, access the user interface using an account that permits access to Administrator level commands and then open the System Parameters menu and define the following parameters:

- **Voltage Calibration:** This option is used to calibrate the voltage readout. To calibrate the voltage, first determine the approximate voltage and then select the Voltage Calibration option and key in the correct voltage. (Default = undefined)
- **Power Factor:** Can be any value from 0.1 to 1.00. (Default = 1.00)
- **Power Efficiency:** Can be any whole number from 1% to 100%. (Default = 100%)

7.1.2. Real Time Clock

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

Notes:

- *The WTI Device will contact the NTP server and update the time whenever you change NTP parameters.*
- *To cause the WTI Device 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 WTI Device 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 WTI Device'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 WTI Device 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 WTI Device 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 7.3.1.6.1.*

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 7.3.1.6.1.*
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 7.3.1.6.1.*
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 WTI Device will retry the connection four times. If neither the primary nor secondary NTP server responds, the WTI Device 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.*

7.1.3. 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 7.10.6, the WTI Device 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 WTI Device 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 WTI Device 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 WTI Device 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 WTI Device 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 WTI Device 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 WTI Device for the defined Web Duration period.

7.1.4. 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 WTI Device 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 7.5) 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 WTI Device will attempt to contact the Callback number.
Callback Delay (Default = 30 Seconds)	The amount of time that the WTI Device will wait between Callback attempts.

7.1.5. Scripting Options

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

Notes:

- *The functions provided by the Scripting Options menu are intended for use in applications where scripts are employed to control the WTI Device. Improper use of Scripting Options menu functions can cause the WTI Device to become unresponsive. Prior to attempting to use the functions provided by the Scripting Options menu, it is recommended to contact WTI Technical Support.*
- *On RPC DC Power Control Products, prompts and parameters that refer to "plugs" or "outlets" are renamed to refer to "circuits."*

Parameter (Default)	Description
Command Confirmation (Default = On)	(Not Present on WTI Console Server Products) When enabled, a "Sure" prompt will be displayed before power switching and reboot commands are executed. When disabled, commands are executed without further prompting.
Automated Mode (Default = Off)	(Not Present on WTI Console Server Products) When enabled, the unit will execute switching and reboot commands without displaying a confirmation prompt, status screen or confirmation messages. For more information on Automated Mode, please refer to Section 7.1.5.3.
Command Prompt (Default = Model Series)	Allows the CLI command prompt to be set to either match other WTI product command prompts or the currently defined Site I.D. Message. This provides compatibility with scripts, written for other WTI products.
IPS Mode (Default = Off)	(Not Present on WTI Console Server Products) This parameter can be used to set up WTI Switched PDU products for use with command scripts that were written for WTI's legacy IPS Series Remote Reboot Switches . When enabled, the "IPS" command prompt will be displayed in the Text Mode, User Accounts will not allow definition of a Username, and only the password prompt will be displayed when logging into the unit (IPS Mode units will not display a "username" prompt.) • Providing that no Administrator level user accounts are defined, the unit will not display the username or password prompts upon login to the user interface. • If one or more Administrator level user accounts have been defined, then the WTI Switched PDU will only display the password prompt upon login to the user interface. If all Administrator level user accounts (aside from the default "super" account) are deleted, then the WTI Switched PDU will return to the status where no username or password prompts are displayed upon login to the user interface.

Parameter (Default)	Description
Emergency Shutoff (Default = Off)	(Not Present on WTI Console Server Products) Enables/disables the Emergency Shutoff Feature. The Emergency Shutoff function can be used to immediately shut off all specified power outlets on the unit in case of emergency. For more information, please contact WTI Customer Service.
Emergency Shutoff Auto Recovery (Default = Off)	(Not Present on WTI Console Server Products) Enables/Disables the Emergency Shutoff Auto Recovery feature. When enabled, following an Emergency Shutoff, all plugs will return to the On/Off status that was selected prior to the Emergency Shutoff.
Single Plug Boot Delay Enable (Default = Off)	(Not Present on WTI Console Server Products) When enabled, the Boot/Sequence Delay value will be applied when a single plug is rebooted, and to the final plug in a Plug Group when an entire Plug Group is rebooted. This allows you to specify the "Off Time" that will be used when a single plug or the last plug in a Plug Group is rebooted. For more information, please refer to Section 7.8.
U-Boot Plugs Enable (Default = Off)	(Not Present on WTI Console Server Products) When enabled, after a power interruption, the WTI Device will switch on all power outlets before the operating system has finished loading. This allows power to be reapplied to connected devices such as servers and routers as quickly as possible after a power interruption.
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.*
USB Client State (Default = On)	(CPM and DSM Series Products Only) Enables/Disables the USB Mini format SetUp Port. **Note:** *For information regarding serial drivers for the USB port, please refer to the WTI.com Knowledge Base.*
Modem Hunt Telnet (Default = Off)	(Console Products Only) Enables the WTI Device to support modem pooling in conjunction with third party Serial Port Redirector software as described in Section 7.1.5.4. **Note:** *The "Modem Hunt Telnet" option is recommended for transmitting ASCII data and the "Modem Hunt Raw" option is recommended for transmitting binary data*.

Parameter (Default)	Description
Modem Hunt Raw (Default = Off)	(Console Products Only) Same as Modem Hunt Telnet, except this function uses a raw socket connection. For more information, please refer to Section 7.1.5.4. **Note:** *The "Modem Hunt Telnet" option is recommended for transmitting ASCII data and the "Modem Hunt Raw" option is recommended for transmitting binary data.*
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.*
Reset Unit	Restarts the WTI Device's operating system. **Note:** *The Reset function does not switch off power to the WTI Device. The reboot function only restarts the WTI Device's operating system.*
TCP Hold Write Options	(Console Products Only) Provides access to the TCP Hold Write Options Menu. For more information, please refer to Section 7.1.5.1.
Voltage Loss Delay Options	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Provides access to the Voltage Loss Delay Options Menu. For more information, please refer to Section 7.1.5.2.

7.1.5.1. TCP Hold Write Options

The TCP Hold Write Options can be used to minimize the number of data packets that are sent from WTI Console Server products and WTI Console Server + Power Control Combo products. In cases where a WTI Device is receiving a slow flow of data from an attached device, the TCP Hold Write Options can be configured to set the size of each packet and define a maximum "hold" time in order to determine how long data is allowed to accumulate in the buffer before being sent.

Note: *The TCP Hold Write Options Menu is only available on WTI Console Server Products and WTI Console Server + Power Control Combo Products.*

Parameter (Default)	Description
TCP Hold Write Enable (Default = Off)	Enables/disables TCP Hold Write.
TCP Hold Write Duration (Default = 2)	The maximum amount of time (in 40 msec intervals) that data will be allowed to accumulate before transmission.
TCP Hold Write Buffer Size (Default = 512 Characters)	Determines the size of the TCP Hold Write Buffer. When the amount of accumulated data reaches the currently defined Hold Write Buffer Size, buffered data will be sent.

7.1.5.2. Voltage Loss Delay Options

Determines how WTI Power Control Products and WTI Console Server + Power Control Combo products with Dual Power Inlets will react when power to one inlet is lost. The Voltage Loss Delay Options allow the unit to automatically turn off outlets and delay the Lost Voltage Alarm when power to one inlet is lost. The Voltage Loss Delay Options menu allows the following parameters to be defined:

Note: *The Voltage Loss Delay Options are not available on WTI Console Server Products, or other WTI Products that include dual power inlets.*

Parameter (Default)	Description
Turn Plugs Off Enable (Default = On)	(Not Present on WTI Console Server Products) When enabled, after power to one inlet is lost, the unit will wait for the defined Voltage Loss Delay period and then switch Off all outlets on the branch that was supported by the inlet that has lost power.
Voltage Loss Delay (Default = 12 Seconds)	(Not Present on WTI Console Server Products) Determines how long the unit will pause before generating a Lost Voltage Alarm and switching off the outlets after power to one of the inlets is lost.

7.1.5.3. Automated Mode

The Automated Mode allows WTI Power Control products and WTI Console Server + Power Control Combo products to execute switching and reboot commands without displaying menus or generating response messages. Automated Mode is designed to allow the WTI Device 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 WTI Device 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 reboot 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 plugs 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 7.3.1.4.*
- *The Automated Mode is not available on DSM Series Console Servers.*

When enabled, WTI Device 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 Plug Status Screen will not be automatically displayed after commands are successfully executed. Note however, that the Plug 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.

7.1.5.4. Modem Pooling

The “Modem Hunt Telnet” and “Modem Hunt Raw” parameters allow WTI Console Server products and WTI Console Server + Power Control Combo products to support modem pooling in conjunction with third party Serial Port Redirector software. This allows you to connect external modems to several serial ports, and then use the WTI Device to automatically find a free modem when you need to create an outbound connection.

The Modem Hunt Telnet and Modem Hunt Raw options function as follows:

> **Note:** *Modem Pooling features are only present on WTI Devices that include serial console ports.*

Modem Hunt Telnet: Offers three different configuration options: “Off” (Disabled), “On - No Password” and “On - Password.” Each of the “On” options selects a default port number for modem pooling:

- On - No Password: Uses port number 2300.
- On - Password: Uses port number 2100. Note that when the password is enabled, you will be prompted to enter a valid username and password.

Modem Hunt Raw: Offers three different configuration options: “Off” (Disabled), “On - No Password” and “On - Password.” Each of the “On” options selects a default port number for modem pooling:

- On - No Password: Uses port number 3300.
- On - Password: Uses port number 3100. Note that when the password is enabled, you will be prompted to enter a valid username and password.

In order to use Modem Pooling functions, the WTI Device must be configured as follows:

- Telnet Access and/or Raw Socket Access must be enabled (Network Configuration Menu.)
- Modem Hunt Telnet and/or Modem Hunt Raw must be enabled (Network Parameters Menu.)
- The Port Mode (Serial Port Configuration Menu) for each serial port attached to an external modem must be set to “Modem Mode.”
- Direct Connect must be enabled (Serial Port Configuration Menu) for each serial port attached to an external modem.

In addition, you must also know the following information regarding the WTI Device and enter it into your Serial Port Redirector software:

- The Port Number (shown above) for the desired Modem Hunt Telnet or Modem Hunt Raw option.
- The IPv4 or IPv6 format IP address for the WTI Device.

To create an outbound modem connection, start your communications program (e.g., PuTTy, TeraTerm, etc.), select the virtual COM port that was defined via your Serial Port Redirector software and then place a call as you normally would.

7.2. Port Configuration (RJ45 and USB Ports)

The Port Configuration menus allow you to select parameters for the WTI Device's Serial RJ45 Ports, USB Ports (if present) and Internal Modem Port (cellular or dial-up.) In addition to setting port modes and communication parameters, the Port Configuration menus can also be used to select a number of other port parameters described in the table below.

To display the Port Configuration menus, first click on the Serial Port Configuration button on the left hand side of the screen. When the Port Configuration top menu appears, click on the down arrow to indicate the desired port and then click "Select Port."

Notes:

- *If the WTI Device includes USB Console ports, in the Port Configuration menu, these ports are described as U1 and U2. USB Port configuration menus are only available on WTI Devices that include USB Console Ports.*
- *When the WTI Device includes USB Console Ports, if required, a 4-Port USB Hub can be connected to the WTI Device's USB ports to provide extra ports for console access. In this case, ports on the USB Hub are addressed as U1.1, U1.2, and etc.*
- *Some parameters listed below are not available on WTI Power Control Products.*
- *To Determine the Serial Port Number for the internal dial-up modem option (if present,) please refer to the Serial Port Status Screen.*
- *When configuring the WTI Device via modem, modem parameters will not be changed until after you exit the user interface and disconnect from the unit.*

The Serial Port Configuration menu offers the following parameters:

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.

Parameter (Default)	Description
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.
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.

Parameter (Default)	Description
Port Mode Parameters	
Port Name (Defaults; RJ45 Serial Ports and USB Console Ports = Undefined; Internal Modem Port = MODEM)	This parameter is used to assign a descriptive name to the Serial Port.
Port Mode (Defaults; Serial Port 1 = Any-to-Any Mode; Serial Ports 2 and above = Passive, Internal Modem Port = Modem Mode)	The operation mode for this port; Any-to-Any Mode, Passive Mode, Buffer Mode, Modem Mode or Modem PPP Mode. For more information, please refer to Section 7.2.1. **Notes:** • *Passive Mode and Buffer Mode are not available at Serial Port 1 (the Setup Port.)* • *The Port Mode for the Internal Modem Port (if present) can only be set to Modem Mode.* • *On units that include the Cellular Modem Option, the Port Mode for the Cellular Modem Port will always be Modem PPP. In this case, Modem PPP parameters are not defined by the user and are instead determined when a connection to the network is established.* • *Only one Port on the WTI Device may be configured for Modem PPP Mode at a given time.*
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 WTI Device 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 7.10.13.
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.

Parameter (Default)	Description
Port Mode Parameters (Continued)	
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 WTI Device 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.
Buffer Date/Time (Default = On)	(Buffer Mode Ports Only) Enables/disables the Time/Date stamp for buffered data at this port. When enabled, the WTI Device will add a time/date stamp whenever five seconds elapse between data items received.
Buffer Connect (Default = Off)	(Buffer Mode Ports Only) When enabled, the WTI Device will continue to Buffer captured data while you are connected to this Buffer Mode port.
Buffer Data to Syslog (Default = Off)	(Buffer Mode Ports Only) The Syslog feature is used to create records of each buffer event. As event records are created, they are sent to a Syslog Daemon, at an IP address defined via the Network Parameters menu. For more information, please refer to Appendix E. The Syslog feature offers three possible settings: • **Off:** Syslog disabled. • **On - Not Connected:** Messages will only be generated when a user is not connected to a buffer port. This prevents information captured from the attached device from being put into Syslog messages while a user is connected to a buffer port. • **On - Always:** All captured information will be sent out via Syslog message; whether a user is connected or not.
Facility (Default = Local_0)	(DSM, CPM and REM Series Products Only) The facility under which this port will log messages when Syslog is enabled.
Level (Default = Emergency)	(DSM, CPM and REM Series Products Only) The severity (or priority) of messages generated by this port when Syslog is enabled.
Buffer Threshold (Default = Off/0)	(DSM, CPM and REM Series Products Only) When the Port Mode is set to Buffer, this parameter enables/disables the Buffer Threshold function and sets the level that will generate traps and/or Buffer Threshold Alarms at this port. If set to "0" (zero), then SNMP Traps are disabled at this port. When a Buffer Threshold value is defined, this also allows the Buffer Threshold Alarm to be employed. **Note:** *This option is not available to Serial Port 1. This is because Port 1 is reserved as a SetUp Port, and cannot be configured as a Buffer Mode Port.*

Parameter (Default)	Description
Port Mode Parameters (Continued)	
Buffer Filtering String 1 (Default = Undefined)	(Buffer Mode Ports Only) This parameter is used to define one of two available text filters that can be used in conjunction with the Buffer Filtering Alarm to provide notification when user specified text strings are found in data that is received at a Buffer Mode port. These parameters are typically used to detect error messages and alerts in data received from attached devices.
Buffer Filtering String 2 (Default = Undefined)	(Buffer Mode Ports Only) This parameter is used to define one of two available text filters that can be used in conjunction with the Buffer Filtering Alarm to provide notification when user specified text strings are found in data that is received at a Buffer Mode port. These parameters are typically used to detect error messages and alerts in data received from attached devices.
Heartbeat (Default = Off)	(DSM, CPM and REM Series Products Only) The Heartbeat parameter can be used in conjunction with the Lost Communication alarm to provide notification when a WTI device that has been attached to one of the serial ports ceases to function. Normally, the WTI Device will send the Heartbeat message to an attached WTI device at regular intervals; if the attached device fails to respond to the Heartbeat message, the WTI Device can then notify you via email, Syslog Message or SNMP Trap as described in Appendix E and Appendix F. **Notes:** • *The Heartbeat function will only work if the port is configured for Any-to-Any mode. In order to employ the Lost Communication Alarm, all target ports must be configured for Any-to-Any mode.* • *The Heartbeat feature is only available when the serial port has been configured for "Any-to-Any" mode.*

Parameter (Default)	Description
Network Services Parameters	
Direct Connect (Default = Off)	(DSM, CPM and REM Series Products Only) Allows users to access the WTI Device and automatically create a connection between the Network Port and a specific serial port by including the appropriate port number in the connect command. For more information, please refer to Appendix D.3. • **Off:** The Direct Connect feature will be disabled at this port. • **On - No Password:** Users will be able to employ the Direct Connect feature to connect to this port without entering a password. • **On - Password:** Users will be able to employ Direct Connect to connect to this port, but will be required to enter a password before the connection is established. **Notes:** • *If "On - Password" is selected, and Administrator level commands are disabled at the Network Port, then only accounts that do not permit Administrator level commands will be allowed to establish a direct connection via the Network Port. If Administrator level commands are disabled at a given port, then that port will not allow access by accounts that permit Administrator level commands.* • *When Direct Connect is enabled, the Serial Port Configuration Menu will also list the port numbers for Telnet, SSH and Raw connections.* • **Telnet Port:** The Telnet port number employed to create a Direct Connection to this port via standard Telnet protocol. • **SSH Port:** When Direct Connect is set to "On - Password", this line will display the port number used to create a Direct Connection to this port via SSH protocol. • **Raw Port:** The port number used to create a Direct Connection to this port via Raw Socket protocol.
IP Alias Ethernet Port (Default = Undefined)	(Not Present on WTI Devices that include only one Ethernet Port) Allows you to define an IP Alias Address for eth0 or eth1.
IP Alias Address (Default = Undefined)	(DSM, CPM and REM Series Products Only) Assigns an IP address of your choice to the serial port. When an IP address is assigned to the serial port, this essentially allows users to create a direct connection to the serial port without first entering a password. **Notes:** • *The IP Alias feature is only available when the Direct Connect feature is set to "On - Password" or "On - No Password."* • *To display the IP Alias status via the Web Browser Interface, use the Alias Status Screen as described in Section 4.3.2.*

Parameter (Default)	Description
Network Services Parameters (Continued)	
Break on Raw Disconnect (Default = Off)	(DSM, CPM and REM Series Products Only) When enabled, the port will send a break character when a Raw Socket connection with the port is terminated. Note that this feature will work with both the "No Password" and "Password" options. In the default state this feature is disabled; no break character is sent when a Raw Socket connection is terminated. **Note:** *If "On - Password" is selected, and Administrator level commands are disabled at the Network Port, then only accounts that do not permit Administrator level commands will be allowed to establish a direct connection via the Network Port. If Administrator level commands are disabled at a given port, then that port will not allow access by accounts that permit Administrator level commands.*
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 WTI Device 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 7.3.1.6.1.* • *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.*
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.

7.2.1. Serial Port Modes

The WTI Device offers five different serial port operation modes:

- **Any-to-Any Mode:** Allows communication between connected ports and permits access to the user interface. Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer or Modem Mode Ports using the /C command in the CLI. The Any-to-Any Mode is available to all ports (except the Internal Modem Port) and is the default Port Mode for Port 1. For more information, please refer to Section 7.2.1.1.
- **Passive Mode:** Allows communication between connected ports, but does not allow access to the user interface. Passive Mode Ports can be connected by accessing the user interface from a free Any-to-Any or Modem Mode port and invoking the /C command in the CLI. Passive Mode is not available at Port 1, the Network Port or the Internal Modem Port, and is the default mode at Ports 2 and above. For more information, please refer to Section 7.2.1.2.
- **Buffer Mode:** Allows storage of data received from connected devices. Collected data can be retrieved by accessing the user interface from a free Any-to-Any or Modem Mode Port, and issuing the Read Buffer (/R) Command in the CLI. Furthermore, Buffer Mode ports can also be configured to support the Syslog and SNMP Trap features, discussed in Appendix E and Appendix F. The Buffer Mode is not available at Port 1, the Network Port or the Internal Modem Port. For more information, please refer to Section 7.2.1.3.
- **Modem Mode:** Allows communication between connected ports, permits access to the user interface and simplifies connection to an external modem. Modem Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem Mode also allows definition of a Hang-Up String, Reset String, and Initialization String and other modem-related parameters. The Modem Mode is not available at the Network Port and is the default mode for the Internal Modem Port (if present.) For more information, please refer to Section 7.2.1.4.
- **Modem PPP Mode:** Allows data normally sent via Ethernet to be sent via phone line. Modem PPP Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem PPP Mode also allows definition of a Hang-Up String, Reset String, Initialization String, IP Address and other communication-related parameters. The Modem PPP Mode is not available at the Network Port. When the Cellular Modem Option is present, the Cellular Modem Port will always be set for Modem PPP Mode. For more information, please refer to Section 7.2.1.5.

7.2.1.1. Any-to-Any Mode

Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer, or Modem Mode ports by accessing the CLI and issuing the /C Command. All ports can be configured for Any-to-Any Mode, and it is also the default mode for Port 1.

7.2.1.2. Passive Mode

Passive Mode Ports function the same as Any-to-Any Mode Ports, but do not allow access to the user interface. A Passive Mode Port can be connected to other serial ports, but cannot access the user interface, and therefore cannot be used to define parameters, display status, or invoke commands to connect ports or control power switching. The Passive Mode is the default at Serial Ports 2 and above.

Passive Mode Ports can be connected by accessing the CLI from a free Any-to-Any or Modem Mode Port, and invoking the Connect Command. Passive Mode ports will not buffer data, except during baud rate conversion.

Note: *In order to ensure Administrator level access to important command functions, the Passive Mode is not available at Port 1 (the SetUp Port) or the Network Port.*

7.2.1.3. Buffer Mode

The Buffer Mode allows collection of data from various devices without the requirement that all devices use the same communication parameters. In addition, Buffer Mode ports can also be configured to support the SYSLOG, SNMP Trap and Buffer Threshold Alarm functions.

Notes:

- *Buffer Mode Ports cannot provide access to the user interface.*
- *Buffer Mode is not available to Port 1 (the SetUp Port) or the Network Port.*

To check port buffers for stored data, access the CLI, using an account that permits Administrator, SuperUser or User level commands, and type /S [Enter] to display the Port Status Screen. The “Buffer Count” column in the Port Status Screen indicates how much data is currently being stored for each port.

To retrieve data from buffer memory, go to a free Any-to-Any or Modem Mode Port, then issue the /R command using the following format: /R xx [Enter]. Where xx is the number of the port buffer to be read.

Notes:

- *The /R command is not available to ViewOnly level accounts.*
- *Buffered data can only be retrieved via the CLI. This function is not available in the Web Browser Interface.*
- *In order to read data from a given port, your account must allow access to that port.*
- *When the /R command is invoked, the counter for the SNMP Trap function will also be reset.*

If the buffer contains data, the WTI Device will display a prompt that offers the following options:

- **Display One Screen:** To send data one screen at a time, press **[Enter]**. Each time **[Enter]** is pressed, the next screen is sent.
- **Display All Data:** To send all data currently stored in the buffer, type `1` and press **[Enter]**.
- **Erase Data on Screen:** To erase the data currently displayed on-screen, type `2` and press **[Enter]**.
- **Erase all Data:** To erase all data currently stored in the buffer, type `3` and press **[Enter]**.
- **Exit:** To exit from Read Buffer mode, press **[Esc]**.

Note: *Only one user can read from a port buffer at a time. If a second user attempts to read from a port that is already being read, an error message will be sent.*

To clear data from any port buffer (with or without reading it first), access the CLI, using an account and port that permit Administrator, SuperUser or User level commands, then issue the /E (Erase Buffer) command using the following format:

`/E xx` [Enter]

Where **`xx`** is the number or name of the port buffer to be cleared.

Notes:

- *The /E command cannot erase data from a port buffer that is currently being read by another port.*
- *The /E command is not available to ViewOnly level accounts.*
- *Buffered data can only be erased via the CLI. The Web Browser Interface does not offer the option to erase buffered data.*

7.2.1.3.1. Port Buffers

The Status Screen lists the amount of Buffer Memory currently used by each port. The WTI Device uses buffer memory in two different ways, depending on the user-selected port mode.

- **Any-to-Any, Passive, and Modem Mode Ports:** When two ports are communicating at dissimilar baud rates, the buffer memory prevents data overflow at the slower port.
- **Buffer Mode Ports:** Stores data received from connected devices. The user issues a Read Buffer command (/R) from an Any-to-Any or Modem Mode port to retrieve data.

If the Status Screen indicates an accumulation of data, the /E (Erase Buffer) command can be invoked to clear the buffer.

Note: *When a Buffer Mode port is reconfigured as an Any-to-Any, Passive, or Modem Mode port, any data stored in the buffer prior to changing the port mode will be lost.*

7.2.1.4. Modem Mode

The Modem Mode provides features specifically related to dial-up modem communication. A Modem Mode Port can perform all functions normally available in Any-to-Any Mode. The Modem Mode is available at all ports except the Network Port.

When a call is received, the unit will prompt the caller to enter a username and password. The WTI Device 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.

Notes:

- *When a Modem Mode port exits the user interface, or the DCD line is lost while the user interface is active, the WTI Device 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.*
- *The Internal Modem Port is always configured for Modem Mode. Note that some models do not include an internal dial-up modem.*
- *WTI Devices that include the Cellular Modem Option do not include a dial-up modem.*
- *When an external dial-up modem is installed at a serial port, other ports can use the modem for calling out. To call out, invoke the /C command to connect to the port, then access the modem as you normally would.*

7.2.1.5. Modem PPP Mode

The Modem PPP Mode allows data normally sent via Ethernet to be sent via phone line. Modem PPP Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem PPP Mode also allows definition of additional communications-related parameters. The Modem PPP Mode is not available at the Network Port.

When a call is received, the unit will prompt the caller to enter a username and password. The WTI Device 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.

Notes:

- *When the Port Mode is set to Modem PPP, that port will appear in the Network Configuration menu, listed as [ppp0].*
- *Only one Serial Port on each WTI Device may be configured for Modem PPP Mode at a given time.*
- *On WTI Console Server products and WTI Console Server + Power Control products that include the Cellular Modem option, Serial Ports cannot be set to Modem PPP Mode.*

7.3. 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.)*
- *(Console Products Only) The settings for the following parameters defined via the Network Parameters menu (Web Interface) and Network Parameters menu (CLI) will also be applied to the USB Mini format SetUp Port: Administrator Mode, Logoff Character, Sequence Disconnect, Inactivity Timeout, Command Echo and Accept Break.*

The Network Configuration Menus:

Depending on the options present on the WTI Device, network parameters are defined via suite of up to six main configuration menus:

- **Network Configuration [eth0] IPv4:** Defines IPv4 Parameters for the primary Ethernet Port (eth0), plus shared parameters that are applicable to both Ethernet Ports and both IP Protocols. For more information, please refer to Section 7.3.1.
- **Network Configuration [eth1] IPv4:** Defines IPv4 Parameters for the optional, secondary Ethernet Port (eth1). For more information, please refer to Section 7.3.2.

If the WTI Device includes the optional Secondary Ethernet Port (eth0), the following two Network Menus will also be present:

- **Network Configuration [eth0] Ipv6:** Defines IPv6 Parameters for the primary Ethernet Port (eth0). For more information, please refer to Section 7.3.3.
- **Network Configuration [eth1] IPv6:** Defines IPv6 Parameters for the optional, secondary Ethernet Port (eth1). For more information, please refer to Section 7.3.4.

If the WTI Device includes the optional Cellular Modem, the following two Network Configuration menus will also be present:

- **Cellular Configuration [cell] IPv4:** Defines IPv4 Parameters for the optional Cellular Modem. For a description of the parameters included in the cell/IPv4 menu, please refer to Section 7.4.1.
- **Cellular Configuration [cell] IPv6:** Defines IPv6 Parameters for the optional Cellular Modem. For a description of the parameters included in the cell/IPv6 menu, please refer to Section 7.4.2.

  Note: *If the WTI Device includes the optional Internal Analog Modem and the Analog Modem is configured for Modem PPP mode, then parameters for network communication via the Analog Modem can be set using the Serial Port Configuration menu as described in Section 7.2.1.5.*

Automation

WTI Devices 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.

7.3.1. Network Configuration [eth0] IPv4 Menu

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

7.3.1.1. Shared Network Parameters

This menu is used to define Network Parameters that will be shared by both IPv4 and IPv6 protocols. If the optional, secondary Ethernet Port (eth1) is present, parameters defined via this menu will also be shared by both Ethernet Ports. 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 WTI Devices's Ethernet Port(s.) When enabled, users connected to the WTI Device 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.

7.3.1.2. Network Parameters [eth0] IPv4

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

Parameter (Default)	Description
IP Address (Default = 192.168.168.168)	The IPv4 format address for the primary 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 WTI Device via the CLI and invoke the /P command as described in Section 12.4.3.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the primary 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 WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the primary 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 WTI Device via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol. When enabled, the WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
Fallback (Default = Off)	(Units with Dual Ethernet Ports Only) Enables/disables Ethernet fallback capabilities. When enabled, WTI Devices that include the optional secondary Ethernet Port will automatically switch to the other Ethernet port whenever the unit detects that a network connection cannot be established via the Ethernet port currently in use. When the Fallback feature is enabled, the same IP Address will be assigned to both eth0 and eth1. **Notes:** • *When Fallback is enabled, identical MAC addresses will be assigned to each Ethernet Port.* • *When Fallback is enabled, the two Ethernet Ports will be bonded, and will share the common parameters of Ethernet Port 0.* • *After the Fallback feature causes the WTI Device to switch to the other Ethernet port, the WTI Device will not automatically return to the initial Ethernet port after connection is restored.*

7.3.1.3. DHCP Server [eth0] IPv4

The DHCP Server menu allows you to define DHCP Server parameters for IPv4 communication via the primary 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 Primary Ethernet Port (eth0.)
Gateway (Default = Undefined)	The IPv4 format Gateway Address for the Primary 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 WTI Device via the CLI.*
Primary DNS (Default = Undefined)	The primary IPv4 format DNS address for the Primary Ethernet Port (eth0.)
Secondary DNS (Default = Undefined)	The secondary IPv4 format DNS address for the Primary Ethernet Port (eth0.)
Domain (Default = Undefined)	The IPv4 format Domain address for the Primary 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.*

7.3.1.4. IP Tables IPv4

The IP Tables menu allow the WTI Device 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.*

7.3.1.5. 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 WTI Device via the primary Ethernet Port (eth0.)

7.3.1.6. 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.

7.3.1.6.1. DNS Servers (Shared)

The DNS Parameters menu is used to select IPv4 or IPv6 format IP addresses for Domain Name Servers for both the primary [eth0] and optional secondary [eth1] Ethernet Ports. 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.*

7.3.1.6.2. 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 WTI Device will ping the DDNS host address.

7.3.1.7. Negotiation [eth0] IPv4/IPv6

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

Notes:

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

7.3.1.8. 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 primary Ethernet Port (eth0.)

7.3.1.8.1. Web Access [eth0] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the primary 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 9.
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 9.
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.

7.3.1.8.2. SSL Certificates [eth0]

Defines SSL Certificate parameters for the primary 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.

7.3.1.8.3. 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 primary 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.

7.3.1.9. Syslog Parameters IPv4/IPv6

Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the WTI Device. Allows definition of IP addresses for both a primary Syslog Daemon and an optional secondary Syslog Daemon. The Syslog Parameters IPv4 menu is used to define Syslog Addresses for both the primary Ethernet Port (eth0) and optional secondary Ethernet Port (eth1, if present.)

7.3.1.9.1. Syslog Client Parameters IPv4

Defines parameters for the Syslog Client for IPv4 communication via the Primary 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.*

7.3.1.9.2. Syslog Server Parameters IPv4

Defines parameters for the Syslog Server for IPv4 communication via the Primary 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

7.3.1.10. SNMP Parameters [eth0] IPv4

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

> **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot 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 WTI Device. It does not effect the ability of the WTI Device to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the WTI Device will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device using SNMPv2 will not be allowed to connect. When V3 is selected, the menu shown in Section 7.3.1.10.1 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 WTI Device via SNMP. Note: In order to define user names for the WTI Device 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 WTI Device.
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 7.3.1.10.1..

7.3.1.10.1. 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.3.1.11. 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 WTI Device'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.

7.3.1.12. LDAP Parameters (Shared)

WTI Devices 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 WTI Device, and existing users can also be removed without the need to delete the account from each WTI Device. This also allows administrators to assign users to LDAP groups, and then specify which plugs the members of each group will be allowed to control at each WTI Device.

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 WTI Device 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 WTI Device 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. If the WTI Device includes the optional, secondary Ethernet Port (eth1,) then parameters will apply to both the primary Ethernet Port (eth0) and secondary Ethernet Port (eth1.)*
- *Port and Plug access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each WTI Device and are specific to that WTI Device unit alone.*
- *When LDAP is enabled, LDAP authentication will supersede any passwords and access rights that have been defined via the WTI Device user directory.*
- *If no LDAP groups are defined on a given WTI Device, 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 WTI Device.
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 WTI Device.
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 WTI Device 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 7.3.1.12.2.*

7.3.1.12.1. 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.

7.3.1.12.2. 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 WTI Device.

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. For more information, please refer to Section 7.5.1.
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.*
Current/Power Metering (Default = Off)	(Units with Current Metering Option Only) This parameter is used to enable/disable the LDAP Group's access to current and power metering functions.
Configure Port Access (Default = Undefined)	(Console Units Only) Select ports that members of this LDAP group will be allowed to connect. **Note**: *When configuring a WTI Device that includes an internal dial-up modem, the Port Access parameter is also used to grant or deny user access to the internal modem port*.
Configure Plug Access (Default = Undefined)	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Determines which plugs members of this group will be allowed to control.
Configure Plug Group Access (Default = Undefined)	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) This item is used to determine which plug 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 Plug Group as described in Section 7.7.*

7.3.1.13. TACACS Parameters [Shared]

The TACACS Parameters [Shared] Menu is used to set TACACS parameters. If the WTI Device includes the optional, secondary Ethernet Port (eth1,) the TACACS Parameters menu will also set TACACS parameters for both Ethernet Ports. The TACACS Parameters Menu includes the following options:

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the TACACS feature at the Network Port(s.)
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.
Fallback Local (Default = Off)	Determines whether or not the WTI Device will fallback to its own username directory when an authentication attempt fails. When enabled, the unit will first attempt to authenticate the password by checking the TACACS Server. If this fails, the unit will then attempt to authenticate the password by checking 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.
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 7.3.1.13.1.

7.3.1.13.1. Default TACACS User Access (Shared)

When enabled, allows TACACS users to access the unit without first defining a TACACS user account on the WTI Device. 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.
Current/Power Metering (Default = Off)	(Units with Current Metering Option Only) Determines whether or not new TACACS users will be allowed to access current metering and power metering functions by default.
Configure Port Access (Defaults; Administrator and SuperUser = All Ports On, User = Undefined, ViewOnly = Undefined)	(DSM, CPM and REM Series Products Only) Determines the default Port Access setting for new TACACS users. The Port Access setting determines which serial ports each account will be allowed to control by default.
Configure Plug Access (Defaults; Administrator and SuperUser = All Plugs On, User = Undefined, ViewOnly = Undefined)	(Power Products Only) Determine which plugs new TACACS users will be allowed to control by default.
Configure Plug Group Access (Defaults; Administrator and SuperUser = All Plug Groups On, User = Undefined, ViewOnly = Undefined)	(Power Products Only) This item is used to determine which plug groups new TACACS users will be allowed to control by default. **Note:** *Prior to setting this parameter, you must first define at least one Plug Group as described in Section 7.7.*

7.3.1.14. RADIUS Parameters [Shared]

The RADIUS Parameters [Shared] Menu is used to set RADIUS parameters for both IPv4 and IPv6 protocols. If the WTI Device includes the optional, secondary Ethernet Port (eth1,) the RADIUS Parameters menu will also set RADIUS parameters for both Ethernet Ports.

Notes:

- *For information regarding setting up the WTI Device 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 WTI Device 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 WTI Device will fallback to its own password/username directory when an authentication attempt fails. When enabled, the WTI Device will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the WTI Device 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 WTI Device 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 7.3.1.12.1.

7.3.1.14.1. Default RADIUS User Access (Shared)

When enabled, allows RADIUS users to access the unit without first defining a RADIUS user account on the WTI Device. 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. **Note:** *The Outbound Telnet option is not available on WTI Power Control Products.*
Current/Power Metering (Default = Off)	(Units with Current Metering Option Only) Determines whether or not new RADIUS users will be allowed to access current metering and power metering functions by default.
Configure Port Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	(Console Products Only) Determines the default Port Access setting for new RADIUS users. The Port Access setting determines which serial ports each account will be allowed to control by default.
Configure Plug Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	(Power Control products only) Determine which plugs new RADIUS users will be allowed to control by default.
Configure Plug Group Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	(Power Control products only) This item is used to determine which plug groups new RADIUS users will be allowed to control by default. **Note:** *Prior to setting this parameter, you must first define at least one Plug Group as described in Section 7.7.*

7.3.1.14.2. 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”`

- **`WTI-Plug-Access`** - (WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Determines which plug(s) the user will be allowed to access. This command provides an argument that consists of a four character string, with one character for each the switched outlets. The following options are available for each switched plug:
  - `0` = Off (Deny Access)
  - `1` = On (Allow Access)

  For example, to allow access to Plugs 2 and 4, the command line would be:

  `WTI-Plug-Access=”0101”`

  Note: *Power switching functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

- **WTI-Group-Access** - (WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Determines which plug group(s) the user will be allowed to access. The argument for this command includes a character for each, defined plug group, with the first character in the string being used to represent the first plug group defined, and the last character in the string representing the last plug group defined. The following options are available for each plug group:

  0 = Off (Deny Access)
  1 = On (Allow Access)

  For example, to allow access to the first three defined plug groups out of a total of six defined plug groups, the command line would be:

  WTI-Group-Access="111000"

  Note: *Power switching functions are only available on WTI Power Control Products and WTI Console Server + Power Control Combo Products.*

Example:

The following command could be used to set the command access level to "User", allow access to Serial Ports 1, 3, 5 and 7:

```
tom  Auth-Type:=Local, User-Password=="tom1"
   Login-Service=Telnet,
   Login-TCP-Port=Telnet,
   User-Name="HARRY-tom",
   WTI-Super="1",
   WTI-Port-Access="10101010",
```

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

Configures the WTI Device's response to ping commands at the primary 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 WTI Device.

7.3.1.16. Email Messaging [IPv4]

The Email Messaging (IPv4) menu is used to define IPv4 parameters that will be used for email communication sent from the primary Ethernet Port (eth0) and the optional secondary Ethernet Port (eth1.) The WTI Device 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 WTI Device 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 WTI Device 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 WTI Device.
From Address (Default = Undefined)	The email address that will appear in the “From” field in email sent by the WTI Device.
To Address (Default = Undefined)	These prompts are used to defined up to three address that will receive email messages generated by the WTI Device. 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.

7.3.2. Network Configuration [eth1] IPv4 Menus

The Network Configuration [eth1] IPv4 Menus are used to define network communication parameters that apply only to IPv4 protocol access to the optional, secondary Ethernet Port (eth1.)

Notes:

- *If the WTI Device does not include the optional secondary Ethernet Port (eth1), then this menu will not be present.*
- *The optional secondary Ethernet Port (eth1) is only available on CPM and DSM Series products.*

7.3.2.1. Network Parameters [eth1] IPv4

This menu is used to assign the IP Address, Subnet Mask and other IPv4 parameters for the optional, secondary Ethernet Port (eth1).

Parameter (Default)	Description
IP Address (Default = 192.168.168.168)	The IPv4 format address for the primary Ethernet Port, eth1. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the WTI Device via the CLI.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the primary Ethernet Port, eth1. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the primary Ethernet Port, eth1. **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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*

7.3.2.2. DHCP Server [eth1] IPv4

The DHCP Server menu allows you to define DHCP Server parameters for IPv4 communication via the primary 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 Primary Ethernet Port (eth0.)
Gateway (Default = Undefined)	The IPv4 format Gateway Address for the Primary 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 WTI Device via the CLI.*
Primary DNS (Default = Undefined)	The primary IPv4 format DNS address for the Primary Ethernet Port (eth0.)
Secondary DNS (Default = Undefined)	The secondary IPv4 format DNS address for the Primary Ethernet Port (eth0.)
Domain (Default = Undefined)	The IPv4 format Domain address for the Primary Ethernet Port (eth0.)
Default Lease (Default = 600)	Defines the 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)	Defines the start of the address pool.
Pool End (Default = 254)	Defines the end of the 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.*

7.3.2.3. Static Route [eth1] IPv4

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 optional, secondary Ethernet Port (eth1) or optional Cellular Modem Port.

7.3.2.4. DDNS Parameters [eth1] IPv4

The DDNS Parameters menu is used to select parameters and define hosts for Dynamic DNS services for IPv4 communication via the optional, secondary Ethernet Port (eth1.) 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 WTI Device will ping the DDNS host address.

7.3.2.5. Negotiation [eth1] IPv4/IPv6

This parameter can be used to solve synchronization problems when the WTI Device negotiates IPv4 communication parameters with another device via the optional, secondary Ethernet Port (eth1.).

Notes:

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

7.3.2.6. Web Selection [eth1] 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 optional, secondary Ethernet Port (eth1.)

7.3.2.6.1. Web Access [eth1] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the optional, secondary Ethernet Port (eth1.)

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 9.
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 9.

7.3.2.6.2. SSL Certificates [eth1]

Defines SSL Certificate parameters for the optional, secondary Ethernet Port (eth1.)

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.

7.3.2.6.3. Import Wildcard Certs [eth1] (SSL Certificate Import)

The Import Wildcard Certs Menu (SSL Certificate Import) is used to import a private key, a signed certificate and a CA Intermediate Certificate for the Web server for the optional, secondary Ethernet Port (eth1]. 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	An intermediate CA certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. Such certificates are called chained root certificates.

7.3.2.7. SNMP Parameters [eth1] IPv4

This menu is used to select IPv4 format access parameters for the SNMP feature at the optional, secondary Ethernet Port (eth1.)

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

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling at the optional, secondary Ethernet Port (eth1.). **Note:** *Applies only to external SNMP polling of the WTI Device. It does not effect the ability of the device to send SNMP traps.*
Version (Default = V1/V2 Only)	Determines which SNMP Version the optional, secondary Ethernet Port (eth1) will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device via eth1 using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the optional, secondary Ethernet Port (eth1.) This controls the ability to access configuration functions and invoke commands. When Enabled, you will not be able to change parameters or invoke other commands when you contact the WTI Device's optional, secondary Ethernet Port (eth1) via SNMP. **Note:** *In order to define user names for the WTI Device 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 WTI Device.
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 7.3.2.7.1.

7.3.2.7.1. 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.3.2.8. Ping Parameters [eth1] IPv4

Configures the WTI Device's response to ping commands at the optional, secondary 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 WTI Device.

7.3.3. 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 primary Ethernet Port (eth0.)

7.3.3.1. Network Parameters [eth0] IPv6

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

Parameter (Default)	Description
IP Address (Default = Undefined)	The IPv6 format address for the primary 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 WTI Device via the CLI.*
Subnet Prefix (Default = Undefined)	Defines the IPv6 Subnet Prefix.
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the primary 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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*

7.3.3.2. IP Tables IPv6

The IP Tables menu allow the WTI Device to restrict unauthorized IP addresses from establishing inbound connections to the unit. If you wish to restrict access to the WTI Device, 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.*

7.3.3.3. 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 primary Ethernet Port (eth0.)

7.3.3.4. DNS Selection Menu [eth0 / IPv6]

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

7.3.3.4.1. DNS Servers (Shared)

The DNS Parameters menu is used to select IP addresses for Domain Name Servers for both the primary [eth0] and optional secondary [eth1] Ethernet Ports. 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.*

7.3.3.4.2. DDNS Parameters [eth0] IPv4

The DDNS Parameters menu is used to select parameters and define hosts for Dynamic DNS services for IPv6 communication via the primary 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 WTI Device will ping the DDNS host address.

7.3.3.5. Negotiation [eth0] IPv4/IPv6

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

Notes:

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

7.3.3.6. 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 primary Ethernet Port (eth0.)

7.3.3.6.1. Web Access [eth0] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the primary Ethernet Port (eth1.)

> **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 9.
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 9.
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.)

7.3.3.6.2. SSL Certificates [eth0]

Defines SSL Certificate parameters for the primary 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.

7.3.3.6.3. 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 primary 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.

7.3.3.7. 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.*

7.3.3.8. SNMP Parameters [eth0] IPv6

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

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

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling at the primary Ethernet Port (eth0.). **Note:** *This parameter applies only to external SNMP polling of the WTI Device. It does not effect the ability of the WTI Device to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the primary Ethernet Port (eth0) will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device via eth0 using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the primary 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 WTI Device's primary Ethernet Port (eth0) via SNMP. **Note:** *In order to define user names for the WTI Device 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 WTI Device.
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.

7.3.3.8.1. 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.3.3.9. 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 WTI Device'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.

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

Configures the WTI Device's response to ping commands at the primary 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 WTI Device.

7.3.3.11. Email Messaging [IPv6]

The Email Messaging (IPv6) menu is used to define IPv6 parameters that will be used for email communication sent from the primary Ethernet Port (eth0) and the optional secondary Ethernet Port (eth1.) The WTI Device 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 WTI Device 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 WTI Device 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 WTI Device.
From Address (Default = Undefined)	The email address that will appear in the “From” field in email sent by the WTI Device.
To Address (Default = Undefined)	These prompts are used to defined up to three address that will receive email messages generated by the WTI Device. 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.

7.3.4. Network Configuration [eth1] IPv6 Menus

The Network Configuration [eth1] IPv6 Menus are used to define network communication parameters that apply only to IPv6 protocol access to the optional, secondary Ethernet Port (eth1.)

Notes:

- *If the WTI Device does not include the optional secondary Ethernet Port (eth1), then this menu will not be present.*
- *The optional secondary Ethernet Port (eth1) is only available on , DSM Series products.*

7.3.4.1. Network Parameters [eth1] IPv6

This menu is used to assign the IP Address, Subnet Mask and other IPv6 parameters for the optional, secondary Ethernet Port (eth1).

Parameter (Default)	Description
IP Address (Default = Undefined)	The IPv6 format address for the primary Ethernet Port, eth1. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the WTI Device via the CLI.*
Subnet Prefix (Default = Undefined)	Defines the IPv6 Subnet Prefix.
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the primary Ethernet Port, eth1. **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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*

7.3.4.2. Static Route [eth1] 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 optional, secondary Ethernet Port (eth1) or optional Cellular Modem Port.

7.3.4.3. DDNS Parameters [eth1] IPv6

The DDNS Parameters menu is used to select parameters and define hosts for Dynamic DNS services for IPv6 communication via the optional, secondary Ethernet Port (eth1.) 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 IPv6 format 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 WTI Device will ping the DDNS host address.

7.3.4.4. Negotiation [eth1] IPv4/IPv6

This parameter can be used to solve synchronization problems when the WTI Device negotiates IPv4/IPv6 communication parameters with another device via the optional, secondary Ethernet Port (eth1.).

Notes:

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

7.3.4.5. Web Selection [eth1] 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 optional, secondary Ethernet Port (eth1.)

7.3.4.5.1. Web Access [eth1] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the optional, secondary Ethernet Port (eth1.)

> **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 9.
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 9.

7.3.4.5.2. SSL Certificates [eth1]

Defines SSL Certificate parameters for the optional, secondary Ethernet Port (eth1.)

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.

7.3.4.5.3. Import Wildcard Certs [eth1] (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 optional, secondary Ethernet Port (eth1]. 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.

7.3.4.6. SNMP Parameters [eth1] IPv6

This menu is used to select IPv6 format access parameters for the SNMP feature at the optional, secondary Ethernet Port (eth1.)

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

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling at the optional secondary Ethernet Port (eth1.). **Note:** *This parameter applies only to external SNMP polling of the WTI Device. It does not effect the ability of the WTI Device to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the optional, secondary Ethernet Port (eth1) will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device via eth0 using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the primary 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 WTI Device's optional, secondary Ethernet Port (eth1) via SNMP. **Note:** *In order to define user names for the WTI Device 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.*
Authentication / **Privacy** (Default = Auth/noPriv)	Configures the Authentication and Privacy features for SNMPv3 communication via the optional, secondary Ethernet Port (eth1.) 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 WTI Device supports DES encryption, but does not currently support the AES protocol.* • *The WTI Device does not support "noAuth/noPriv" for SNMPv3 communication.*
SNMPv3 User Name (Default = Undefined)	Sets the User Name for SNMPv3 communication via the optional, secondary Ethernet Port (eth1.) Note that this option is not available when the Version parameter is set to V1/V2.

Parameter (Default)	Description
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)	Determines which authentication protocol will be used at the optional secondary Ethernet Port (eth1.) WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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 for the optional, secondary Ethernet Port (eth1.)
System Name (Default = Undefined)	The host name of the WTI Device.
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 7.3.4.6.1.

7.3.4.6.1. SNMP V3 Users (eth1 / 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.3.4.7. Ping Parameters (Ping Access) [eth1] IPv6

Configures the WTI Device's response to ping commands at the optional, secondary 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 WTI Device.

7.4. Cellular Configuration

When the Internal Cellular Modem Option is present, the Cellular Configuration menus are used to select IPv4 and IPv6 parameters for cellular communication.

> **Note:** *The Cellular Configuration menus are only present on WTI Devices that include the Cellular Modem Option.*

The Cellular Configuration Menus:

Cellular Configuration parameters are defined via two sets of configuration menus; one for IPv4 parameters and one for IPv6 Parameters:

- **Cellular Configuration IPv4:** Defines IPv4 Parameters for Cellular Modem option.
- **Cellular Configuration IPv6:** Defines IPv6 Parameters for the Cellular Modem option.

7.4.1. Cellular Configuration IPv4 Menus

The Cellular Configuration IPv4 Menus are used to assign IPv4 parameters for the optional Cellular Modem.

7.4.1.1. Network Parameters [cell] IPv4

The Network Parameters [cell] IPv4 menu is used to enable the Default Gateway and DHCP for IPv4 communication with the WTI Device via cellular.

> ***Note:*** *There are two separate menus for IPv4 and IPv6 communication, allowing you to choose a different enable/disable status for IPv4 and IPv6.*

Parameter (Default)	Description
Default Gateway (Default = Off)	Enables/disables the Default Gateway for IPv4 communication. **Note:** *The status of the Default Gateway parameter cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol. When enabled, the WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
Use Peer DNS (Default = Off)	When enabled, the DNS information from the Cellular provider will be used.

7.4.1.2. Static Route [cell] IPv4/IPv6

The Static Route menu allows you to define Linux routing commands for IPv4 and/or IPv6 that will be automatically executed each time that a user accesses the user interface via the optional, Cellular Modem Port.

7.4.1.3. DDNS Parameters [cell] IPv4

The DDNS Parameters [cell] menus are used to select parameters and define hosts for Dynamic DNS services. The IPv4 DDNS Parameters menus offers the following options:

> **Note:** *There are two separate DDNS [cell] menus; one for IPv4 communication and one for IPv6 communication. This allows you to set up separate DDNS parameters for each protocol.*

Parameter (Default)	Description
Services (Default = None)	Sets the service type to either Dyn or None.
Host Name (Default = Undefined)	The IPv6 format 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 WTI Device will ping the DDNS host address.

7.4.1.4. Web Selection [cell] 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 optional, Cellular Modem.

7.4.1.4.1. Web Access [cell] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the optional, Cellular Modem.

> **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 9.
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 9.

7.4.1.4.2. SSL Certificates [cell]

Defines SSL Certificate parameters for the optional, Cellular Modem.

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.

7.4.1.4.3. Import Wildcard Certs [cell] (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 optional, Cellular Modem Port. 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.

7.4.1.5. SNMP Parameters [cell] IPv4

The SNMP Parameters [cell] menu is used to define SNMP Parameters for IPv4 communication via the optional Cellular Modem Port. Note that

Notes:

- *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
- *There are two separate SNMP Parameters [cell] menus; one for IPv4 communication and one for IPv6 communication.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling at the optional Cellular Modem Port. **Note:** *This parameter applies only to external SNMP polling of the WTI Device. It does not effect the ability of the WTI Device to send SNMP traps.*
Version (Default = V1/V2 Only)	This parameter determines which SNMP Version the optional, Cellular Modem Port will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device via eth0 using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the optional, Cellular Modem Port. 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 WTI Device's optional, Cellular Modem Port via SNMP. **Note:** *In order to define user names for the WTI Device 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 WTI Device.
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 7.4.1.5.1.

7.4.1.5.1. SNMP V3 Users [cell / 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.4.1.6. Ping Parameters (Ping Access) [cell] IPv4/IPv6

Configures the WTI Device's response to ping commands at the optional, Cellular Modem Port.

> **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 WTI Device.

7.4.1.7. Modem PPP Parameters

The Modem PPP Parameters Menu is used to display currently defined Modem PPP parameters for the optional, Cellular Modem Port. Note that the IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will instead be automatically supplied by the ISP when a PPP communication session is started.

Parameter (Default)	Description
PPP Phone Number	The phone number for the line used for PPP communication.
IP Address	The temporary IP address that will be assigned to the PPP communication session by the ISP.
P-t-P	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	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.

7.4.1.8. Public IP [cell] IPv4/IPv6

Defines the IPv4 or IPv6 format Public IP address for communication via the optional Cellular Modem Port.

7.4.1.9. Wakeup on Failure

The Wakeup On Failure feature allows WTI units that include the cellular modem option to put the cell modem into a non connected sleep state, with its wired Ethernet port(s) acting as the unit's primary network interfaces. The modem will only wakeup when certain failure conditions are detected on specified wired Ethernet ports.

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the Wakeup on Failure feature.
Interface to Monitor (Default = eth0)	Selects the Ethernet interface(s) that will be monitored for failed ping responses. A Wakeup event will be triggered if the network cable is disconnected or a failed ping response is detected at the selected Ethernet interface(s.)
Primary Address / Host to Ping (Default = Undefined)	Selects the primary host that will be pinged in order to test for failures. If primary and secondary hosts both fail to respond to pings on the specified interface(s), a Wakeup is triggered.
Secondary Address / Host to Ping (Default = Undefined)	Selects the secondary host that will be pinged in order to test for failures. If primary and secondary hosts both fail to respond to pings on the specified interface(s), a Wakeup is triggered.
Ping Interval (Default = 60)	Determines how often the selected IP Address will be pinged. The Ping Interval can be any whole number, from 1 to 3,600 seconds.
Interval After Failed Ping (Default = 10)	Determines how often the Ping command will be sent after a previous Ping command receives no response.
Consecutive Failures (Default = 5)	Determines how many consecutive failures pings must be detected in order to initiate a Wakeup on Failure.
Autorecovery (Default = Off)	When enabled, the cellular modem will automatically be put back into sleep state when failure is resolved. When disabled, Wakeup On Failure must be manually re-enabled to put the modem back into sleep state.
Ethernet Default Gateway Port (Default = eth0)	The Ethernet port that will be used as the default gateway when the cellular modem is in the sleep state.
Ethernet Default Gateway Address (Default = Undefined)	When the cellular modem is defined as the default gateway, this parameter determines which Ethernet interface will be the default gateway while the cellular modem is in sleep state.
Sleep Mode (Default = Attach)	Determines whether the cell modem will be attached or detached from the cell tower when sleep mode is active.
Re-enable Wakeup on Failure	After an Ethernet failure has triggered a Wakeup, this feature is used to manually re-enable Wakeup On Failure, and put the cellular modem back to sleep after the failure has been resolved. This is only applicable when Autorecovery is disabled. When Autorecovery is enabled, Wakeup On Failure is automatically re-enabled once the issue is resolved.
Ping Wakeup on Failure Hosts	Pings the currently defined primary and secondary host addresses.

7.4.1.10. IP Passthrough

Allows the WTI device to share its cellular internet connection and public IP to a downstream device, (i.e., a router), making the modem connection appear as a regular Ethernet connection to the downstream device. This allows the cellular internet connection to serve as a primary or backup WAN interface for your device or LAN.

While IP Passthrough mode passes any connections to the cellular modem's public IP through to the downstream device, connections can still be terminated on the WTI interface via Service Local Termination Ports. This makes the unit accessible for normal out of band management.

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables the IP Paasthrough feature.
Interface (Default = eth0)	Selects the interface that your downstream device/router will be connected to. The cell modem public IP will be passed to this device.
MAC (Default = Undefined)	The MAC address of your downstream device/router. The cell modem public IP will be passed to this device. If no MAC is specified, the cell modem public IP will be passed to the last device to request an IP via DHCP. Format should be aa:bb:cc:dd:ee:ff
HTTP Enable: (Default = Off)	Enables/disables HTTP.
HTTP Port (Default = 80)	When IP Passthrough is enabled, the Cellular HTTP Port will be incremented by 5000. This port will terminate locally on this unit and will not be passed through to the downstream device/router. When IP Passthrough is disabled, the HTTP Port will be restored to its original value.
HTTPS Enable (Default = On)	Enables/disables HTTPS.
HTTPS Port (Default = 443)	When IP Passthrough is enabled, the Cellular HTTPS Port will be incremented by 5000. This port will terminate locally on this unit and will not be passed through to the downstream device/ router. When IP Passthrough is disabled, the HTTPS Port will be restored to its original value.
SSH Enable (Default = On)	Enables/disables SSH.
SSH Port (Default = 22)	When IP Passthrough is enabled, the Cellular SSH Port will be incremented by 5000. This port will terminate locally on this unit and not be passed through to the downstream device/router. When IP Passthrough is disabled, SSH Port will be restored to its original value.

7.4.2. Cellular Configuration IPv6 Menus

The Cellular Configuration IPv6 Menus are used to assign IPv6 parameters for the optional Cellular Modem.

7.4.2.1. Network Parameters [cell] IPv6

The Network Parameters [cell] IPv4 and Network Parameters [cell] IPv6 menus are used to enable the Default Gateway and DHCP for IPv4 and IPv6 communication with the WTI Device via cellular.

Note: *There are two separate menus for IPv4 and IPv6 communication, allowing you to choose a different enable/disable status for IPv4 and IPv6.*

Parameter (Default)	Description
Default Gateway (Default = Off)	Enables/disables the Default Gateway for IPv6 communication. **Note:** *The status of the Default Gateway parameter cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol. When enabled, the WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
Use Peer DNS (Default = Off)	

7.4.2.2. Static Route [cell] IPv4/IPv6

The Static Route menu allows you to define Linux routing commands for IPv4 and/or IPv6 that will be automatically executed each time that a user accesses the user interface via the optional, Cellular Modem Port.

7.4.2.3. DDNS Parameters [cell] IPv6

The DDNS Parameters [cell] menus are used to select parameters and define hosts for Dynamic DNS services. The IPv6 DDNS Parameters menus offers the following options:

> **Note:** *There are two separate DDNS [cell] menus; one for IPv4 communication and one for IPv6 communication, allowing you to set up separate DDNS parameters for each protocol.*

Parameter (Default)	Description
Services (Default = None)	Sets the service type to either Dyn or None.
Host Name (Default = Undefined)	The IPv6 format 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 WTI Device will ping the DDNS host address.

7.4.2.4. Web Selection [cell] 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 optional, Cellular Modem.

7.4.2.4.1. Web Access [cell] IPv4/IPv6

This menu is used to define both IPv4 and IPv6 Web Access Parameters for the optional, Cellular Modem.

> **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 9.
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 9.

7.4.2.4.2. SSL Certificates [cell]

Defines SSL Certificate parameters for the optional, Cellular Modem.

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.

7.4.2.4.3. Import Wildcard Certs [cell] (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 optional, Cellular Modem Port. 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.

7.4.2.5. SNMP Parameters [cell] IPv6

The SNMP Parameters [cell] menu is used to define SNMP Parameters for IPv4 communication via the optional Cellular Modem Port.

Notes:

- *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
- *There are two separate SNMP Parameters [cell] menus; one for IPv4 communication and one for IPv6 communication. This allows you to set up separate SNMP Parameters for each protocol.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/disables SNMP Polling via IPv4 at the optional, Cellular Modem Port. **Note:** *This parameter applies only to external SNMP polling of the WTI Device. It does not effect the ability of the WTI Device to send SNMP traps.*
Version (Default = V1/V2 Only)	Determines which SNMP Version the optional, Cellular Modem Port will respond to. For example, if this item is set to V3, then clients who attempt to contact the WTI Device via cell using SNMPv2 will not be allowed to connect.
Read Only (Default = No)	Enables/Disables the "Read Only Mode" at the optional, Cellular Modem Port. 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 WTI Device's optional, Cellular Modem Port via SNMP. **Note:** ***In order to define user names for the WTI Device 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 WTI Device.
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 7.4.2.5.1.

7.4.2.5.1. SNMP V3 Users [cell / 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 WTI Device supports DES encryption, but does not currently support the AES protocol. • The WTI Device 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. WTI Devices support both MD5 and SHA1 authentication. **Notes:** • *The Authentication Protocol that is selected for the WTI Device must match the protocol that your SNMP client will use when querying the WTI Device.* • *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.

7.4.2.6. Ping Parameters (Ping Access) [cell] IPv4/IPv6

Configures the WTI Device's response to ping commands at the optional, Cellular Modem Port.

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 WTI Device.

7.4.2.7. Modem PPP Parameters

The Modem PPP Parameters Menu is used to display currently defined Modem PPP parameters for the optional, Cellular Modem Port. Note that the IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will instead be automatically supplied by the ISP when a PPP communication session is started.

Parameter (Default)	Description
PPP Phone Number	The phone number for the line used for PPP communication.
IP Address	The temporary IP address that will be assigned to the PPP communication session by the ISP.
P-t-P	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	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.

7.4.2.8. Public IP [cell] IPv4/IPv6

Defines the IPv4 or IPv6 format Public IP address for communication via the optional Cellular Modem Port.

7.5. 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 serial ports and/or switched outlets 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.

7.5.1. 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. WTI Devices offer four different Access Levels for User Accounts:

Notes:

- *Power switching functions are only present on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *Serial Console Port functions are only present on WTI Console Server products and WTI Console Server products plus Power Control Combo products.*

- **Administrator:**Administrator accounts are allowed to invoke all configuration and operation commands, view all status screens, and control all serial ports and switched outlets present on the WTI Device.
- **SuperUser:** SuperUser accounts are allowed to invoke all port connection and power 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 serial ports and switched outlets present on the WTI Device.
- **User:** User accounts are not allowed to access configuration menus, and are only allowed to access serial ports and switched outlets (if present) that are specifically permitted by the account.
- **ViewOnly:** ViewOnly accounts are allowed to view Status Menus, but are not allowed to invoke port connection and power switching commands or view configurations menus or change parameters. ViewOnly accounts can display the Port/Plug Status screens (if present,) but can only view the status of ports and plugs allowed by the account.

Section 12.3 summarizes command access for all four access levels.

In the default state, WTI Devices include one predefined account that provides access to Administrator commands and allows to control of all present serial ports and switched power outlets. 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 WTI Device is reset to default parameters, all User Accounts will be cleared, and the default "super" account will be restored.*

7.5.2. 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.” For more information on Command Access Levels, please refer to Section 7.5.1. and Section 12.3.
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, and whether the account will be allowed to initiate outbound connections. **Notes:** • *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 WTI Device, please refer to Section 7.3.1.1.* • *The Outbound Service option is only available on WTI Console Server products and WTI Console Server + Power Control Combo products.*
Current / **Power Metering** (Default = Off)	Enables/Disables account access to Current and Power Metering functions. **Notes:** • *Current and Power Metering functions are only available on WTI Devices that include the Current and Power Metering option.* • *Current/Power Metering functions cannot be disabled for Administrator level accounts or SuperUser level accounts.*

Parameter (Default)	Description
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 as described in Section 7.1.4. **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.
Configure Port Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	Determines which Serial Console Ports this account will be allowed to access. **Notes:** • *Administrator and SuperUser level accounts will always provide access to all Serial Ports.* • *ViewOnly accounts are allowed to display the status of Serial Ports, but are limited to the ports specified by the account. ViewOnly accounts are not allowed to create connections between ports.* • *The Port Access parameter is also used to grant or deny user access to the internal modem port (if present.)*
Configure Plug Access (Defaults; Administrator & SuperUser = All On, User = Undefined, ViewOnly = Undefined)	Determines which switched outlet(s) this account will be allowed to control. **Notes:** • *Power Control functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.* • *Administrator and SuperUser level accounts will always have access to all outlets.* • *ViewOnly accounts are allowed to display the On/Off status of outlets, but are limited to the outlets specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.* • On RPC Series DC Power Control products, this submenu is referred to as "Configure Circuit Access."

Parameter (Default)	Description
Configure Plug Group Access (Defaults; Administrator & SuperUser = All Groups On, User = Undefined, ViewOnly = Undefined)	Determines which Plug Groups this account will be allowed to control. **Notes:** • *Power Control functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.* • *In order to use this feature, Plug Groups must first be defined as described in Section 7.7.* • *Administrator and SuperUser level accounts will always have access to all plug groups.* • *ViewOnly accounts are allowed to display the On/Off status of plug groups, but are limited to the plug groups specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.* • *On RPC Series DC Power Control products, this submenu is referred to as "Configure Circuit Group Access."*

7.5.3. 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.

7.5.4. 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.

7.5.5. 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 WTI Device 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.*

7.6. 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.)

7.6.1. 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)	

7.6.2. 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)	

7.6.3. 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)	

7.7. The Plug Group Directory

Notes:

- *Power Switching functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *On RPC Series DC Power Control products, this item is referred to as the "Circuit Group Directory."*

The Plug Group Directory allows you to designate groups of plugs that are dedicated to a similar function, and will most likely be switched or rebooted all at the same time or controlled by the same user or department. When two or more switched outlets are assigned to a Plug Group, this allows you to direct On/Off/Boot commands to all switched outlets in the group, without addressing each outlet individually.

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

7.7.1. Adding Plug Groups

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

Note: *On RPC Series DC Power Control products, Plug Groups are referred to as "Circuit Groups."*

Parameter (Default)	Description
Plug Group Name (Default = Undefined)	Assigns a descriptive name to the Plug Group or Circuit Group.
Plug Access (Default = Undefined)	Determines which switched outlets (or circuits) will be included in this Plug Group (or Circuit Group.) **Notes:** • *When a series of outlets are switched On/Off or Rebooted, the Boot/Sequence Delay parameter can be used to insert a delay time between each switching operation. For more information, please refer to Section 7.8.* • *If needed, the Boot Priority parameter can be used to determine the order in which plugs are switched On/Off or rebooted. For more information, please refer to Section 7.8.1.*

7.7.2. Viewing Plug Groups

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

7.7.3. Modifying Plug Groups

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

7.7.4. Deleting Plug Groups

This function is used to delete individual Plug 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 accounts cannot be automatically restored.*

7.8. Plug Parameters

Notes:

- *Power Switching functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *On RPC Series DC Power Control Products, Plug Parameters are referred to as "Circuit Parameters."*

The Plug Parameters Menu is used to define Plug Names, boot/sequence delay times and Power Up Default values for each of the Switched Outlets. Note that this function is only available when you have accessed the user interface using a password that permits Administrator Level commands. The Plug Parameters Menu allows you to define the following parameters:

Parameter (Default)	Description
Line Input	When the WTI Device includes more than one power inlet, this item lists the sequence of outlets that draw power for each inlet.
Line Input Name (Default = Undefined)	When the WTI Device includes more than one power inlet, this item can be used to assign a descriptive name to each input.
Plug (Circuit)	The default, alphanumeric name for each switched outlet.
Plug Name (Circuit Name) (Default = Undefined)	This item can be used to assign a descriptive name to each switched outlet.
Boot/Seq. Delay (Default = 0.5 Second)	When multiple outlets (or circuits) are switched, the Boot / Sequence delay determines how much time will elapse between each switching action. When the Boot/Sequence Delay is applied, the WTI Device will wait for the user-defined delay period before switching On the next plug. For more information, please refer to Section 7.8.1. When Reboot cycles and switching actions are initiated, the Boot/Sequence Delay will be applied as follows: • **Reboot Cycle Delay:** During a reboot cycle, the WTI Device will first switch all selected plugs "Off" (with a 0.5 second pause between each "Off" operation), and then begin to switch selected plugs back On, pausing for the user-defined Boot/Sequence Delay before switching On the next plug. • **"On" Sequence Delay:** When two or more plugs are switched On, the WTI Device will pause for the user-defined Boot/Sequence Delay before switching On the next plug.

Parameter (Default)	Description
Power Up Default (Default = On)	Determines how this plug will react after power to the unit has been interrupted and then restored, or when the "Default All Plugs" command (/DPL) is invoked via the CLI. When power is restored, or the Default Command is invoked, the WTI Device will automatically switch each outlet On or Off as specified by the Power-Up Default value. **Notes:** • *If the Default command is invoked by an account that has Administrator or SuperUser level command access, then all switched outlets will be set according to the Power Up Default.* • *If the Default command is invoked by an account that has User level command access, then only the outlets allowed by the account will be set to the Power Up Default.* • *The Default command is not available to ViewOnly level accounts.*
Boot Priority (Default = All plugs prioritized according to Plug Number)	When commands are applied to two or more outlets (or circuits,) the Boot Priority parameter determines the order in which the plugs will be switched On. The outlet that has been assigned a Boot Priority value of "1" will be switched on first, followed by the outlet that has been assigned the Boot Priority value of "2", and so forth. For more information, please refer to Section 7.8.1.

7.8.1. The Boot Priority Parameter

Normally, when an "On" or "Reboot" command is invoked, the WTI Power Control Product or WTI Console Server + Power Control Combo unit will switch on it's plugs or circuits in their default, numeric order. Although in many cases, the default, numeric order will work fine, there are other cases where an individual device (such as a router) must be switched on first, in order to support a second device that will be switched on later.

The Boot Priority Parameter simplifies the process of setting the order in which plugs or circuits are switched On, by assigning a priority number to each plug or circuit, rather than by requiring the user to make certain that devices are always connected to the WTI Device in a set order. Likewise, when new devices are added to your equipment rack, the Boot Priority Parameter eliminates the need to unplug all existing devices and then rearrange the plugs connected to the WTI Device to ensure that they are switched on in the desired order.

Notes:

- *Power Switching functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *No two plugs or circuits can be assigned the same Boot Priority number.*
- *The Boot Priority is also displayed on the Plug Status Screen.*
- *On RPC Series DC Power Control Products, the Boot Priority Parameter is referred to as the "Circuit Priority Parameter."*

7.8.1.1. Example 1: Change Plug 3 to Priority 1

In the Example shown in Figure 7.1, we start out with all Plugs set to their default Boot Priorities, with Plug 1 first, Plug 2 second and so forth.

Next, the Boot Priority for Plug 3 is changed to Priority 1. This means that Plug 3 will now be switched On first after a reboot, and that Plug 1 will be switched On second, Plug 2 will be third, etc.

Note that when the Boot Priority for Plug 3 is set to 1, the Boot Priorities for all plugs that were previously Booted before plug A1 are now lowered by a factor of one.

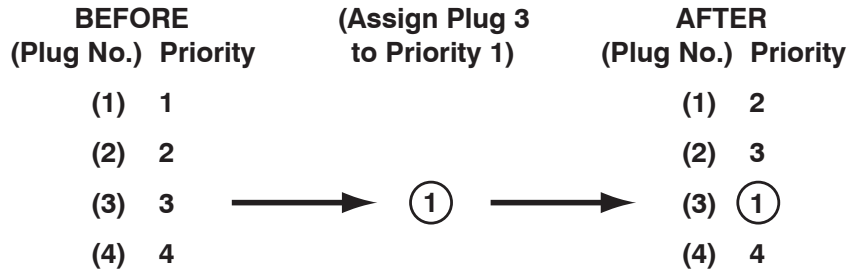

Figure 7.1: Boot Priority Example 1

7.8.1.2. Example 2: Change Plug 4 to Priority 2

In the second Example shown in Figure 7.2, we start out with Boot Priorities for the outlets set as they were at the end of Example 1; Plug 3 is first, Plug 1 is second, Plug 2 is third and Plug 4 is fourth.

Next, the Boot Priority for Plug 4 is changed to Priority 2. This means that Plug 3 will continue to be switched on first after a reboot, but now Plug 4 will be switched on second, Plug 1 will be third and Plug 2 will be fourth.

Once again, note that when the Boot Priority for Plug 4 is set to 2, the Boot Priorities for all plugs that were previously Booted before plug 4 are now lowered by a factor of one

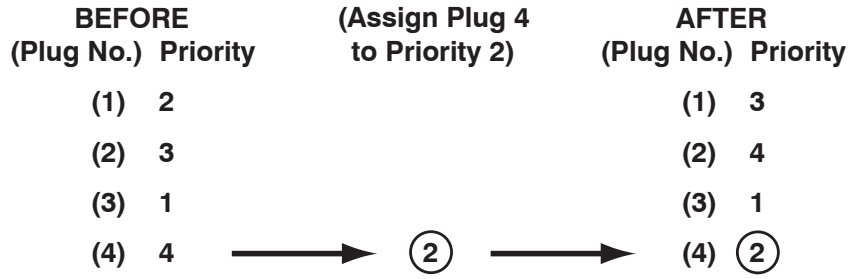

Figure 7.1: Boot Priority Example 1

7.9. Reboot Options

In addition to performing reboot cycles in response to commands, WTI Power Control products and WTI Console Server + Power Control Combo products can also be configured to automatically reboot outlets (or circuits) when an attached device does not respond to a Ping command (Ping-No-Answer Reboot) or according to a user defined schedule (Scheduled Reboot.)

> **Note:** *Power switching and reboot functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

- **Ping-No-Answer Reboot:** When the Ping-No-Answer feature is enabled, the WTI Device will Ping a user selected IP address at regular intervals. If the IP address fails to respond to the Ping command, the WTI Device will reboot one or more user selected outlet(s).
- **Scheduled Reboot:** A scheduled reboot is used to initiate a reboot cycle at a user selected time and day of the week. When properly configured and enabled, the WTI Device will reboot one or more outlets on a daily or weekly basis. The Scheduled Reboot feature can also be used to switch outlet(s) Off at a user selected time, and then back On again at a later, user selected time.

This section describes the procedure for configuring and enabling Ping-No-Answer Reboots and Scheduled Reboots.

7.9.1. Ping-No-Answer Reboot

A Ping-No-Answer Reboot can be used to reboot one or more outlets (or circuits) when an attached device does not respond to a Ping Command. When a device fails to respond to a ping, the Ping-No-Answer Reboot feature can also be configured to send an email, Syslog Message or SNMP Trap. Please refer to Section 7.10.5 for instructions on setting up email alarm notification for Ping-No-Answer reboots.

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

> **Note:** *In order for the Ping-No-Answer Reboot 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.*

7.9.1.1. Adding Ping-No-Answer Reboots

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

Note: *Power switching and reboot functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

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 WTI Power Control unit will reboot the selected outlets. **Note:** *In order to use domain names, DNS Server parameters must first be defined as described in Section 7.3.1.6.1.*
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 WTI Device will wait to send additional Ping commands, after a Ping-No-Answer Reboot has been initiated. Typically, this option is used to allow time for a device to fully "wake up" after a Ping-No-Answer Reboot before 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 Reboot.
Boot (Default = No)	Enables/Disables the Ping-No-Answer Reboot function for the specified IP address. When disabled, the WTI Device will not reboot the specified outlet(s) when a Ping-No-Answer event is detected. However, the WTI Device 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 as described in Section 7.10.5. **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 as described in Section 7.3.1.9.* • *In order for SNMP Trap Notification to function, you must first define SNMP parameters as described in Section 7.3.1.11.*

Parameter (Default)	Description
PNA Action (Default = Continuous Alarm/ Reboot)	Determines how the WTI Device will react when the IP address fails to respond to a ping: • **Continuous:** The WTI Device will continuously reboot the specified outlet(s) and send notification until the IP address responds and the Ping-No-Answer Reboot is cleared • **Single:** The WTI Device will reboot the specified outlet(s) and send notification only once each time the Ping-No-Answer Reboot is initially triggered.)
Select Plugs (Default = Undefined)	Determines which outlet(s) or circuit(s) will be rebooted when the IP address for this Ping-No-Answer operation does not respond to a Ping command.
Select Plug Groups (Defaults = Undefined)	Determines which Plug Group(s) the Ping-No-Answer Reboot for this IP Address will be applied to. **Note:** *Prior to setting this parameter, you must first define at least one Plug Group as described in Section 7.7.*

7.9.1.2. Viewing Ping-No-Answer Reboot Profiles

After you have defined one or more Ping-No-Answer Reboot 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.

7.9.1.3. Modifying Ping-No-Answer Reboot 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.

7.9.1.4. Deleting Ping-No-Answer Reboot 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.

7.9.2. Scheduled Reboot

The Scheduled Reboot feature can be used to reboot one or more outlets (or circuits) or automatically switch outlets/circuits Off or On according to a user defined schedule. In order to configure a Scheduled Reboot, you must access the user interface using a password that permits access to Administrator level commands.

> **Note:** *Power switching and reboot functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

7.9.2.1. Adding Scheduled Reboots

Up to 54 Scheduled Reboots to be defined. The Add Scheduled Reboot menu offers the following parameters:

Parameter (Default)	Description
Scheduled Reboot Name (Default = Undefined)	Assigns a name to this Scheduled Reboot.
Plug Action (Circuit Action) (Default = Turn Off)	Determines whether the Scheduled Reboot will result in the outlet(s) being switched Off, Switched On or cycled Off and then On again (Reboot.)
Time (Default = 12:00)	Determines the time of the day when this Scheduled Reboot will occur.
Select Days (Default = Undefined)	Provides access to a submenu used to determine which day(s) of the week this Scheduled Reboot will be performed.
Select Plugs (Select Circuits) (Default = Undefined)	Determines which outlet(s) or circuit(s) this Scheduled Reboot action will be applied to.
Select Plug Groups (Select Circuit Groups) (Default = Undefined)	Determines which Plug Group(s) or Circuit Group(s) this Scheduled Reboot action will be applied to.

7.9.2.2. Viewing Scheduled Reboot Actions

After you have defined one or more Scheduled Reboots, you can review the parameters selected for each Reboot using the View Scheduled Reboot feature. In order to view the configuration of an existing Scheduled Reboot, you must access the user interface using a password that allows Administrator level commands.

7.9.2.3. Modifying Scheduled Reboots

After you have defined a Scheduled Reboot, you can edit the configuration of the Reboot action using the Modify Scheduled Reboot feature. In order to modify the configuration of an existing Scheduled Reboot action, you must access the user interface using a password that allows Administrator level commands.

7.9.2.4. Deleting Scheduled Reboots

After you have defined one or more Scheduled Reboot actions, you can delete Reboot actions that are no longer needed using the Delete Scheduled Reboot feature. In order to delete an existing Scheduled Reboot, access the user interface using a password that allows Administrator level commands.

7.10. Alarm Configuration

When properly configured, the WTI Device 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 WTI Device can also notify support personnel via Email, Syslog Message or SNMP trap. In addition to the monitoring and notification capabilities provided by standard WTI Devices, models that include the Current Metering Option can also measure and record current, power and voltage conditions at each power outlet.

Notes:

- *In order to send alarm notification via email, email addresses and parameters must first be defined as described in Section 7.3.1.16. 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 7.3.1.9. 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 7.3.1.11. 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.*

7.10.1. The Over Current Alarms

The Over Current Alarms are designed to inform you when current consumption reaches or exceeds user-defined levels. Depending on the specific WTI Device model, units can have up to four Over Current Alarms (two sets of two alarms):

- The Over Current Line (Initial) Alarm
- The Over Current Line (Critical) Alarm

Notes:

- *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*
- *The Over Current Alarms monitor the load on each input line.*

The Initial alarm is used to provide notification when the level of current consumption reaches a point where you might want to investigate it, whereas the Critical alarms can provide notification when the level of current consumption approaches the maximum allowed level. The trigger levels for the Initial alarms are generally set lower than the trigger levels for the Critical alarms.

If the user-defined trigger levels for current load are exceeded, the WTI Device can automatically shut off power to non-essential devices ("Load Shedding") in order to decrease current load. After Load Shedding has taken place, the WTI Device can also restore power when current load drops to user-defined acceptable levels.

Notes:

- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

To configure the Over Current Alarms, access the user interface using a password that permits Administrator Level commands. The configuration menus for both Over Current Alarms offer essentially the same set of parameters, but the parameters defined for each alarm are separate. Therefore, parameters defined for a Critical Alarm will not be applied to an Initial Alarm and vice versa.

Both the Initial and Critical Threshold Current Alarm Configuration menus 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 Parameters include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all other alarms.*
Alarm Set Threshold (Defaults: Initial = 80%; Critical = 90%)	The trigger level for this alarm. When current load exceeds the Alarm Set Threshold, the WTI Device can send an alarm and/or begin load shedding (if enabled.) Note that the Alarm Set Threshold is entered as a percentage of maximum capacity and is applied to both Over Current Branch Alarm and Over Current Line Alarm (if present.)
Alarm Clear Threshold (Defaults: Initial Alarms = 70%; Critical Alarms = 80%)	Determines how low the current load must drop in order for the Alarm condition to be cancelled and for load shedding recovery (if enabled) to occur. The Alarm Clear Threshold is entered as a percentage of maximum capacity and is applied to both Over Current Branch Alarm and Over Current Line Alarm (if present.)
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device will wait to resend an email message generated by this alarm when the initial attempt was unsuccessful.

Parameter (Default)	Description
Notify Upon Clear (Default = On)	When enabled, the WTI Device will send additional notification when the situation that caused the alarm has been corrected.
Email Message	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 defined, then the text under the parameters will list the current, user selected email addresses.*
Subject (Defaults = "Alarm: Over Current (Initial)" or "Alarm: Over Current (Critical)")	Defines the text that will appear in the "Subject" field for all email notification messages generated by the alarm.
Facility (Default = 0)	Facility number used to generate Syslog Messages for Alarm Log Events.
Level (Default = Info)	Severity level used to generate Syslog Messages for Alarm Log Events.
Line Input	On WTI devices that include multiple branches and/or power inlets, this parameter indicates the selected input line, branch or fuse that will trigger the load shedding operation. Note that you can define a different load shedding operation for each input line, branch or fuse.
Load Shedding	Provides access to a submenu used to configure and enable the Load Shedding feature for the Over Current Alarm. For more information on the Load Shedding Feature and Auto Recovery, please refer to Section 7.10.1.1.

7.10.1.1. Over Current Alarms - Load Shedding and Auto Recovery

The Load Shedding feature is used to switch specific, user-defined outlets or circuits On or Off when current load exceeds the Alarm Set Threshold value. This allows the WTI Device to automatically shut Off plugs in order to reduce current load when the load approaches user-defined critical levels. When the Auto Recovery feature is enabled, the WTI Device can also automatically "undo" the effects of the Load Shedding feature when current load again falls to a user-defined non-critical level.

> **Note:** *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*

The Load Shedding Configuration Menus allow you to define the following parameters:

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables Load Shedding for the corresponding alarm. When enabled, the WTI Device will switch the user specified plugs whenever current load exceeds the Alarm Set Threshold value.
Plug State (Default = Off)	Determines whether the selected plugs/plug groups will be switched On or Off when Load Shedding is enabled and current load exceeds the user-defined Alarm Set Threshold.
Auto Recovery (Default = Off)	Enables/Disables the Auto Recovery feature for the selected branch or line. When both Load Shedding and Auto Recovery are enabled, the WTI Device will return plugs to their former On/Off state after current load falls below the Alarm Clear Threshold value.
Select Plugs (Default = Undefined)	Determines which Plug(s) will be switched when current load exceeds the Alarm Set Threshold and Load Shedding is triggered.
Select Plug Groups (Default = Undefined)	Determines which Plug Group(s) will be switched when the Load Shedding feature is triggered. **Note:** *Plug Groups must first be defined (as described in Section 7.7) before they will be displayed in the Load Shedding menu's Configure Plug Group Access submenu.*

7.10.2. 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:

- *Load Shedding and Auto Recovery Capabilities are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.11.*

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 WTI Device can send an alarm (if enabled) and/or begin Load Shedding (if enabled.) For more information on Load Shedding, please refer to Section 7.10.2.1. **Note:** *The Alarm Set Threshold value must be greater than the Alarm Clear Threshold value. The WTI Device 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. For more information on Load Shedding and Auto Recovery, please refer to Section 7.10.2.1. **Note:** *The System Parameters menu is used to set the temperature format for the WTI Device to either Fahrenheit or Celsius.*
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device 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 Device 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.
Load Shedding	Provides access to a submenu which is used to configure and enable the Load Shedding feature for the Over Temperature Alarm. For more information, please refer to Section 7.10.2.1. **Note:** *Load Shedding and Auto Recovery Capabilities are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

7.10.2.1. Over Temperature Alarms - Load Shedding and Auto Recovery

Note: *Load Shedding and Auto Recovery Capabilities are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*

The Load Shedding feature is used to switch specific, user-defined outlets On or Off when ambient rack temperature exceeds the Alarm Set Threshold value. This allows the WTI Device to automatically shut Off non-essential devices in order to reduce the temperature generated within the rack, or automatically switch On devices such as fans or cooling systems dissipate heat from the rack. When Auto Recovery is enabled, the WTI Device can also automatically "undo" the effects of the Load Shedding feature when the temperature again to a user-defined non-critical level.

The Load Shedding configuration menus for both the Over Temperature (Initial Threshold) alarm and the Over Temperature (Critical Threshold) alarm offer the following parameters:

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables Load Shedding for the corresponding alarm. When enabled, the WTI Device will switch the specified plugs whenever current load exceeds the Alarm Set Threshold value.
Plug State (Default = Off)	Determines whether the selected plugs/plug groups will be switched On or Off when Load Shedding is enabled and current load exceeds the user-defined Alarm Set Threshold.
Auto Recovery (Default = Off)	Enables/Disables the Auto Recovery feature for the selected branch or line. When both Load Shedding and Auto Recovery are enabled, the WTI Device will return plugs to their former On/Off state after current load falls below the Alarm Clear Threshold value.
Select Plugs **(Select Circuits)** (Default = Undefined)	Determines which Plug(s) or Circuit(s) will be switched when the temperature exceeds the Alarm Set Threshold and the Load Shedding feature is triggered.
Select Plug Groups **(Select Circuit Groups)** (Default = Undefined)	Determines which Plug Group(s) or Circuit Group(s) will be switched when the temperature exceeds the Alarm Set Threshold and the Load Shedding feature is triggered. **Note:** *Plug Groups must first be defined (as described in Section 7.7) before they will be displayed in the Configure Plug Group Access submenu.*

7.10.3. The Circuit Breaker Open Alarm

The Circuit Breaker Open Alarm can provide notification when a Circuit Breaker on the WTI Device is open. When an open circuit breaker is detected, the WTI Device can provide notification via Email, Syslog Message or SNMP Trap. The Circuit Breaker Open Alarm configuration menu offers the following parameters:

Note: *The Circuit Breaker Open alarm is only present on breakered WTI Devices.*

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 DSM 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 Device 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: Circuit Breaker Open")	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.

7.10.4. The Lost Communication Alarm

The Lost Communication with Unit Alarm is intended to provide notification when communication with the WTI Device is disrupted. When this alarm is triggered, the WTI Device can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for this alarm to provide notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for this alarm to provide notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for this alarm to provide notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10. and Section 7.3.1.11.*
- *In order for the Lost Communication Alarm to function, the Heartbeat parameter must be enabled at each serial port that you wish to monitor as described in Section 7.2.*
- *In order for the Lost Communication Alarm to function correctly, it may be necessary to update the software on your remote WTI equipment.*

To configure the Lost Communication Alarm, access the user interface using a password that permits Administrator Level commands. Enable the Heartbeat function and select "Any-to-Any" port mode at the desired Serial Port as described in Section 7.2. The Lost Communication 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 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 Device 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 Device 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.

Parameter (Default)	Description
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: Lost Comm with Unit")	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.

7.10.5. 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.

Note that the depending on the type of WTI Device, the Ping-No-Answer Alarm offers slightly different response options:

- **WTI Console Server Products:** When a target device fails to respond to a ping command, WTI Console Servers can automatically notify administrators via Email, Syslog Message or SNMP Trap.
- **WTI Power Control Products and WTI Console Server + Power Control Combos:** When a target device fails to respond to a ping command, these WTI Devices can automatically notify administrators via Email, Syslog Message or SNMP Trap and also switch user specified outlets or circuits On/Off.

Accordingly, the procedure for configuring the Ping-No-Answer Alarm also differs slightly for WTI Console Server Products and WTI Power Control Products as described in the sections that follow.

7.10.5.1. Ping-No-Answer Notification - Console Servers

When properly configured, WTI Console Server Products can provide notification when a device at a user-specified IP address fails to respond to a ping command. When one of the user-defined IP addresses fails to answer a Ping command, the WTI Console Server can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *For instructions regarding Ping-No-Answer Alarm configuration on WTI Power Control products and WTI Console Server + plus Power Control Combo products, please refer to Section 7.10.5.1.1 and Section 7.10.5.1.2.*
- *In order for the Ping-No-Answer Alarm 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.*
- *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined as described in Section 7.10.5.1.1.*
- *In order for the WTI Device to provide Email alarm notification, communication parameters must be defined as described in SSection 7.3.1.16.*
- *In order for the WTI Device to provide Syslog Message notification, Syslog parameters must be defined and Syslog Messages enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

7.10.5.1.1. Defining Ping No Answer IP Addresses - Console Servers

In order for the Ping No Answer Alarm to function, you must first define at least one target IP address. On WTI Console Server products, the Ping No Answer Configuration Menu offers options that allow you to either View, Modify or Delete previously defined Ping No Answer IP Addresses, or add new Ping No Answer Addresses.

After one or more Ping No Answer IP Addresses have been defined, the Ping No Answer Alarm function can be enabled and configured as described in Section 7.10.5.1.2. Up to 54 Ping No Answer IP Addresses can be defined. The Add Ping No Answer menu is used to define the following parameters for each new Ping No Answer IP Address:

Parameter (Default)	Description
IP Address or Domain Name (Default = Undefined)	The IP address or Domain Name for the target device. When the device at this address fails to respond to the Ping command, the Ping No Answer Alarm can provide user notification. **Notes:** • *In order to use Domain Names, you must first define DNS parameters as described in Section 7.3.1.6.1.* • *The target IP Address can be entered in either IPv4 format or IPv6 format.*
Protocol (Default = IPv4)	Allows definition of an IPv4 format IP or IPv6 format IP Address. If needed, both IPv4 and IPv6 addresses may be defined.
Ping Interval (Default = 60 Minutes)	Determines how often the Ping command will be sent to the IP Address. The Ping Interval can be 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 WTI Console Server will wait to send additional ping commands after the Ping No Answer Alarm has been triggered.
Consecutive Failures (Default = 5)	Determines how many consecutive failures of the Ping command must be detected in order to trigger the Alarm.
Boot (Default = No)	
PNA Action (Default = Continuous Alarm)	Determines how the Ping No Answer Alarm will react when triggered: • **Continuous Alarm -** The WTI Console Server will continue to generate new alarms until the Ping No Answer Alarm is cleared. • **Single Alarm -** The WTI Console Server will generate only one alarm. No additional alarms will be sent until a new Ping No Answer condition is detected.

7.10.5.1.2. Configuring the Ping No Answer Alarm - Console Servers

To configure the Ping-No-Answer Alarms on WTI Console Server products, access the user interface using a password that permits Administrator Level commands. The Ping-No-Answer 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:** • *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined as described in Section 7.10.5.1.1.* • *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 Device 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 Device 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.

7.10.5.2. Ping No Answer Alarm - WTI Power Control Products

Note: *This procedure applies only to WTI Power Control Products and WTI Console Server + Power Control Combo products.*

The Ping-No-Answer Alarm can provide notification when one of the IP addresses defined via the Ping No Answer Reboot feature fails to respond to a Ping command. If the Ping No Answer alarm is triggered, WTI Power Control Products and WTI Console Server + Power Control Combo products can provide notification via Email, Syslog Message or SNMP Trap and also automatically switch user specified plugs or circuits.

Notes:

- *For instructions regarding Ping-No-Answer Alarm configuration on WTI Console Server products, please refer to Section 7.10.5.1.*
- *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, IP Addresses for the Ping-No-Answer reboot feature must first be defined as described in Section 7.9.1.*
- *If you wish to use the Ping-No-Answer alarm without generating Ping-No-Answer reboots, make certain that the Boot parameter in the Ping-No-Answer Reboot menu is set to "No."*
- *When a Ping-No-Answer condition is detected, WTI Power Control products and WTI Console Server + Power Control Combo products can still reboot user-selected outlet(s), and can also send an email, Syslog Message and/or SNMP trap if configured as described in this section.*
- *In order for the WTI Device to provide Email alarm notification, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device 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 7.3.1.10 and Section 7.3.1.11.*

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 as described in Section 7.9.1.* • *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.

7.10.6. The Serial Port Invalid Access Lockout Alarm

The Serial Port Invalid Access Lockout Alarm can provide notification when the WTI Device 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:

- *The Serial Port Invalid Access Lockout Alarm is only intended to provide notification when the Invalid Access Lockout feature has locked the serial ports. To apply the Invalid Access Lockout feature to the Network Port, please refer to Section 7.1.3.*
- *In order for this alarm to function, target ports must be set to "Any-to-Any" mode and Invalid Access Lockout parameters for the desired serial port(s) must be configured and enabled.*
- *The WTI Device can also be configured to count Invalid Access attempts at the serial ports, and provide notification when the counter exceeds a 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 WTI Device to provide Email alarm notification, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device 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 7.3.1.10 and Section 7.3.1.11.*

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 WTI Device 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 WTI Device 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.

7.10.7. The Power Cycle Alarm

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

Notes:

- *The Power Cycle Alarm is only present on WTI Devices that include only one power inlet.*
- *To provide notification when only one power input line is lost or disconnected on WTI Devices that include two or more power inlets, please use the Lost Voltage (Line In) Alarm as described in Section 7.10.11.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

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.

7.10.8. The Alarm Input Alarm

The Alarm Input Alarm can be used to monitor dry contacts that have been connected to the Alarm Inputs on the RPC-40L8A4's back panel. Typically, the Alarm Input Alarm is used to detect open doors and other situations where a dry contact has been opened or closed.

> **Note:** *The Alarm Input Alarm is only available on RPC-40L8A4 Series products. The Alarm Input Alarm is not available on RPC-4850 Series units.*

To configure the Alarm Input Alarm, you must first connect a dry contact relay to the alarm inputs on the RPC-40L8A4 back panel and then access the RPC-40L8A4 user interface 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.*
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device 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 WTI Device 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 7.3.1.16,) 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.
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.
Alarm Input Parameters	Provides access to a submenu that is used to Enable/Disable the alarm at each Alarm Input as described in Section 7.10.8.1.

7.10.8.1. The Alarm Input Alarm - Alarm Input Parameters

This submenu is used to Enable/Disable the alarm at each Alarm Input, name the Alarm Inputs, set trigger levels for each Alarm Input and also provides access to another submenu that is used to select load shedding parameters for each Alarm Input.

Notes:

- *The Alarm Input Alarm is only available on RPC-40L8A4 Series products. The Alarm Input Alarm is not available on RPC-4850 Series units.*
- *The Alarm Input Alarm must be enabled in order to access the Alarm Input Parameters submenu.*

The Alarm Input Parameters submenu offers the following configuration options:

Parameter (Default)	Description
Name (Default = Undefined)	Assigns a descriptive name for each Alarm Input.
Enable (Default = Off)	Enables/Disables each Input Alarm.
Level (Default = Open)	Defines the trigger level for each Alarm Input as either Open or Closed. For example, if the Level is set to “Open” and the Alarm Input Alarm is properly configured, an alarm will be generated when the dry contact relay connected to the corresponding Alarm Input is Opened.
Load Shedding	Provides access to a series of submenus which allow the Alarm Input Alarm to automatically shut off user specified circuits or circuit groups when an Alarm is generated, as described in Section 7.10.8.2. **Note:** *There is a separate Load Shedding configuration menu for each Alarm Input.*

7.10.8.2. The Alarm Input Alarm - Load Shedding

Allows the Alarm Input Alarm to automatically shut off user specified circuits or circuit groups when an Alarm is generated. Note that different Load Shedding parameters can be assigned to each Alarm Input.

Note: *The Alarm Input Alarm is only available on RPC-40L8A4 Series products. The Alarm Input Alarm is not available on RPC-4850 Series units.*

Parameter (Default)	Description
Enable (Default = Off)	Enables/Disables Load Shedding for the corresponding Alarm Input.
Circuit State (Default = Off)	Determines whether the selected Circuits / Circuit Groups will be Opened or Closed when Load Shedding is enabled and the Alarm Input Alarm is triggered.
Auto Recovery (Default = Disable)	Enables/Disables the Auto Recovery feature for the selected circuit. When both Load Shedding and Auto Recovery are enabled, the WTI Device will return circuits to their former Open/Closed state after the Alarm Input Alarm is cleared.
Configure Circuit Access (Default = Undefined)	Determines which Circuit(s) will be Opened/Closed when the Alarm Input Alarm is triggered by this Circuit.
Configure Circuit Group Access (Default = Undefined)	Determines which Circuit Group(s) will be Opened/Closed when the Alarm Input Alarm is triggered by this Circuit. **Note:** *Circuit Groups must first be defined (as described in Section 7.7) before they will be displayed in the Configure Circuit Group Access submenu.*

7.10.9. The Buffer Threshold Alarm

The Buffer Threshold Alarm can provide notification when the amount of data stored in the buffer for a given serial port exceeds the Buffer Threshold Value. When the Buffer Threshold Alarm is triggered, the WTI Device can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *The Buffer Threshold Alarm is not present on WTI Power Control Products.*
- *In order for the Buffer Threshold Alarm to function, you must define the Buffer Threshold value for each desired serial port as described in Section 7.2.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.11.*
- *If the Buffer Threshold Alarm is not enabled, the WTI Device can still send SNMP Traps to notify you when the amount of accumulated data at a buffer mode port exceeds the Buffer Threshold value, providing that SNMP Trap Parameters have been defined as described in Section 7.3.1.11.*

To configure the Buffer Threshold Alarm, access the user interface using a password that permits Administrator Level commands, then set the Port Mode for the desired Serial Port to Buffer Mode and define the Buffer Threshold value for the port as described in Section 7.2.

The Buffer Threshold 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 WTI Device 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 Device 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 7.3.1.16) 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: Buffer Threshold")	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.

7.10.10. The Plug Current Alarm

The Plug Current Alarm allows you to monitor current consumption at each of the switched outlets and generate an alarm when current exceeds the "High" threshold or falls below the "Low" threshold. The Plug Current Alarm can also be applied to user-defined Plug Groups or Circuit Groups in order to generate an alarm when total current consumption for the given Plug Group or Circuit Group rises too high or falls too low.

> **Note:** *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*

The Plug Current Alarm can also be configured to automatically shut off individual plugs or circuits or user-defined Plug Groups or circuit groups, whenever current consumption rises above a user-defined threshold value.

The Plug Current 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.*
Plug Hysteresis (Default = 0.5 Amps)	This parameter can be used to prevent the Plug Current Alarm from generating excessive "Alarm" and "Clear" messages when current consumption fluctuates back and forth across the trigger value. The Plug Hysteresis parameter allows you to define a margin at both the Low Threshold and High Threshold that the current level must cross in order to clear an alarm.
Plug "Off" Low Alarm (Default = On)	Allows you to configure the "Low" current alarm to suppress triggering when an outlet is purposely switched Off. **Notes:** • *The Plug "Off" Low Alarm feature will also be applied to Plug Groups.* • *When the Plug "Off" Low Alarm feature is enabled, the WTI Device will always generate a Low current alarm when current drops below the Low threshold value, even when the current drop was caused by one or more outlets in the Plug Group being purposely switched Off.* • *When the Plug "Off" Low Alarm feature is disabled, the WTI Device will not generate a Low current Alarm when a current drop is caused by all outlets in the Plug Group being purposely switched Off.*
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device will wait to resend an email message generated by this alarm, when the initial attempt was unsuccessful.

Parameter (Default)	Description
Notify Upon Clear (Default = On)	When enabled, the WTI Device 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 7.3.1.16) 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: Plug Current")	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.
Plug Thresholds	Provides access to a submenu used to define current consumption level(s) that will trigger alarm(s) at each switched outlet as described in Section 7.10.10.1.
Plug Group Thresholds	Provides access to a submenu used to Define current consumption level(s) that will trigger alarm(s) for each Plug Group as described in Section 7.10.10.2.
Plug Shedding	Provides access to a submenu used to configure the Plug Current Alarm to automatically switch plugs Off or On when current consumption at the target plug rises above or falls below the user-defined Plug High Threshold value as described in Section 7.10.10.3.
Plug Group Shedding	Provides access to a submenu used to configure the Plug Current Alarm to automatically switch Plug Groups Off or On when current consumption by the target Plug Group rises above the user-defined Plug Group High Threshold as described in Section 7.10.10.4. **Note:** *In order to enable Plug Group Shedding, you must first set the high Plug Group Threshold for each desired Plug Group.*

7.10.10.1. The Plug Current Alarm - Plug Thresholds

The Plug Current Alarm's Plug Thresholds submenu is used to define current consumption levels that will trigger alarms at each switched outlet. Plug Thresholds can be set to trigger an alarm when current consumption rises above a user-defined High value and/or when current consumption falls below a user-defined Low value.

> **Note:** *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*

The Plug Current Alarm's Plug Thresholds submenu allows the following parameters to be defined:

Parameter (Default)	Description
Plug	The fixed alphanumeric tag assigned to each switched outlet.
Name	The user-defined descriptive name that has been assigned to each switched outlet.
Amps	The current reading detected at each switched outlet.
High (Default = Off)	Enables/disables and defines the high end current threshold (in Amps) that will trigger a Plug Current Alarm.
Low (Default = Off)	Enables/disables and defines the low end current threshold (in Amps) that will trigger a Plug Current Alarm.

7.10.10.2. The Plug Current Alarm - Plug Group Thresholds

The Plug Current Alarm's Plug Group Thresholds submenu is used to define current consumptions levels that will trigger an alarm for each user-defined plug group. Plug Group Thresholds can be configured to trigger an alarm when total current consumption for a Plug Group rises above a user-defined High value and/or when current consumption falls below a user-defined Low value.

Notes:

- *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*
- *In order to define Plug Group Thresholds, you must first define at least one Plug Group as described in Section 7.7.*

The Plug Current Alarm's Plug Group Thresholds submenu allows the following parameters to be defined:

Parameter (Default)	Description
Group Name	The user-defined descriptive name that has been assigned to each user-defined Plug Group.
Amps	The current consumption reading in Amps, for each user-defined Plug Group.
High (Default = Off)	Enables/disables and defines the high end current threshold (in Amps) that will trigger a Plug Current Alarm for each Plug Group.
Low (Default = Off)	Enables/disables and defines the low end current threshold (in Amps) that will trigger a Plug Current Alarm for each Plug Group.

7.10.10.3. The Plug Current Alarm - Plug Shedding

Plug Shedding is used to switch user-specified outlets On or Off when current load at a switched outlet rises above the user-defined Plug Threshold value. This allows the WTI Device to automatically shut Off plugs in order to reduce current load when the load approaches user-defined critical levels.

Notes:

- *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*
- *In order to enable Plug Shedding, you must first set the Plug Threshold values for each desired plug.*

The Plug Current Alarm's Plug Shedding submenu allows the following parameters to be defined:

Parameter (Default)	Description
Plug	The fixed alphanumeric tag assigned to each switched outlet.
Name	The user-defined descriptive name that has been assigned to each switched outlet.
Amps	The current reading detected at each switched outlet.
High	The high end current threshold (in Amps) that has been defined via the Plug Threshold submenu as described in Section 7.10.10.1.
Action (Default = Leave On)	Selects the switching action that will be performed at each plug when current consumption levels exceed the high-end threshold value that has been defined via the Plug Threshold submenu.

7.10.10.4. The Plug Current Alarm - Plug Group Shedding

Plug Group Shedding is used to switch Plug Groups On or Off when current load at a given Plug Group rises above the user-defined Plug Group Threshold value. This allows the WTI Device to automatically shut Off Plug Groups in order to reduce current load when the load approaches user-defined critical levels.

Notes:

- *Current and Power Monitoring features are only available on WTI Devices that include the Current Monitoring option.*
- *In order to enable Plug Group Shedding, you must first set the Plug Group Threshold values for each desired Plug Group as described in Section 7.10.10.2.*

The Plug Current Alarm's Plug Group Shedding submenu allows the following parameters to be defined:

Parameter (Default)	Description
Group Name	The user-defined descriptive name that has been assigned to each user-defined Plug Group.
Amps	The current consumption reading in Amps, for each user-defined Plug Group.
High	The high end current threshold (in Amps) that has been defined via the Plug Group Threshold submenu as described in Section 7.10.10.2.
Action (Default = Leave On)	Selects the switching action that will be performed at each Plug Group when current consumption levels exceed the user-defined high-end threshold value established via the Plug Group Threshold submenu.

7.10.11. The Lost Voltage (Line In) Alarm

The Lost Voltage (Line Input) Alarm can provide notification when power to one of the available power inlets is interrupted.

Notes:

- *The Lost Voltage (Line In) Alarm is not available on units that include two or more power inlets.*
- *This alarm will not function if all input power to the unit is lost. To provide notification when all input power is lost and restored, please use the Power Cycle Alarm as described in Section 7.10.7.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

To configure the Lost Voltage (Line Input) Alarm, access the user interface using a password that permits Administrator Level commands. The Lost Voltage (Line In) 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 WTI Device 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 Device 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.
Subject (Default = "Alarm: Lost Voltage")	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.

7.10.12. The Emergency Shutoff Alarm

The Emergency Shutoff Alarm can provide notification when the Emergency Shutoff feature is activated.

Notes:

- *The Emergency Shutoff Alarm is only available on WTI Power Control products and WTI Console Server + Power Control Combo products.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

To configure the Emergency Shutoff Alarm, you must access the user interface using a password that permits Administrator Level commands. The Lost Voltage 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 WTI Device 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 Device 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: Emergency Shutoff")	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.

7.10.13. The No Dialtone Alarm

The No Dialtone Alarm allows the WTI Device to monitor a telephone line connected to an external modem installed at the WTI Device'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 WTI Device 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 as described in Section 7.2.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

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 WTI Device 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 Device 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.

7.10.14. The Wakeup On Failure Alarm

The Wakeup On Failure menu provides notification when the unit has recovered from a failure to communicate via cellular and the Wakeup On Failure function has been triggered. For more information regarding the Wakeup on Failure feature, please refer to the WTI.com Knowledge Base.

Notes:

- *The Wakeup On Failure Alarm is only available on WTI Devices that include the Cellular Modem Option.*
- *In order for this alarm to function, Wakeup On Failure parameters must first be defined as described in Section 7.4.1.9.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

The Wakeup On Failure 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 WTI Device 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 Device 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 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 specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Wakeup On Failure")	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.

7.10.15. The IP Passthrough Data Usage Alarm

The IP Passthrough Data Usage Alarm allows the WTI Device to monitor data being used for IP Passthrough cellular communication and provide notification when data usage rises above a user-defined Usage Threshold value. When the WTI device is being used in IP Passthrough mode as a secondary/backup WAN connection, a sudden rise in IP Passthrough Data Usage is a reliable indication that primary WAN communication may be down. This alarm alerts support personnel that troubleshooting the primary WAN communication may be necessary.

Notes:

- *The IP Passthrough Data Usage Alarm is only available on WTI Devices that include the Cellular Modem Option.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must first be defined.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

The IP Passthrough Data Usage 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.*
Usage Threshold (Default = 100 KBytes)	Defines the trigger level for this alarm. IP Passthrough Data Usage must rise above the Usage Threshold value for defined Time Period in order to generate an alarm.
Time Period (Default = 2 Minutes)	Defines the amount of time that IP Passthrough Data Usage must remain above the defined Usage Threshold in order to generate an alarm.
Idle Time to Clear (5 Minutes)	Defines the amount of time that IP Passthrough Data Usage must remain below the defined Usage Threshold in order to clear a previously generated alarm.
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device 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 Device 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 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 specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: IP Passthrough Data Usage")	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.

7.10.16. The Buffer Filtering Alarm

The Buffer Filtering Alarm can monitor data as it is received at a Buffer Mode port and provide notification when specific text strings are detected. Typically, this alarm is used to notify support personnel when error messages and other text strings are detected in buffered data.

Notes:

- *When the Buffer Filtering Alarm is triggered, the alarm will not be cleared until the Buffer Filtering String is cleared from buffer memory.*
- *The Buffer Filtering Alarm is only available on WTI Devices that include Serial or USB Console ports.*
- *In order for this alarm to function, Buffer Filtering String(s) must first be defined as described in Section 7.2.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must be defined, and SNMP Traps must be enabled as described in Section 7.3.1.11.*

The Buffer Filtering 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, 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 Device 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 Device 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 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 specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: Buffer Filtering")	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.

7.10.17. The No Cellular PPP Connection Alarm

The No Cellular PPP Connection Alarm is used to provide notification when a cellular connection to the WTI Device is not available. This helps to detect loss of cellular communication with the WTI device, and allows support personnel to restore the cellular connection to ensure that cellular Out-of-Band access to the WTI Device is available when needed.

Notes:

- *The No Cellular PPP Connection Alarm is only available on WTI Devices that include the Cellular Modem Option.*
- *In order for the WTI Device to provide alarm notification via Email, communication parameters must be defined as described in Section 7.3.1.16.*
- *In order for the WTI Device to provide alarm notification via Syslog Message, Syslog parameters must be defined and Syslog Messages must be enabled as described in Section 7.3.1.9.*
- *In order for the WTI Device to provide alarm notification via SNMP Trap, SNMP parameters must be defined, and SNMP Traps must be enabled as described in Section 7.3.1.10 and Section 7.3.1.11.*

The No Cellular PPP Connection 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, 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.*
Time Period (Default = 7 Days)	Determines how often the WTI Device will check its cellular connection. If the check detects a problem with the cellular connection, an alarm will be generated..
Resend Delay (Default = 60 Minutes)	Determines how long the WTI Device 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 Device 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 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 specified, then the text under the parameters will list the current, user defined email addresses.*
Subject (Default = "Alarm: No Cellular PPP Connection")	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.

7.11. Download Unit Configuration

Once the WTI Device 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 WTI Devices, allowing rapid set-up when several identical units will be configured with similar parameters.

The WTI Device'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 WTI Device 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.*

7.11.1. Restoring Saved Configuration Parameters

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

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 WTI Device parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the XML file to the WTI Device. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the WTI Device 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 WTI Device 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.

7.12. 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 WTI Devices 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 7.3.1.11.
Syslog Test	Sends a test Syslog Message to the Syslog Manager that was defined as described in Section 7.3.1.9.
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 primary Ethernet Port (eth0,) the optional secondary Ethernet Port (eth1,) or via the optional cell modem.

8. The Cellular Modem Option

This section provides a basic overview of the procedure for installing and setting up WTI's Cellular Modem option on WTI Devices.

Notes:

- *The Cellular Modem Option is only available on DSM Series, CPM Series and REM Series products.*
- *It is recommended to use the Command Line Interface (CLI) when setting up the Cellular Modem Option.*

8.1. Installation

In order to communicate with your WTI Device via the Cellular Modem Option, you will first need to purchase a cellular plan. When choosing a cellular plan, WTI recommends that the plan should provide the following:

- A Static IP Address
- A VPN (Virtual Private Network)

Note: *For further information regarding Cellular Carrier options, please refer to the WTI.com Knowledge Base.*

8.1.1. Attaching the Cellular Antennae

Attach the two Cellular Antennae (included with the unit,) to the two threaded connectors on the WTI Device's face plate.

8.1.2. Installing the SIM Card

Once you have purchased a cellular plan, the next step is to install the SIM card, (provided with your cellular plan,) in your WTI Device. To install the SIM card, proceed as follows:

Note: *Prior to installing the SIM Card, make certain that your WTI Device is powered Off.*

1. Remove the SIM Card cover panel on the left hand side of the WTI unit, located adjacent to the cellular antenna. Note that the panel is held in place by a small Phillips Head screw.
2. Carefully slide the SIM card into the SIM Card Slot with the keyed/notched corner of the card facing towards the unit's faceplate (see diagram on cover plate.) Make certain the SIM Card is firmly seated, but do not apply excess pressure that might damage the card.
3. Replace the panel that covers the SIM Card Slot, reinstall the retaining screw and restore power to the WTI Device.

8.1.3. Configuring the SIM Card

After installing the SIM Card, use the **`/cell`** command to configure the SIM Card as described below:

1. Access the Command Line Interface (CLI) for the WTI Device as described in Section 3.3.
2. When the command prompt appears, type **`/cell`** and press **[Enter]** to display the Cell Modem Statistics menu.
3. At the Cell Modem Statistics menu, select "APN, Carrier."
4. At the Access Point Name configuration menu, use the Access Point Name (APN) option to key in the APN, (supplied with your cellular plan,) and press **[Enter]**. Then use the MTSMC-L4N1 Carrier option to select the service provider (carrier) that the WTI Device will use. The Cellular Modem Option will be automatically configured, based on the information on the SIM Card.
5. The configuration procedure will require several minutes. When configuration is complete, Cell Modem Statistics menu be redisplayed, indicating that configuration was successful.

8.2 Defining the Static Route

After the SIM Card has been installed and configured, the next step is to define the Static Route.

> **Note:** *The Static Route is only required if the Cell Modem Port is not defined as the default gateway.*

8.2.1. Defining Static Route when Default Gateway Address is Known

If you already know the default gateway address for your cellular network, then proceed as follows. If you don't know the default gateway address, please proceed to Section 8.2.2.

1. Type **`/p modem`** and press **[Enter]** to display the Cell Modem Parameters menu.
2. When the Cell Modem Parameters menu is displayed, select Static Route to display the Static Route submenu. When the Static Route submenu is displayed, key in a number for the first vacant Static Route definition line and press **[Enter]**.
3. Define the Static Route using the following format:

   `route add GGG.GGG.GGG.GGG gw CCC.CCC.CCC.CCC`

   Where:
   `GGG.GGG.GGG.GGG` is the default Gateway Address
   `CCC.CCC.CCC.CCC` is the IP Address for the Cell Modem.
4. Press **[Esc]** once to exit the Static Route menu, then press **[Esc]** again to exit the Cell Modem Parameters menu and save the newly defined Static Route. Note that it may require several minutes for the Cell Modem to save newly defined parameters.
5. Perform the verification procedure described in Section 8.4 to make certain that cellular access has been properly enabled.

8.2.2. Defining Static Route when Default Gateway Address is Unknown

If you don't know the default gateway address used by the cellular network, then you will need to use the WTI Device's **`/bash`** command to display the default gateway address as described below:

1. If you are communicating via local network and do not require the default gateway address, log into the WTI Device via serial port, USB or network (if your network is on the same network and doesn't require the default gateway.)

2. **Temporarily Disable Default Gateway for the Network Port:** When the command prompt appears, type **`/N`** and press **[Enter]** to display the Network Parameters menu.

   a) At the Network Parameters menu, select Gateway Address. The Gateway Address submenu will be displayed. Record the currently defined Gateway Address.

   Note: *Make certain to write down or save the currently defined Gateway Address; you will need this address later, when you re-enable the Default Gateway at the Network port after Static Route definition is complete.*

   b) At the Gateway Address submenu, press the **[Space]** bar and then press **[Enter]**. This will delete the currently defined Gateway Address, disabling the Default Gateway at the Network Port.

   c) Press **[Esc]** twice to exit the Network Parameters menu and save changed parameters.

3. **Enable the Default Gateway for the Cell Modem Port:** At the Command Line Interface (CLI) command prompt, type **`/p modem`** and then press **[Enter]** to display the Cell Modem Parameters menu.

   a) When the Cell Modem Parameters menu is displayed, select Default Gateway. Use the resulting menu to enable the Default Gateway for the Cell Modem Port.

   b) Press **[Esc]** twice to exit the Default Gateway menu and save newly defined parameters.

   Note: *It may require several minutes for the Cell Modem to save the newly defined Default Gateway status.*

4. **Display the IP Address for the Cell Modem Port:**

   a) At the WTI Device's command prompt, type **`/cell`** and press **[Enter]** to display the Cell Modem Statistics menu.

   b) When the Cell Modem Statistics menu is displayed, write down the IP Address for the Cell Modem Port (listed under the Cell Connection Information heading.)

   c) Press **[Esc]** to exit from the Cell Modem Statistics menu.

5. Establish an SSH connection to the WTI Device via the cellular network.

6. **Display the Gateway Address:** At the WTI Device's command prompt, type **`/bash netstat -nat`** and press **[Enter]** to display the Active Internet Connections screen. Note that it may take several minutes for the unit to respond.

   a) The Cell Modem Port IP Address with be displayed in the "Foreign Address" column.

   b) The "State" column for the Cell Modem Port IP address will read "Established."

   c) Note the Gateway Address (Local Address,) that corresponds with the Cell Modem Port IP address (Foreign Address.)

   d) To exit from the Active Internet Connections menu, press **[Enter]**.

7. **Define the Static Route:** At the WTI Device's command prompt, type **`/p modem`** and press **[Enter]** to display the Cell Modem Parameters menu.

   a) When the Cell Modem Parameters menu is displayed, select Static Route to access the Static Route submenu. When the Static Route submenu is displayed, key in a number for the first vacant Static Route definition line and press **[Enter]**.

   b) At the Static Route menu, refer to the Cell Modem Port Address (Foreign Address) and Gateway Address (Local Address) that were determined above. Enter a route command using the following format:

      `route add GGG.GGG.GGG.GGG gw CCC.CCC.CCC.CCC`

      Where:

      `GGG.GGG.GGG.GGG` is the Gateway Address (Local Address)
      `CCC.CCC.CCC.CCC` is the Cell Modem Address (Foreign Address)

   c) Press **[Enter]** to select the newly defined Static Route, then press **[Esc]** twice to save the Static Route definition and exit the Static Route menu. Note that it will require several minutes for newly defined parameters to be saved.

   d) For more information, please refer to the following example.

Static Route Definition Example:

Assume that the address for the Cell Modem Port address (Foreign Address) is **CCC.CCC.CCC.CCC** and the netstat function returns the Active Internet Connections screen shown in Figure 8.***1***. In this example, the Gateway Address (Local Address) would be **GGG.GGG.GGG.GGG**. Therefore, the static route would be defined as follows:

`route add GGG.GGG.GGG.GGG gw CCC.CCC.CCC.CCC`

8. **Disable the Default Gateway for the Cell Modem Port:**

   a) At the WTI Device's command prompt, type **`/p modem`** and press **[Enter]** to display the Cell Modem Parameters menu.

   b) When the Cell Modem Parameters menu is displayed, access the Default Gateway submenu and disable the Default Gateway for the Cell Modem Port.

   c) Press **[Esc]** twice to exit from the Cell Modem Parameters and save the newly defined Default Gateway Status.

   Note: *It may require several minutes for the Cell Modem to save the newly defined parameters.*

9. **Re-Enable the Default Gateway for the Network Port:** When the command prompt appears, type **`/N`** and press **[Enter]** to display the Network Parameters menu.

   a) At the Network Parameters menu, select Gateway Address. The Gateway Address submenu will be displayed.

   b) At the Gateway Address submenu, key in the previous Gateway Address that you saved in Step 2 at the beginning of this section and then press **[Enter]**.

   c) Press **[Esc]** twice to exit the Network Parameters menu and save changed parameters.

   Note: *It may require several minutes for the Cell Modem to save the newly defined parameters.*

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 GGG.GGG.GGG.GGG:22      CCC.CCC.CCC.CCC:2892    ESTABLISHED
tcp        0      0 :::22                   :::*                    LISTEN
```

Figure 8.1: Static Route Definition Example

8.3. Enable Web Access

If you need to allow access to the WTI Device's Web Browser Interface via cellular, you must First enable Web Services via the Command Line Interface (CLI) Cell Modem Parameters menu.

1. At the CLI command prompt, type **`/p modem`** and press **[Enter]** to display the Cell Modem Parameters menu.
2. When the Cell Modem Parameters menu appears, use the Web Access option to enable Web Access.
3. Press **[Esc]** twice to exit from the Cell Modem Parameters menu and save the newly defined Web Services status.

   Note: *It may require several minutes for the Cell Modem to save the newly defined Web Services status.*

8.4. Verify that Cellular Access is Available

After setting up Cellular Access, it is recommended to perform this procedure to verify that the procedure was completed successfully.

1. If you are still connected to the WTI Device interface, type **`/x`** and press **[Enter]** to disconnect from the unit.

2. **Verify Cellular Access to Command Line Interface (CLI):**

   a) Create an SSH connection to the WTI Device via cell. When the login prompt is displayed, enter your username and password. When the command prompt appears, type **`/cell`** and press **[Enter]**.

   b) If the Cell Modem Statistics screen appears, this indicates that cellular network access has been successfully enabled.

   c) If the Cell Modem Statistics screen fails to appear after several minutes, this probably means that there is an error in the definition of the Static Route. In this case, use the procedure described in Section 8.2 to display the Static Route definition. Carefully check the Static Route definition to make sure that the IP addresses were entered correctly and that there are no syntax errors.

3. **Verify Cellular Access to Web Browser Interface:**

   a) Start your Web Browser, key the Cell Modem Port IP Address for the WTI Device into the browser's address bar. When the login prompt is displayed, key in your username and password.

   b) If the WTI Device's home page is displayed, this means that cellular access to the WTI Device has been successfully enabled.

   c) If the WTI Device's home page is not displayed, this probably means that either Web Access has not been enabled or there is an error in the Static Route definition.

      i. **Web Access Not Enabled:** Make certain that web access has been enabled as described in Section 8.3.

      ii. **Static Route Error:** Use the procedure described in Section 8.2 to display the Static Route definition. Carefully check the Static Route definition to make sure that the IP address were entered correctly and that there are no syntax errors.

8.5. Setting Up the Firewall/IP Tables (Optional)

If you wish to restrict access to the WTI Device unit via cellular, you must define a firewall. The IP Tables menu is used to define a firewall which determines which IP addresses will be allowed to access the WTI Device and which IP addresses will be denied. To define the firewall, proceed as follows:

1. In the Web Browser Interface, click on Network Configuration link on the left hand side of the screen, and then select either eth0 [IPv4] or eth0 [IPv6].
2. When the Network Configuration menu is displayed, select the IP Tables option.
3. When the IP Tables menu is displayed, use Linux syntax 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.

This completes the set-up procedure for the WTI Cellular Modem Option. For further information, please refer to the remainder of this User's Guide.

9. 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 WTI Device, without the need to go to an outside service. The principal disadvantage of Self Signed certificates, is that when you access the WTI Device 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 WTI Device 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 WTI Device 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.

9.1. 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 WTI Device, make certain to define all of the following parameters. Although most SSL/TLS applications require only the Common Name, in the case of the WTI Device 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 WTI Device. 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 WTI Device will be located (e.g., California.)
- **7. Locality:** The city or town where the WTI Device will be located (e.g., Irvine.)
- **8. Country Code:** The two character country code for the nation where the WTI Device will be located (e.g., US.)
- **9. Email Address:** An email address, that can be used to contact the person responsible for the WTI Device (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 WTI Device will prompt you to create a password. Key in the desired password and then press **[Enter]**. When the WTI Device prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the WTI Device 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 WTI Device via the Web Interface, using an HTTPS connection.

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

   b) The WTI Device 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.

9.2. 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 12.1 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 WTI Device 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 WTI Device:** After the signed certificate is returned from the certificate authority, return to the Web Access menu.

   a) Access the WTI Device 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 WTI Device. 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 WTI Device 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.

9.3. Downloading the Server Private Key

When configuring the WTI Device'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 WTI Device, make certain that SSL/TLS parameters have been defined as described in Section 9.1, 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 WTI Device, 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 WTI Device. 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.

9.4. 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.

9.5. 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.

10. Saving and Restoring Configuration Parameters

Once the WTI Device 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 WTI Devices, 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 WTI Device via the CLI.*

10.1. Sending Parameters to a File

10.1.1. 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 WTI Device will prompt you to select a file transfer protocol. Key in the number for the desired protocol, and press **[Enter]**.
   b) The WTI Device 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 WTI Device’s Save Parameter File menu, and press **[Enter]** to proceed. WTI Device parameters will be saved on your hard drive in the file specified in Step 2 above.
   4. The WTI Device 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.

10.1.2. Downloading & Saving Parameters via Web Browser Interface

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

Notes:

- *Although WTI Device 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.

10.2. Restoring Downloaded Parameters

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

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

1. Start your terminal emulation program and access the WTI Device'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 WTI Device parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the WTI Device. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the WTI Device 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 WTI Device 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.

10.3. Restoring Recently Saved Parameters

If you make a mistake while configuring the WTI Device, and wish to return to the previously saved parameters, the CLI's "Reboot System" command (/I) offers the option to reinitialize the WTI Device 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 WTI Device will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved WTI Device 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 (Section 3.3.)
2. At the command prompt, type `/I` and press **[Enter]**. The WTI Device 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 WTI Device will reboot and previously saved parameters will be restored.

11. 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 WTI Devices.

> **Note:** *When upgrading software on WTI Power Control products or WTI Console Server + Power Control Combo products, power outlets will not be switched On or Off during the upgrade process. For more information, please refer to the WTI.com Knowledge Base.*

11.1. WMU Enterprise Management Software (Recommended)

The WMU Enterprise Management Software provides the preferred method for updating WTI Devices. The WMU software allows you to manage software updates for multiple WTI Devices 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 WTI Device must be at least v6.23 or higher. When upgrading older WTI Devices that feature pre v6.23 software, it is recommended to use the WTI Software Upgrade Utility.

11.2. The Firmware Upgrade Function (Web Browser Interface)

The Firmware Upgrade function provides a method for updating the WTI Device 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 WTI device, 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 WTI Device 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 WTI Device while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

11.3. The Upgrade Software Function (Command Line Interface)

The Upgrade Software function provides an alternative method for updating the WTI Device 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 WTI Device 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 WTI Device's operating software.

   Note that after any of the above options is selected, the WTI Device 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 WTI Device 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 WTI Device, using an account and port that permit access to Administrator Level commands.

6. Transfer the md5 format upgrade file to the WTI Device.

7. After the file transfer is complete, the WTI Device 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 WTI Device will send a message to all currently connected network sessions, indicating that the WTI Device is going down for a reboot.

   Note: *Do not power down the WTI Device 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 WTI Device via the Network Port, in order to start the FTP/SFTP servers, the WTI Device 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 WTI Device using your former IP address.

   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the WTI Device'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.

12. The Command Line Interface (Scripting)

In addition to the Web Browser Interface and WMU Enterprise Management Software, the WTI Device 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 WTI Device, 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.

12.1. 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 WTI Device 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 WTI Device 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 WTI Device 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:** Cellular communication with the WTI Device is only available when the Cellular Modem Option is present.
- **Access via Local PC:** Your PC must be connected to the WTI Device's Serial SetUp Port, the SetUp Port must be configured for Any-to-Any Mode, (default port Mode for the SetUp Port,) and your PC must include a communications program (Such as Tera Term or PuTTY.) Serial Port 1 is designated as a Set Up Port, and by default, is configured for communication with a local control device. Some WTI Devices also include a USB Mini format SetUp Port. For instructions regarding configuration of the USB Mini SetUp Port, please refer to Section 7.3.1.1.

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

Notes:

- *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.*
- *Some WTI Devices include an optional, secondary Ethernet Port in addition to the primary Ethernet port in order to allow connection to both a primary and secondary network.*

1. Contact the WTI Device:

   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 WTI Device 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 WTI Device's 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 WTI Device's IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Dial-Up Modem:** If the WTI Device includes the optional external modem or if you have installed a modem at one of the 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 WTI Device includes the Cellular Modem Option, and the cellular modem has been set up as described in Section 8, 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.

12.2. Command Conventions

Most CLI commands described conform to the following conventions:

- **Power Control Functions:** WTI Console Server products do not support power control functions. Power reboot and switching functions are only available on WTI Power Control products and WTI Console Server + Power Control Combo products.
- **Serial Port Management Functions:** WTI Power Control products do not support serial port management functions. Comprehensive serial port connection and buffering functions are only available on WTI Console Server products and WTI Console Server + Power Control Combo products.
- **Apply Command to All Ports:** When an asterisk is entered as the argument of the **/D** (Disconnect) or **/E** commands (Erase Buffer) the command will be applied to all available ports. For example, to erase all serial port buffers, type **/E * [Enter]**.
- **Apply Command to All Plugs:** (DSM and CPM Series products only) When an asterisk is entered as the argument of the **/ON** (Switch Plugs On), **/OFF** (Switch Plugs Off) or **/BOOT** (Reboot Plugs) commands, the command will be applied to all available plugs. For example, to reboot all allowed plugs, type **/BOOT * [Enter]**.
- **Command Queues:** (WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) If a switching or reboot command is directed to a plug that is already being switched by a previous command, then the new command will be placed into a queue until the plug is ready to receive additional commands.
- **"Busy" Plugs:** (DSM and CPM Series products only) If the "Status" column in the Plug Status Screen includes an asterisk, this means that the plug is currently busy, and is in the process of completing a previously issued command. If a new command is issued to a busy plug, then the new command will placed into a queue to be executed later.
- **Plug Name Wild Card:** (WTI Power Control Products and WTI Console Server + Power Control Combo Products only) It is not always necessary to enter the entire plug name. Plug names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (*****). For example, a plug named "SERVER" can be specified as "**S***". (Note however, that this command would also be applied to any other plug name that begins with an "S".)
- **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 reboot Plug 4 without displaying the Sure prompt, type **/BOOT 4,Y [Enter]**.
- **Connected Ports:** When two ports are connected, most WTI Device commands will not be recognized by either of the connected ports. The only exception is the Resident Disconnect Sequence (Default = **^X** (**[Ctrl]** plus **[X]**).)

12.3. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Port and Plug Status❶	`/S` **[Enter]**	X❷	X❷	X❷	X❷
Port Diagnostics	`/SD` **[Enter]**	X❷	X❷	X❷	X❷
Port Diagnostics (USB Console)	`/SDU` **[Enter]**	X❷	X❷	X❷	X❷
Port Parameters (Who)	`/W [n]` **[Enter]**	X❷	X❷	X❷	X❷
Plug Group Status❶	`/SG` **[Enter]**	X❷	X❷	X❷	X❷
Network Status	`/SN` **[Enter]**	X	X	X	X
Network Configuration Summary	`/RN` **[Enter]**	X	X	X	X
IP Alias Status	`/SA` **[Enter]**	X	X	X❷	X❷
Alarm Status	`/AS [alarm]` **[Enter]**	X			
Current Metering❾	`/M` **[Enter]**	X	X	X⓾	X⓾
View Connection (with Echo)	`/V <n>` **[Enter]**	X	X		
View Connection (without Echo)	`/VE <n>` **[Enter]**	X	X		
Help Menu	`/H` **[Enter]**	X	X	X	X
Log Functions	`/L` **[Enter]**	X	X		
Site ID / Unit Information	`/J [*]` **[Enter]**	X	X	X	X
Cellular Modem Status	`/CELL` **[Enter]**	X			
Control					
Exit CLI	/X [Enter]	X	X	X	X
Connect - Local <Remote>	`/C <n> [n]` **[Enter]**	X	X	X❹	
Disconnect Ports	`/D <n|Nn|*>` **[Enter]**	X	X		
Read Buffer	`/R <n>` **[Enter]**	X	X	X	
Erase Buffer(s)	`/E <n|*>` **[Enter]**	X	X	X	
Boot Plug *n* ❶	`/BOOT <n>[,Y]` **[Enter]**❺	X	X	X	
Turn Plug *n* On ❶	`/ON <n>[,Y]` **[Enter]**❺	X	X	X	
Turn Plug *n* Off ❶	`/OFF <n>[,Y]` **[Enter]**❺	X	X	X	
Default All Plugs ❶	`/DPL[,Y]` **[Enter]**❺	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	
Broadcast Mode	`/broadcast <port list>` **[Enter]**	X	X		
Test Network Configuration	`/TEST` **[Enter]**	X			
Configuration					
System Parameters	`/F` **[Enter]**	X	❼		
Serial Port Parameters	`/P` **[Enter]**	X	❼		
Plug Parameters ❶	`/PL <n>` **[Enter]**	X	❼		
Plug Group Parameters ❶	`/G` **[Enter]**	X	❼		
Network Configuration - Eth0/IPv4	`/N` **[Enter]**	X	❼		
Network Selection Menu - IPv4/IPv6	`/N*` **[Enter]**	X	❼		
Ping No Answer Configuration ❽	`/PNA` **[Enter]**	X	❼		
Reboot Options ❶	`/RB` **[Enter]**	X	❼		
Alarm Configuration	`/AC` **[Enter]**	X	❼		
Reboot System	`/I` **[Enter]**	X	X		
Upgrade Software	`/UFW` **[Enter]**	X			
Copy Port Parameters	`/CP <z>` **[Enter]**	X			
VPN Configuration	`/VPN` **[Enter]**	X			

❶ Power control functions are only available on WTI Power Control Products and WTI Console Server + Power Control Combo Products.

❷ In Administrator and SuperUser mode, all ports/plugs/plug groups are displayed. In User and ViewOnly mode, the screen will only display ports/plugs/plug groups allowed by the account. WTI Console Server Products do not include switched plugs.

❸ User and ViewOnly level accounts are only allowed to view parameters for the port that was used to access the user interface.

❹ User level accounts are only allowed to create a connection to Serial Ports permitted by the account. User level accounts are not allowed to create Third Party (remote) port connections.

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

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.

❽ Not Available on WTI Power Control products and WTI Console Server + Power Control Combos; Ping No Answer parameters are defined via the Reboot Options Menu.

❾ Current and Power Metering capabilities are only available on WTI Devices that include the Current Metering Option.

⓾ The User Directory can disable access to Current and Power Metering functions for User and View Level accounts.

12.4. Command Set

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

12.4.1. Display Commands

/S Display Port (and Plug) Status Screen

Displays the Port and Plug Status Screen, which lists the current status of the WTI Device's serial ports and switched outlets.

Notes:

- *WTI Power Control products and WTI Console Server + Power Control Combo products will also display plug (outlet) status. Power control and power status functions are not available on WTI Console Server products.*
- *RPC Series units will display Circuit Status, rather than Plug Status.*
- *In Administrator Mode and SuperUser Mode, all WTI Device ports and outlets are displayed. In User Mode and ViewOnly Mode, the Port and Plug Status Screen will only include the ports and plugs allowed by the account.*

Availability: Administrator, SuperUser, User, ViewOnly

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

/SD Display Port Diagnostics

(Console Server products and Console Server + Power Control Combo products only.) Provides detailed information regarding the status of each serial port. When issued by a User level or View Only level account, the resulting screen will only display parameters for the ports allowed by the account.

Availability: Administrator, SuperUser, User, ViewOnly

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

Response: Displays Port Diagnostics Screen.

/SDU Display Port Diagnostics

(WTI Devices with USB Console Port only.) Provides detailed information regarding the status of each USB Console port. When issued by a User level or View Only level account, the resulting screen will only display parameters for the USB Console Ports allowed by the account. If a 4-Port USB Hub has been connected to the USB Port(s), then the ports on the hub connected to port U1 will be listed as U1.1, U1.2, U1.3 and U1.4 and the ports on the hub connected to port U2 will be listed as U2.1, U2.2, U2.3 and U2.4.

Availability: Administrator, SuperUser, User, ViewOnly

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

Response: Displays Port Diagnostics Screen.

/W Display Port Parameters (Who)

(Console Server products and Console Server + Power Control Combo products only.) Displays configuration information for an individual port, but does not allow parameters to be changed. User and ViewOnly accounts can only display parameters for their resident port.

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 Plug Group Status Screen

(Power Control products and Console Server + Power Control Combo products only.) Displays the Plug Group Status Screen, which lists and briefly describes all user-defined Plug Groups.

> **Note:** *In Administrator Mode all user defined Plug Groups are displayed. In SuperUser Mode, User Mode and ViewOnly Mode, the Plug Group Status Screen will only include the Plug 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 WTI Device's 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 names, alias IP addresses and Direct Connect status for the WTI Device's serial ports.

> **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]**

/V View Connection (with Echo)

When two WTI Device ports are connected, the /V command can be used to display data sent between the two connected serial ports, including data that has been echoed.

Notes:

- *To display data sent between two connected serial ports without including echoed data, please refer to the /VE command.*
- *To terminate the View Connection function, type* **^x** *(**[Ctrl]** + **[X].**)*

Availability: Administrator, SuperUser

Format: **/V <n> [Enter]**

Where **n** is the number of one of the two connected serial ports.

/VE View Connection (without Echo)

When two WTI Device ports are connected, the /VE command can be used to display data that is sent between the two connected serial ports, but will not include data that has been echoed.

Notes:

- *To display data sent between two connected serial ports, including echoed data, please refer to the /V command.*
- *To terminate the View Connection function, type* **^x** *(**[Ctrl]** + **[X]**.)*

Availability: Administrator, SuperUser

Format: **/VE <n> [Enter]**

Where **n** is the number of one of the two connected serial ports.

/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 the most available WTI Device 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, Temperature Log (WTI Console Server Products only,) Current Metering Log (WTI Devices that include the Current Metering Option only) and Power Metering Log (WTI Devices that include the Current Metering Option only.) For more information on Log Functions, please refer to Section 4.8.

Availability: Administrator, SuperUser

Format: **/L [Enter]**

/M Current Metering (WTI Devices with Current Metering Option Only)

Displays the Current Metering Screen, which lists Current, Power, Voltage and Temperature readings as well as settings for the Current and Temperature alarms.

Notes:

- *Current Metering functions are not available on WTI Console Server Products.*
- *If desired, the User Directory can disable access to Current and Power Metering functions for User and View Only level accounts.*

Availability: Administrator, SuperUser, User, View Only

Format: `/M` **[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 Current (Initial)	OCI
Over Current (Critical)	OCC
Over Temperature (Initial)	OTI
Over Temperature (Critical)	OTC
Circuit Breaker Open	CBO
Lost Communication with Unit	CL
Ping No Answer	PNA
Serial Port Invalid Access Lockout	LO
Power Cycle (Cold Boot)	CB
Alarm Input Alarm	AI
Buffer Threshold	BT
Plug Current	PC
Lost Voltage (Line In)	VL
No Dialtone	ND
Emergency Shutoff	ES
Wakeup On Failure	WOF
IP Passthrough Data Usage	IPDU
Buffer Filtering	BF
No Cellular PPP Connection	NP

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 WTI Device.

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 WTI Device.

/CELL Cellular Modem Statistics

(WTI Devices with Cellular Modem Option Only) Displays data regarding the Cell Modem, including the model, make, cell network carrier and other information. Displays currently defined Cell Modem Configuration parameters and indicates whether or not a PPP session has been established. Also includes prompts for defining Cell Modem Parameters, including the Access Point Name, Public IP Address and Wakeup On Failure function. .

> **Note:** *SuperUsers are allowed to view cell modem settings, but are not allowed to change cell modem configuration parameters.*

Availability: Administrator, SuperUser

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

12.4.2. 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

(DSM, CPM and REM Series Only) Establishes a bidirectional connection between two ports. For more information, see Section 5.1.1. There are two types of connections:

- **Resident Connect:** If the /C command specifies only one port, your resident port will be connected to the specified port.
- **Third Party Connect:** If the /C command specifies two ports, the unit will connect the two ports indicated. Third Party Connections can only be initiated by ports and accounts that permit Administrator level commands.

Notes:

- *User level accounts can only connect to the ports that are specifically permitted by the account.*
- *User level accounts are not allowed to create "Third Party" connections. For example, a User level account, that is logged in via the Network Port cannot connect Serial Port 3 to Port 4.*
- *Administrator and SuperUser level accounts are allowed to connect to any WTI Device Serial Port.*
- *The Serial Ports are not allowed to create a Third Party connection to the Network Port. For example, Serial Port 1 cannot connect Serial Port 3 to the Network Port.*
- *If the WTI Device includes USB Console Ports, then those ports are addressed as U1 and U2.*
- *If a 4-Port USB Hub has been connected to USB Port U1 and/or USB Port U2, then the ports on the hub connected to U1 will be addressed as U1.1, U1.2, U1.3 and U1.4 and the ports on the hub connected to U2 will be addressed as U2.1, U2.2, U2.3 and U2.4.*

Availability: Administrator, SuperUser, User

Format: `/C <x> [x]` **[Enter]**

Where `x` is the number or name of the port(s) to be connected.

/D Third Party Disconnect

(CPM Series and DSM Series products only.) Invoke the /D command at your resident port to disconnect two other ports.

Notes:

- *The /D command cannot disconnect your resident port*
- *SuperUsers and Users are limited to the ports specifically allowed by the account.*

Availability: Administrator, SuperUser

Format: **`/D[/Y] <x> [x]`** **[Enter]**

Where:

`/Y`	(Optional) suppresses the "Sure?" prompt.
`x`	Is the number or name of the port(s) to be disconnected. To disconnect all allowed ports, enter an asterisk. To disconnect, enter the "Nn" format Network Port Number.

Example: To disconnect Port 2 from Port 3 without the "Sure?" prompt, access the CLI from a third port with Administrator level command capability and type:

`/D/Y 2` **[Enter]** or **`/D/Y 3`** **[Enter]**

/R Read Buffer

(CPM Series and DSM Series products only.) Reads from Buffer Mode ports as described in Section 7.2.1.3.

Notes:

- *SuperUsers and Users are limited to the ports that are specifically allowed by their accounts*
- *When the /R command is invoked, the counter for the SNMP Traps function will also be reset.*

Availability: Administrator, SuperUser, User

Format: **`/R <n>`** **[Enter]**

Where **`n`** is the number or name of the port buffer to be read.

/E Erase Buffer

(CPM Series and DSM Series products only.) Erases data from the buffer for specified Buffer Mode port(s).

Notes:

- *Users accounts are limited to the ports that are specifically allowed by the account definition.*
- *Erased data cannot be recovered.*

Availability: Administrator, SuperUser, User

Format: **`/E[/Y] <x> [x]`** **[Enter]**

Where:

`x`	Is the number or name of the port buffer(s) to be cleared. To erase buffers for all ports, enter an asterisk.
`/Y`	(Optional) Suppresses the “SURE? (Y/N)” prompt.

Example: To clear the buffer for Port 3, access the CLI using an account that provides access to Port 3, and then type **`/E 3`** **[Enter]**.

/BOOT Initiate Boot Cycle

(WTI Power Control Products and WTI Console Server + Power Control Combo Products only.) Initiates a boot cycle at the selected plug(s) or Plug Group(s). When a Boot cycle is performed, the unit will first switch the selected plug(s) Off, then pause for the Boot/Sequence Delay Period, then switch the plug(s) back on. The /BOOT command can also be entered as /BO.

Notes:

- *On RPC Series DC Power Control products, the /BOOT command applies to Circuits and Circuit Groups.*
- *When the /BOOT command is used to reboot more than one plug, the Boot/Sequence Delay Periods will be applied as described in Section 7.8.*
- *When invoked in Administrator Mode or SuperUser Mode, the command can be applied to all plugs and Plug Groups on the unit. When invoked in User Mode, the command will only be applied to the plugs and/or Plug Groups allowed by the account.*

Availability: Administrator, SuperUser, User
Format: `/BOOT <n>[,Y]` **[Enter]** or `/BO <n>` **[Enter]**
Where:

`n`	The number or name of the plug(s) or Plug Group(s) that you intend to boot. To apply the command to several plugs, enter a plus sign (`+`) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (`:`). To apply the command to all plugs allowed by your account, enter an asterisk character (`*`).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example: Assume that your account allows access to Plug 2 and Plug 3. To initiate a boot cycle at Plugs 2 and 3, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/BOOT 2+3,Y` **[Enter]** or `/BO 2+3,Y` **[Enter]**

/ON Switch Plug(s) ON

Switches selected plugs(s) or Plug Group(s) On.

Notes:

- *On RPC Series DC Power Control products, this command applies to Circuits and Circuit Groups.*
- *This command is not available on WTI Console Server Products.*
- *When the /ON command is used to switch more than one plug, the Boot/Sequence Delay Periods will be applied as described in Section 7.8.*
- *When invoked in Administrator Mode or SuperUser Mode, the command can be applied to all plugs and Plug Groups on the unit. When invoked in User Mode, the command can only be applied to Plugs and/or Plug Groups allowed by the account.*

Availability: Administrator, SuperUser, User

Format: `/ON <n>[,Y]` **[Enter]**

Where:

`n`	The number or name of the plug(s) or Plug Group(s) you intend to Switch On. To apply the command to several plugs, enter a plus sign (`+`) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (`:`). To apply the command to all plugs allowed by your account, enter an asterisk character (`*`).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example: Assume that your account allows access to Plug 2 and Plug 3. To switch Plugs 2 and 3 On, without displaying the optional command confirmation prompt, invoke following command line:

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

/OFF Switch Plug(s) OFF

Switches selected plugs(s) or Plug Group(s) Off. When used to switch more than one plug, the Boot/Sequence Delay Period will be applied as described in Section 7.8. The /OFF command can also be entered as /OF.

Note:

- *On RPC Series DC Power Control products, this command applies to Circuits and Circuit Groups.*
- *This command is not available on WTI Console Server Products.*
- *When invoked in Administrator Mode or SuperUser Mode, this command can be applied to all plugs and Plug Groups on the unit. When invoked in User Mode, the command will only be applied to the plugs and/or Plug Groups allowed by the account.*

Availability: Administrator, SuperUser, User

Format: **`/OFF <n>[,Y]`** **[Enter]** or **`/OF <n>[,Y]`** **[Enter]**

Where:

`n`	The number or name of the plug(s) or Plug Group(s) you intend to Switch Off. To apply the command to several plugs, enter a plus sign (**+**) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (**:**). To apply the command to all plugs allowed by your account, enter an asterisk character (*****).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Examples: Assume that your account allows access to Plug 2 and Plug 3. To switch Plugs 2 and 3 on your WTI Device Off, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/OFF 2+3,Y` **[Enter]** or **`/OF 2+3,Y`** **[Enter]**

/DPL Set All Plugs to Default States

Sets all switched outlets to their user-defined default state. For information on setting outlet defaults, please refer to Section 7.8.

Notes:

- *On RPC Series DC Power Control products, this command applies to Circuits and Circuit Groups.*
- *This command is not available on WTI Console Server Products.*
- *When invoked in Administrator Mode and SuperUser Mode, this command will be applied to all outlets on the unit. When invoked in User Mode, the command will only be applied to the plugs allowed by the account.*

Availability: Administrator, SuperUser, User

Format: **`/DPL[,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 10.1.1. 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 WTI Device 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 7.5. In addition, Telnet Access and Outbound Access must also be enabled via the Network Configuration menu, as described in Section 7.3.1.1.*
- *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 7.5. In addition, SSH Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 7.3.1.1.*
- *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.

/BROADCAST Broadcast Text or Commands to Serial Ports

(DSM Series and CPM Series products only.) Broadcasts text or commands to a user-specified selection of Serial Ports.

Notes:

- *The Broadcast command will only be applied to Serial Ports that are configured for Any-to-Any Mode or Passive Mode. Text or commands will not be broadcast to Modem Mode or Buffer Mode ports.*
- *The Broadcast command will only be applied to Serial Ports that are not currently connected. Text or commands will not be broadcast to connected Serial Ports.*
- *Flow control (handshake) at target Serial Ports must be "ready" in order to receive text or commands.*
- *The Broadcast command will not send text or commands to the Serial Port that initiated the command.*
- *To exit Broadcast mode and send text or commands, press [Esc] or type ^X ([Ctrl] plus [X].)*

Availability: Administrator, SuperUser

Format: **/BROADCAST <port list> [Enter]**

Where "**port list**" is a series of port numbers or names, separated by spaces or commas. Note that the "**port list**" argument can also include wild cards.

12.4.3. Configuration Commands

/F System Parameters

Displays a menu used to define general system parameters for the WTI Device. 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 WTI Device.
Real Time Clock (Default = Undefined)	Provides access to a submenu which is used to set and configure the Real Time Clock as described in Section 7.1.2.
Invalid Access Lockout (Default = Off)	Provides access to a submenu which is used to set up the Invalid Access Lockout function as described in Section 7.1.3.
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 7.1.4.
Front Panel Buttons (Default = On)	Enables/disables control functions for the front panel buttons.
Analog Modem Phone No. (Default = Undefined)	If the WTI Device includes the optional internal dial-up modem, this parameter can be used to record the phone number. When the WTI Device 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 7.1.5.
Power Configuration (Default = Undefined)	(WTI Products with Current Metering Option Only) Provides access to a submenu which is used to calibrate voltage readings and define the Power Factor parameter and Power Efficiency parameter. For more information on Power Configuration, please refer to Section 7.1.1.1.
Asset Tag (Default = Undefined)	Allows a descriptive tag or tracking number to be assigned to the WTI Device. 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 WTI Device 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 Port Configuration (RJ45 and USB Ports)

Displays a menu used to select parameters for the RJ45 serial console ports, USB Console Ports (if present,) and internal modem port.

Notes:

- *On WTI Console Server products, the Serial Port Parameters menus are used to configure all available serial ports, including the serial Setup Port.*
- *On WTI Power Control products, the Serial Port Parameters menus are only used to configure the serial setup port.*
- *To configure an RJ45 Serial Console Port, type* **`/P <n>`** *and press* ***[Enter]****. (Where* **`<n>`** *is the number or name of the desired port.)*
- *To configure an USB Console Port, type* **`/P U<n>`** *and press* ***[Enter].*** *(Where* **`<n>`** *is the number of the desired USB Console Port.)*
- *To configure the internal modem port, type* **`/P modem`** *and press* ***[Enter]****, or type* **`/P <n>`** *and press* ***[Enter]****. (Where* **`<n>`** *is the port number for the modem.)*

The Serial Port Parameters menu offers the following configuration options:

Parameter (Default)	Description
Communication Settings	
Baud Rate (Defaults; Serial Ports 1 to 8 = 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.

Parameter (Default)	Description
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 CLI 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.
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 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.

Parameter (Default)	Description
Port Mode Parameters	
Port Name (Defaults; Serial Ports 1 and above = Undefined; Internal Modem Port = MODEM)	Assigns a descriptive name to the Port.
Port Mode (Defaults; Serial Port 1 = Any-to-Any Mode; Serial Ports 2 and above = Passive, Internal Modem Port = Modem Mode)	The operation mode for this port; Any-to-Any Mode, Passive Mode, Buffer Mode, Modem Mode or Modem PPP Mode. For more information, please refer to Section 7.2.1. **Notes:** • *Passive Mode and Buffer Mode are not available at Serial Port 1 (the Setup Port.)* • *The Port Mode for the Internal Modem Port (if present) can only be set to Modem Mode.* • *On units that include the Cellular Modem Option, the Port Mode for the Cellular Modem Port will always be Modem PPP. In this case, Modem PPP parameters are not defined by the user and are instead determined when a connection to the network is established.* • *Only one Port on the WTI Device may be configured for Modem PPP Mode at a given time.*
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.
Buffer Parameters	(Buffer Mode Ports Only) Provides access to a submenu which is used to define the parameters described in the "Buffer Mode Parameters" section of this table.
Any-to-Any Mode and Passive Mode Port Parameters	
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.
Heartbeat (Default = Off)	(Any-to-Any Mode Ports Only) The Heartbeat parameter can be used in conjunction with the Lost Communication alarm to provide notification when a WTI Device that has been attached to one of the serial ports ceases to function. Normally, the WTI Device will send the Heartbeat message to an attached WTI Device at regular intervals; if the attached device fails to respond to the Heartbeat message, the WTI Device can then notify you via email, Syslog Message or SNMP Trap as described in Section 7.10.4. **Notes:** • *The Heartbeat function will only work if the port is configured for Any-to-Any mode. In order to employ the Lost Communication Alarm, all target ports must be configured for Any-to-Any mode.* • *The Heartbeat feature is only available when the serial port has been configured for "Any-to-Any" mode.*

Parameter (Default)	Description
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 WTI Device 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 7.10.13.
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 WTI Device 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 WTI Device 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 7.3.1.6.1.* • *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 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.
Internal Cell Modem Port Parameters	
Default Gateway (Default = Off)	(Internal Cell Modem Port Only) Enables/disables the Default Gateway for IPv4 communication. **Note:** *The status of the Default Gateway parameter cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
User Peer DNS **(Default = Off)**	(Internal Cell Modem Port Only) When enabled, internet connections will use your carrier's DNS rather than the standard DNS.
Static Route (Default = Undefined)	(Internal Cell Modem Port Only) Allows definition of Linux routing commands that will be automatically executed each time a user accesses the user interface via this Ethernet Port.
DDNS Services (Default = Undefined)	(Internal Cell Modem Port Only) This option is used to define DDNS parameters. For more information, please refer to Section 7.3.1.6.
Modem Stay Alive (Default = Off)	(Internal Cell Modem Port Only) When enabled, the internal cellular modem will not time out due to inactivity. **Note:** *This parameter is only available via the CLI.*
LCP Echo	(Internal Cell Modem Port Only) Sets the values for the LCP Echo Interval and LCP Echo Failure functions.
Protocol (Default = IPv4)	(Internal Cell Modem Port Only) Selects communication via IPv4, IPv6 or both.
MTU/MRU (Default = 552)	(Internal Cell Modem Port Only) Maximum Receive Unit and Maximum Transmit Unit. Will Send/Receive data packets of no more than n bytes through the cellular network.
Web Access (Default = Off)	(Internal Cell Modem Port Only) Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access.

Parameter (Default)	Description
Internal Cell Modem Port Parameters (continued)	
SNMP Access (Default = Off)	(Internal Cell Modem Port Only) Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the primary Ethernet Port (eth0.) For more information, please refer to Section 7.3.1.10. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
PING Access (Default = Allow All Pings)	((Internal Cell Modem Port Only) Configures the WTI Device's response to ping commands at the Cellular Modem Port. **Note:** *Disabling Ping Access at the Modem Port will not effect the operation of the Ping-No-Access Alarm.*
Buffer Mode Port Parameters	
Time/Date Stamp (Default = On)	(Buffer Mode Ports Only) Enables/disables the Time/Date stamp for buffered data at this port. When enabled, the WTI Device will add a time/date stamp whenever five seconds elapse between data items received.
Buffer Connect (Default = Off)	(Buffer Mode Ports Only) When enabled, the WTI Device will continue to Buffer captured data while you are connected to this Buffer Mode port.
Buffer Data To Syslog (Default = Off)	(Buffer Mode Ports Only) The Syslog feature is used to create records of each buffer event. As event records are created, they are sent to a Syslog Daemon, at an IP address defined via the Network Parameters menu. For more information, please refer to Appendix E. The Syslog feature offers three possible settings: • **Off:** Syslog disabled. • **On - Not Connected:** Messages will only be generated when a user is not connected to a buffer port. This prevents information captured from the attached device from being put into Syslog messages while a user is connected to a buffer port. • **On - Always:** All captured information will be sent out via Syslog message; whether a user is connected or not.
Buffer Threshold (Default = Off/0)	(Buffer Mode Only) When the Port Mode is set to Buffer, this parameter enables/disables the Buffer Threshold function and sets the level that will generate traps and/or Buffer Threshold Alarms at this port. If set to "0" (zero), then SNMP Traps are disabled at this port. When a Buffer Threshold value is defined, this also allows the Buffer Threshold Alarm to be employed. **Note:** *This option is not available to Serial Port 1. This is because Port 1 is reserved as a SetUp Port, and cannot be configured as a Buffer Mode Port.*

Parameter (Default)	Description
Buffer Filter String 1 (Default = Undefined)	(Buffer Mode Only) This parameter is used to define one of two available text filters that can be used in conjunction with the Buffer Filtering Alarm to provide notification when user specified text strings are found in data that is received at a Buffer Mode port. These parameters are typically used to detect error messages and alerts in data received from attached devices.
Buffer Filter String 2 (Default = Undefined)	(Buffer Mode Only) This parameter is used to define the second of two available text filters that can be used in conjunction with the Buffer Filtering Alarm to provide notification when user specified text strings are found in data that is received at a Buffer Mode port. These parameters are typically used to detect error messages and alerts in data received from attached devices.
Network Services	
Direct Connect (Default = Off)	(Console Products Only) Allows users to access the WTI Device and automatically create a connection between the Network Port and a specific serial port by including the appropriate port number in the connect command. For more information, please refer to Appendix D.3. • **Off:** The Direct Connect feature will be disabled at this port. • **On - No Password:** Users will be able to employ the Direct Connect feature to connect to this port without entering a password. • **On - Password:** Users will be able to employ Direct Connect to connect to this port, but will be required to enter a password before the connection is established. • **Off - Break On Raw Disconnect:** Port will send a break character when a Raw Socket connection with the port is terminated. Note that this feature will work with both the "No Password" and "Password" options. When Direct Connect is enabled, the menu will also list the following: • **Telnet Port:** The Telnet port number employed to create a Direct Connection to this port via standard Telnet protocol. • **SSH Port:** The port number used to create a Direct Connection to this port via SSH protocol. • **Raw Port:** The port number used to create a Direct Connection to this port via Raw Socket protocol. **Notes:** • *If "On - Password" is selected, and Administrator level commands are disabled at the Network Port, then only accounts that do not permit Administrator level commands will be allowed to establish a direct connection via the Network Port. If Administrator level commands are disabled at a given port, then that port will not allow access by accounts that permit Administrator level commands.* • *When Direct Connect is enabled, the Serial Port Configuration Menu will also list the port numbers for Telnet, SSH and Raw connections.*

Parameter (Default)	Description
Network Services (continued)	
IP Alias Address (Default = Undefined)	(Console Products Only) Assigns an IP address of your choice to the serial port. When an IP address is assigned to the serial port, this essentially allows users to create a direct connection to the serial port without first entering a password. **Notes:** • *If the WTI Device includes the optional Secondary Ethernet Port (eth1,) then separate IP aliases can be defined for each Ethernet Port.* • *The IP Alias feature is only available when the Direct Connect feature is set to "On - Password" or "On - No Password."* • *To display the IP Alias status via the Web Browser Interface, use the Alias Status Screen as described in Section 4.3.*

Availability: Administrator

Format: **`/P <n>`** **[Enter]**

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

- **Configure Modem Port:** If the unit includes an internal modem, type **`/P modem`** to configure the modem port.
- **Configure USB Console Port:** If the unit includes USB Console Ports, type **`/P U<x>`** to configure the USB Ports (Where **`x`** is the number of the desired USB Port.)

/PL Plug Parameters

Displays a menu used to select parameters for the switched plugs. All functions provided by the /PL command are also available via the Web Browser Interface. For more information, please refer to Section 7.8.

Notes:

- *This command is not available on WTI Console Server products*
- *On RPC Series DC Power Control products, this command applies to Circuits rather than plugs/outlets.*

In the CLI, all plug parameters are defined via a single menu. There are four parameters available for each plug/circuit; and parameters are grouped according to each plug or circuit's alphanumeric name. The Plug Parameters menu offers the following configuration options:

Parameter (Default)	Description
Line Input Name (Default = Undefined)	When the WTI Device includes more than one power inlet, this item can be used to assign a descriptive name to each input.
Plug Name (Circuit Name) (Default = Undefined)	This item can be used to assign a descriptive name to each switched outlet.

Parameter (Default)	Description
Boot/Seq. Delay (Default = 0.5 Second)	When multiple outlets (or circuits) are switched, the Boot / Sequence delay determines how much time will elapse between each switching action. When the Boot/Sequence Delay is applied, the WTI Device will wait for the user-defined delay period before switching On the next plug. When Reboot cycles and switching actions are initiated, the Boot/Sequence Delay will be applied as follows: • **Reboot Cycle Delay:** During a reboot cycle, the WTI Device will first switch all selected plugs "Off" (with a 0.5 second pause between each "Off" operation), and then begin to switch selected plugs back On, pausing for the user-defined Boot/Sequence Delay before switching On the next plug. • **"On" Sequence Delay:** When two or more plugs are switched On, the WTI Device will pause for the user-defined Boot/ Sequence Delay before switching On the next plug.
Power Up Default (Default = On)	Determines how this plug will react after power has been interrupted and then restored, or when the "Default All Plugs" command (/DPL) is invoked. When power is restored, or the Default Command is invoked, the WTI Device will switch each outlet On or Off as specified by the Power-Up Default value. **Notes:** • *If the Default command is invoked by an account that has Administrator or SuperUser level command access, then all switched outlets will be set according to the Power Up Default.* • *If the Default command is invoked by an account that has User level command access, then only the outlets allowed by the account will be set to the Power Up Default.* • *The Default command is not available to ViewOnly level accounts.*
Boot Priority (Default = All plugs prioritized according to Plug Number)	When commands are applied to two or more outlets (or circuits,) the Boot Priority parameter determines the order in which the plugs will be switched On. The outlet that has been assigned a Boot Priority value of "1" will be switched on first, followed by the outlet that has been assigned the Boot Priority value of "2", and so forth. For more information, please refer to Section 7.8.

Availability: Administrator

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

/G Plug Group Parameters

Displays a menu used to View, Add, Modify or Delete Plug Groups. For more information on Plug Groups, please refer to Section 7.7.

Notes:

- *This command is not available on WTI Console Server Products.*
- *On RPC Series DC Power Control products, this command applies to Circuits Groups rather than Plug Groups.*

The Add Plug Group menu offers the following configuration options:

Parameter (Default)	Description
Plug Group Name (Default = Undefined)	Assigns a descriptive name to the Plug Group or Circuit Group.
Plug Access (Default = Undefined)	Determines which switched outlets (or circuits) will be included in this Plug Group (or Circuit Group.) **Notes:** • *When a series of outlets are switched On/Off or Rebooted, the Boot/Sequence Delay parameter can be used to insert a delay time between each switching operation. For more information, please refer to Section 7.8.* • *If needed, the Boot Priority parameter can be used to determine the order in which plugs are switched On/Off or rebooted.*

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 primary Ethernet Port, optional secondary Ethernet Port, and optional Cellular Modem Port.

If an optional internal Dial-Up Modem is present or if one of the available serial ports has been configured for Modem PPP Mode, then the /N* command will provide access to configuration menus for the optional Dial-Up Modem in place of the optional Cellular Modem. In addition, the Network Selection menu also allows access to configuration menus for both IPv4 and IPv6 protocols.

Notes:

- *All functions provided by the /N* command are also available via the Web Browser Interface.*
- *WTI Devices cannot include both the optional Cellular Modem and the optional Dial-Up Modem.*

Depending on the options present, the Network Selection Menu may offer access to up to six network port configuration menus:

- **[eth0] IPv4:** Primary Network Port, IPv4 and Shared Parameters
- **[eth1] IPv4:** Optional Secondary Network Port, IPv4 Parameters
- **[cell] IPv4:** Optional Cellular Modem Port, IPv4 Parameters
- **[eth0] IPv6:** Primary Network Port, IPv6 Parameters
- **[eth1] IPv6:** Optional Secondary Network Port, IPv6 Parameters
- **[cell] IPv6:** Optional Cellular Modem Port, IPv6 Parameters

If the unit does not include the optional Analog Modem, then the Network Selection Menu will offer access to the following Modem PPP configuration menus:

- **ppp0, IPv4:** Optional Analog Modem Port, IPv4 Parameters. For a description of the parameters included in the ppp0/IPv4 menu, please refer to Section 7.4.
- **ppp0, IPv6:** Optional Analog Modem Port, IPv6 Parameters. For a description of the parameters included in the ppp0/IPv4 menu, please refer to Section 7.4.

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 Primary 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 primary 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 WTI Device via the CLI as described in Section 3.3.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the primary 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 WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the primary 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 WTI Device via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol, defines the DHCP 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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
IP Tables (Default = Undefined)	Allows the WTI Device to restrict unauthorized IP addresses from establishing inbound connections as described in Section 7.3.1.4.
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.

Parameter (Default)	Description
Communication Settings (continued)	
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 7.3.1.6.
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the WTI Device negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the WTI Device's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the WTI Device's Negotiation parameter should be set to match the other device* (e.g., "100/Full.)
Fallback (Default = Off)	(Dual Ethernet Units Only) When enabled, the WTI Device will automatically fallback to the other Ethernet Port when communication via one port fails. For example, if communication via eth0 fails, the unit will automatically switch to eth1 (and vice versa.) In addition to switching Ethernet Ports, the unit will also use the same MAC Address and IP Address as were used before the fallback occurred.
General Parameters	
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]+[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.*
General Parameters (continued)	

Parameter (Default)	Description
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.*
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.*
Servers and Clients	
Telnet Access (Default = Off)	Enables/disables Telnet access to the Ethernet Port(s,) 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.*

Parameter (Default)	Description
Servers and Clients (continued)	
SSH Access (Default = On)	Enables/disables SSH communication at the Ethernet Port(s,) 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 WTI Device.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the primary Ethernet Port (eth0.) For more information, please refer to Section 7.3.1.10. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot 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 7.3.1.11.
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 7.3.1.12.
TACACS (Default = Off)	Provides access to a submenu that is used to define TACACS parameters and Default TACACS User Access as described in Section 7.3.1.13.
RADIUS (Default = Off)	Provides access to a submenu that is used to define parameters for RADIUS authentication per Section 7.3.1.14.
Ping Access (Default = Allow All Pings)	Configures the WTI Device's response to ping commands at the primary 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 per Section 7.3.1.16.
Outbound Access (Default = Off)	Enables/Disables the ability to create outbound SSH/Telnet connections via the WTI Devices's Ethernet Port(s) and sets the Outbound Secure Level.
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: eth1, IPv4

This menu is used to define IPv4 communication parameters for the Optional Secondary Ethernet Port (eth1) plus Shared parameters. The eth1, IPv4 menu offers the following options:

Note: *This menu is not present on WTI Devices that do not include the Optional Secondary Ethernet Port.*

Parameter (Default)	Description
Communication Settings	
IP Address (Default = 192.168.168.168)	The IPv4 format address for the Optional Secondary Ethernet Port, eth1. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the WTI Device via the CLI as described in Section 3.3.*
Subnet Mask (Default = 255.255.255.0)	The IPv4 format Subnet Mask for the Optional Secondary Ethernet Port, eth1. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv4 format Gateway Address for the Optional Secondary Ethernet Port, eth1. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
DHCP (Default = Off)	Enables/disables Dynamic Host Configuration Protocol, defines the DHCP 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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
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.
DDNS Services (Default = Undefined)	Provides access to a submenu, which is used to define DDNS parameters. For more information, please refer to Section 7.3.1.6.

Parameter (Default)	Description
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the WTI Device negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the WTI Device's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the WTI Device's Negotiation parameter should be set to match the other device* (e.g., "100/Full.)
Servers and Clients	
Web Access (Default = Off)	Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access. For more information, please refer to Section 7.3.1.8.
Syslog	Provides access to a submenu that can be used to Enable/Disable Syslog Server functions and define the Port Number, Transport, Secure Syslog and Block IPs as described in Section 7.3.1.9.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the primary Ethernet Port (eth0.) For more information, please refer to Section 7.3.1.10. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
Ping Access (Default = Allow All)	Configures the WTI Device's response to ping commands at the primary Ethernet Port (eth0). **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

Network Parameters [cell] IPv4

This menu is used to define IPv4 communication parameters for the Optional Cellular Modem Port (cell.) The [cell] IPv4 menu offers the following options:

> **Note:** *This menu is not present on WTI Devices that do not include the Optional Cellular Modem.*

Parameter (Default)	Description
Communication Settings	
Default Gateway (Default = Off)	Enables/disables the Default Gateway for IPv4 communication. **Note:** *The status of the Default Gateway parameter cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
User Peer DNS (Default = Off)	When enabled, internet connections will use your carrier's DNS rather than the standard DNS.
Static Route (Default = Undefined)	Provides access to a submenu which allows you to define Linux routing commands for IPv4 that will be automatically executed each time that a user accesses the user interface via the optional Cellular Modem Port. .
DDNS Services (Default = Undefined)	The DDNS Parameters [cell] menus are used to select parameters and define hosts for Dynamic DNS services. Note that there are two separate DDNS [cell] menus; one for IPv4 communication and one for IPv6 communication. This allows you to set up separate DDNS parameters for each protocol. For more information, please refer to Section 7.4.1.3.
Modem Stay Alive (Default = Off)	When enabled, the optional cellular modem will not time out due to inactivity. **Note:** *This parameter is only available via the CLI.*
LCP Echo (Default = On)	Provides access to a submenu that is used to define values for the LCP Echo Interval and LCP Echo Failure.
Protocol (Default = IPv4)	Selects the protocol for communication with the cellular provider; IPv4, IPv6 or both IPv4 & IPv6.
MTU/MRU (Default = 552)	Sets the Maximum Receive Unit and Maximum Transmit Unit. Will Send/Receive data packets of no more than n bytes through the cellular network.
Modem PPP Params	Displays currently defined Modem PPP parameters for the optional Cellular Modem Port. **Note:** *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will instead be supplied by the ISP.*

Parameter (Default)	Description
Servers and Clients	
Web Access	Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access. For more information, please refer to Section 7.4.1.4.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the Cellular Modem Port. For more information, please refer to Section 7.4.1.5. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
PING Access (Default = Allow All)	Configures the WTI Device's response to ping commands at the Cellular Modem Port. **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

Network Parameters [eth0] IPv6

This menu is used to define IPv6 communication parameters for the Primary 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 primary 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 WTI Device via the CLI as described in Section 3.3.*
Subnet Prefix (Default = Undefined)	The IPv6 Subnet Prefix for the primary 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 WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the primary 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 WTI Device via the CLI.*

Parameter (Default)	Description
Communication Settings (continued)	
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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
IP Tables (Default = Undefined)	Allows the WTI Device to restrict unauthorized IP addresses from establishing inbound connections as described in Section 7.3.3.2.
Static Route (Default = Undefined)	Allows definition of Linux routing commands that will be automatically executed each time a user accesses the user interface via this Ethernet Port.
DDNS Services (Default = Undefined)	This option is used to define DDNS parameters. For more information, please refer to Section 7.3.3.4.
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the WTI Device negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the WTI Device's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the WTI Device's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*
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. For more information, please refer to Section 7.3.3.6.1.
SYSLOG Address (Default = Off)	Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the WTI Device.

Parameter (Default)	Description
Servers and Clients (continued)	
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the primary Ethernet Port (eth0.) For more information, please refer to Section 7.3.3.8. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot 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 7.3.3.9.
Ping Access (Default = Allow)	Configures the WTI Device's response to ping commands at the primary 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 as described in Section 7.3.3.11.

Network Parameters [eth1] IPv6

This menu is used to define IPv6 communication parameters for the optional Secondary Ethernet Port (eth1.) The eth1 IPv6 menu offers the following options:

Note: *This menu is only available on WTI Devices that include the optional Secondary Ethernet Port (eth1.)*

Parameter (Default)	Description
Communication Settings	
IP Address (Default = Undefined)	The IPv6 format address for the optional Secondary Ethernet Port, eth1. **Note:** *The IP Address cannot be changed via the Web Browser Interface. In order to change the IP address, you must access the WTI Device via the CLI as described in Section 3.3.*
Subnet Prefix (Default = Undefined)	The IPv6 Subnet Prefix for the optional Secondary Ethernet Port, eth1. **Note:** *The Subnet Mask cannot be changed via the Web Browser Interface. In order to change the Subnet Mask, you must access the WTI Device via the CLI.*
Gateway Address (Default = Undefined)	The IPv6 format Gateway Address for the optional Secondary Ethernet Port, eth1. **Note:** *The Gateway Address cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device 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 WTI Device 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 WTI Device.* • *DHCP status cannot be changed via the Web Browser Interface. In order to change DHCP status, you must access the WTI Device via the CLI.*
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.

Parameter (Default)	Description
Communication Settings (continued)	
DDNS Services (Default = Undefined)	This option is used to define DDNS parameters. For more information, please refer to Section 7.3.4.3.
Negotiation (Default = Auto)	This parameter can be used to solve synchronization problems when the WTI Device negotiates communication parameters with another device. **Notes:** • *If the other device is set for automatic negotiation, then the WTI Device's Negotiation parameter should also be set to Auto.* • *If the other device is not set for automatic negotiation, then the WTI Device's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*
Servers and Clients	
Web Access (Default = Off)	Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access. For more information, please refer to Section 7.3.4.5.
Syslog	Provides access to a submenu that can be used to Enable/Disable Syslog Server functions and define the Port Number, Transport, Secure Syslog and Block IPs as described in Section 7.3.3.7.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the primary Ethernet Port (eth0.) For more information, please refer to Section 7.3.4.6. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
Ping Access (Default = All On)	Configures the WTI Device's response to ping commands at the primary Ethernet Port (eth0). **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

Network Parameters [cell] IPv6

This menu is used to define IPv6 communication parameters for the Optional Cellular Modem Port (cell.) The [cell] IPv4 menu offers the following options:

> **Note:** *This menu is not present on WTI Devices that do not include the Optional Cellular Modem.*

Parameter (Default)	Description
Communication Settings	
Default Gateway (Default = Undefined)	Enables/disables the Default Gateway for IPv6 communication via the optional Cellular Modem Port. **Note:** *The status of the Default Gateway parameter cannot be changed via the Web Browser Interface. In order to change the Gateway Address, you must access the WTI Device via the CLI.*
Static Route (Default = Undefined)	Provides access to a submenu which allows you to define Linux routing commands for IPv4 that will be automatically executed each time that a user accesses the user interface via the optional Cellular Modem Port.
DDNS Services (Default = Undefined)	The DDNS Parameters [cell] menus are used to select parameters and define hosts for Dynamic DNS services. Note that there are two separate DDNS [cell] menus; one for IPv4 communication and one for IPv6 communication. This allows you to set up separate DDNS parameters for each protocol. For more information, please refer to Section 7.4.2.3.
Modem PPP Params	Displays currently defined Modem PPP parameters for the optional Cellular Modem Port. **Note:** *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will instead be supplied by the ISP.*
Servers and Clients	
Web Access (Default = Off)	Provides access to the Web Access and SSL Certificates menu. Enables/disables and configures HTTP access and HTTPS access. For more information, please refer to Section 7.4.2.4.
SNMP Access (Default = Off)	Enables/disables SNMP Polling and selects IPv4 format access parameters for the SNMP feature at the Cellular Modem Port. For more information, please refer to Section 7.4.2.5. **Note:** *After you have configured SNMP Access Parameters, you will then be able to manage the WTI Device's User Directory, control power and reboot switching and display unit status via SNMP, as described in Appendix G.*
PING Access (Default = All On)	Configures the WTI Device's response to ping commands at the Cellular Modem Port. **Note:** *Disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm.*

/PNA Ping No Answer Configuration Parameters

(WTI Console Server Products Only) 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 WTI Device 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 7.10.5.

> **Note:** *This command is only available on WTI Console Server Products. The PNA command is not available on WTI Power Control Products and Console Server + Power Control Combos.*

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. When this address fails to respond to the Ping command, the WTI Power Control product will reboot the selected outlets. **Note:** *In order to use domain names, DNS Server parameters must first be defined per Section 7.3.1.6.1.*
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)	Assigns a descriptive name to each switched outlet or circuit.
Ping Delay After PNA Action (Default = 15 Minutes)	Determines how long the WTI Device will wait to send additional Ping commands, after a Ping-No-Answer Reboot has been initiated. Typically, this option is used to allow time for a device to fully "wake up" after a Ping-No-Answer Reboot before 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 Reboot.
PNA Action (Default = Continuous Alarm)	Determines how the WTI Device will react when the IP address fails to respond to a ping: • **Continuous:** The WTI Device will continuously reboot the specified outlet(s) and send notification until the IP address responds and the Ping-No-Answer Reboot is cleared • **Single:** The WTI Device will reboot the specified outlet(s) and send notification only once each time the Ping-No-Answer Reboot is initially triggered.
Ping Test	Pings the Address specified in the "IP Address or Domain Name" Field.

Availability: Administrator

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

/RB Reboot Options

Displays a menu that is used to configure Scheduled Reboots and Ping-No-Answer Reboots:

- **Scheduled Reboots:** Regularly reboots specific outlets based on a user-defined schedule.
- **Ping No Answer Reboots:** Pings a device at a user specified IP Address or domain and automatically reboots outlet when the IP Address or Domain Name fails to respond.

For more information on Reboot options and parameters, please refer to Section 7.9.

Notes:

- *This command is not available on WTI Console Server Products.*
- *On RPC Series DC Power Control products, reboot operations are applied to Circuits rather than plugs/outlets.*
- *If desired, the Ping-No-Answer Reboot function can also be configured to send email notification whenever a Ping-No-Answer Reboot is generated. For more information, please refer to Section 7.10.5.*

Availability: Administrator

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

/AC Alarm Configuration Parameters

Displays a menu used to configure and enable the WTI Device's monitoring and alarm functions. When properly configured and enabled, these Alarm Functions can provide notification when numerous conditions are detected by the WTI Device. For more information on Alarm Configuration, please refer to Section 7.10. The Alarm Configuration Menu allows the following alarms to be defined:

Alarm Name (Default)	Description
Over Current (Initial) (Default = On - 80% of max)	(WTI Devices with Current Metering Option Only) Provides notification when the current consumption level reaches a point that might indicate a potential problem.
Over Current (Critical) (Default = On - 90% of max)	(WTI Devices with Current Metering Option Only) Provides notification when the current consumption level reaches a point that indicates a hazardous condition.
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.
Circuit Breaker Open (Default = On)	(Breakered WTI Devices Only) Provides notification when a Circuit Breaker on the WTI Device is open.
Lost Communication with Unit (Default = On)	Provides notification when communication with the WTI Device is disrupted.
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 WTI Device has locked serial ports due to repeated, invalid attempts to access the user interface via serial port.
Power Cycle (Cold Boot) (Default = On)	(WTI Devices with Single Power Inlets Only) Provides notification when all input power to the WTI Device unit is lost and then restored.
Alarm Input Alarm (Default = On)	(RPC Series Units Only) Monitors dry contacts connected to the Alarm Inputs on the RPC's back panel.
Buffer Threshold (Default = On)	(CPM, DSM and REM Series Devices Only) Provides notification when the amount of data stored in the buffer for a given serial port exceeds the Buffer Threshold Value.
Plug Current (Default = On)	(WTI Devices with Current Metering Option Only) Monitors current consumption at each of the switched outlets and generates an alarm when current exceeds the High threshold or falls below the Low threshold.
Lost Voltage (Line In) (Default = On)	(WTI Devices with Dual Power Inlets Only) Provides notification when power to one of the available power inlets is interrupted.
No Dialtone (Default = On)	Monitors a telephone line connected to an external modem installed at the WTI Device's Setup Port, and then provides notification if the phone line is dead or no dialtone is present.

Alarm Name (Default)	Description
Emergency Shutoff (Default = On)	(WTI Power Control Products and WTI Console Server + Power Control Combo Products Only) Provides notification when the Emergency Shutoff feature is activated.
Wakeup On Failure (Default = On)	(WTI Devices with Optional Cellular Modem Only) Provides notification after the unit recovers from a failure to communicate via cellular.
IP Passthrough Data Usage (Default = On)	(WTI Devices with Optional Cellular Modem Only) Allows the WTI Device to monitor data for IP Passthrough cellular communication and provide notification when data usage rises above a user-defined Threshold value. A sudden rise in IP Passthrough Data Usage is often an indication that primary WAN communication may be down.
Buffer Filtering (Default = On)	(WTI Console Products and Console + Power Combos Only) Monitors data as it is received at a Buffer Mode port and provides notification when specific text strings are detected. Typically, this alarm is used to notify support personnel when error messages and other text strings are generated.
No Cellular PPP Connection (Default = On)	(WTI Devices with Optional Cellular Modem Only) Provides notification when a cellular connection to the WTI Device is not available. Detects loss of cellular communication with the WTI device, and allows support personnel to restore cellular connection to ensure Out-of-Band access.

Availability: Administrator

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

/I Reboot System (Default)

Re-initializes the WTI Device and offers the option to either retain user-defined parameters or reset to default parameters. As described in Section 10.3, 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 WTI Device software become available, this command can be used to update existing software as described in Section 11.2.

Notes:

- *The WMU Enterprise Management Utility is the preferred method for managing WTI Device software upgrades. The /UFW command is intended to provide an alternative to the WMU. For more information, please refer to Section 11.1.*
- *When a software upgrade is performed, the WTI Device will require 15 minutes for the upgrade procedure.*
- *When upgrading software on WTI Power Control products or WTI Console Server + Power Control Combo products, power outlets will not be switched On or Off during the upgrade process. For more information, please refer to the WTI.com Knowledge Base.*

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]**

/CP Copy RS232 Port Parameters

Allows quick set-up when several serial ports will be configured with similar parameters. When the /CP command is invoked, the WTI Device will display a menu that can be used to copy parameters to RS232 ports. For more information regarding port configuration options, please refer to Section 7.2.

Note: *To proceed with the Copy function after selecting new parameters, press **[Esc]**; the WTI Device will then display the confirmation prompt before proceeding.*

Availability: Administrator
Format: `/CP` **[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 7.3.1.6.1.*
- *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. For more information, please refer to Section 7.6.

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

WTI Devices 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 WTI Devices, 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 a serial port on a DSM Series or CPM Series unit, 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 WTI Device supports SSH connections, which provide secure, encrypted access via network. In order to communicate with the WTI Device 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 WTI Device 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 WTI Device, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the WTI Device 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 WTI Device 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.*

D.3. The Direct Connect Feature

The Direct Connect feature allows you to initiate an SSH, Raw Socket or Telnet session with a DSM Series or CPM Series unit and make an immediate connection to a specific serial port of your choice, without first being presented with the command interface. This allows you to connect to a TCP port that is mapped directly to one of the DSM/CPM's serial ports.

Direct Connect employs unique, pre-assigned TCP port numbers for each serial port. The user connects to the port of choice by including the associated TCP port number in the SSH or Telnet connect command line. The Direct Connect feature can be individually configured at each serial port and can be used to connect to Any-to-Any, Passive, Buffer, or Modem Mode ports.

D.3.1. Standard SSH, Raw Socket and Telnet Protocol

The Direct Connect feature allows you to establish port connections using either Standard Telnet Protocol, SSH encryption or Raw Socket. When Standard Telnet Protocol is used, the DSM/CPM will respond to all IACs. When configuring a serial port to allow Direct Connections using SSH protocol, note that the Direct Connect option (Serial Port Configuration menu,) must be set to "On - Password" as described in Section 7.2. When configuring a serial port to allow Direct Connections using either Standard Telnet or Raw Socket Mode, note that the Direct Connect option (Serial Port Configuration menu,) may be set to either "On - Password" or "On - No Password".

D.3.2. Configuration

The Direct Connect Function is configured on a per port basis using the Serial Port Configuration menu's "Direct Connect" option. The following options are available:

1. **OFF:** Direct Connect disabled at this port. (Default)
2. **ON - NO PASSWORD:** The Direct Connect feature is enabled at this port, but no password is required in order to connect to the port.
   a) When the connection is established, the user is immediately connected directly to the specified port, and the client is notified at the TCP level.
   b) This option is intended for situations where security is provided by the attached device.

   Note: *The SSH Direct Connection function is disabled when the "On - No Password" option is selected.*
3. **ON - PASSWORD:** The Direct Connect feature is enabled at this port, but a password must be entered before a Direct Connection is established.
   a) Upon login, the DSM/CPM will prompt for a username and password. If a valid username/password is entered, the DSM/CPM will return a message which confirms the connection and lists the name and number of the port (providing the user account allows access to the target port.)
   b) If a valid username / password is not entered in 30 seconds or three attempts, the port will timeout and disconnect.

4. **OFF - Break on Raw Disconnect:** When the Direct Connect option has been enabled as described in Steps 2 or 3 above, this option can be used to configure the DSM/CPM to send a break character whenever a Raw Socket connection to this port is terminated. The Break on Raw Disconnect option will work when the password feature is either enabled or disabled as described below:

   a) **Password Disabled:** To employ the Break on Raw Disconnect option with the Direct Connect password disabled, proceed as follows:

      i. Access the Serial Port configuration menu for the desired DSM/CPM serial port, and then use the Direct Connect option to select the "On - No Password" option. After "On - No Password" is selected, the menu will return to the Serial Port configuration screen.

      ii. Use the Direct Connect option to select the "Break on Raw Disconnect" parameter. After "Break on Disconnect" is selected, the menu will return to the Direct Connect configuration screen. Note that at this point, the prompt for the "Break on Disconnect" option will read "On - Break on Disconnect", indicating that both the Direct Connect feature and the Break on Disconnect feature are enabled.

   b) **Password Enabled:** To employ the Break on Raw Disconnect option with the Direct Connect password enabled, proceed as follows:

      i. Access the Serial Port configuration menu for the desired DSM/CPM serial port, and then use the Direct Connect option to select the "On - Password" option. After "On - Password" is selected, the menu will return to the Serial Port configuration screen.

      ii. Use the Direct Connect option to select the "Break on Raw Disconnect" parameter. After "Break on Disconnect" is selected, the menu will return to the Direct Connect configuration screen. At this point, the prompt for the "Break on Disconnect" option will read "On - Break on Disconnect", indicating that both the Direct Connect feature and the Break on Disconnect feature are enabled.

Notes:

- *If you intend to create "Raw Socket" connections to DSM/CPM serial ports, then the "Raw Socket Access" feature must also be enabled at the Network Port, as described in Section 7.3.1.1.*
- *If you intend to use SSH to establish direct connections to the DSM/CPM, the "Direct Connect ON - PASSWORD option must be selected.*
- *If Administrator level commands are disabled at the Network Port, then accounts that permit Administrator level commands will not be able to initiate a Direct Connection.*
- *If Administrator level commands are enabled at the Network Port, then accounts with Administrator level access and accounts without Administrator level access will both be allowed to establish Direct Connections.*
- *If your user account does not permit access to the target port, the connection will be refused.*

D.3.3. Connecting to a Serial Port using Direct Connect

Direct Connect TCP port numbers are as follows:

1. Standard Telnet Direct Connection (with Password):

   a) DSM-8 Series and CPM-800 Series units:
      - Serial Ports: TCP port numbers 2101 through 2108.
      - Optional Internal Modem Port: TCP port number 2109.

   b) CPM-1600 Series units:
      - Serial Ports: TCP port numbers 2101 through 2116.
      - Optional Internal Modem Port: TCP port number 2117.

   c) DSM-24 Series units:
      - Serial Ports: TCP port numbers 2101 through 2124.
      - Optional Internal Modem Port: TCP port number 2125.

   d) DSM-40 Series units:
      - Serial Ports: TCP port numbers 2101 through 2140.
      - Optional Internal Modem Port: TCP port number 2141.

   e) REM Series units:
      - Serial RJ45 Ports: TCP port numbers 2101 through 2104.
      - USB Console Ports: TCP port numbers 2143 and 2151.

2. Standard Telnet Direct Connection (without Password):

   a) DSM-8 Series and CPM-800 Series units:
      - Serial Ports: TCP port numbers 2301 through 2308.
      - Optional Internal Modem Port: TCP port number 2309.

   b) CPM-1600 Series units:
      - Serial Ports: TCP port numbers 2301 through 2316.
      - Optional Internal Modem Port: TCP port number 2317.

   c) DSM-24 Series units:
      - Serial Ports: TCP port numbers 2301 through 2324.
      - Optional Internal Modem Port: TCP port number 2325.

   d) DSM-40 Series units:
      - Serial Ports: TCP port numbers 2301 through 2340.
      - Optional Internal Modem Port: TCP port number 2341.

   e) REM Series units:
      - Serial RJ45 Ports: TCP port numbers 2301 through 2304.
      - USB Console Ports: TCP port numbers 2343 and 2351.

3. SSH Direct Connection (with Password):

   a) DSM-8 Series and CPM-800 Series units:
      - Serial Ports: TCP port numbers 2201 through 2208.
      - Optional Internal Modem Port: TCP port number 2209.

   b) CPM-1600 Series units:
      - Serial Ports: TCP port numbers 2201 through 2216.
      - Optional Internal Modem Port: TCP port number 2217.

   c) DSM-24 Series units:
      - Serial Ports: TCP port numbers 2201 through 2224.
      - Optional Internal Modem Port: TCP port number 2225.

   d) DSM-40 Series units:
      - Serial Ports: TCP port numbers 2201 through 2240.
      - Optional Internal Modem Port: TCP port number 2241.

   e) REM Series units:
      - Serial RJ45 Ports: TCP port numbers 2201 through 2204.
      - USB Console Ports: TCP port numbers 2243 and 2251.

4. Raw Socket Direct Connection (with Password):

   a) DSM-8 Series and CPM-800 Series units:
      - Serial Ports: TCP port numbers 3101 through 3108.
      - Optional Internal Modem Port: TCP port number 3109.

   b) CPM-1600 Series units:
      - Serial Ports: TCP port numbers 3101 through 3116.
      - Optional Internal Modem Port: TCP port number 3117.

   c) DSM-24 Series units:
      - Serial Ports: TCP port numbers 3101 through 3124.
      - Optional Internal Modem Port: TCP port number 3125.

   d) DSM-40 Series units:
      - Serial Ports: TCP port numbers 3101 through 3140.
      - Optional Internal Modem Port: TCP port number 3141.

   e) REM Series units:
      - Serial RJ45 Ports: TCP port numbers 3101 through 3104.
      - USB Console Ports: TCP port numbers 3143 and 3151.

5. Raw Socket Direct Connection (without Password):

   a) DSM-8 Series and CPM-800 Series units:
      - Serial Ports: TCP port numbers 3301 through 3308.
      - Optional Internal Modem Port: TCP port number 3309.

   b) CPM-1600 Series units:
      - Serial Ports: TCP port numbers 3301 through 3316.
      - Optional Internal Modem Port: TCP port number 3317.

   c) DSM-24 Series units:
      - Serial Ports: TCP port numbers 3301 through 3324.
      - Optional Internal Modem Port: TCP port number 3325.

   d) DSM-40 Series units:
      - Serial Ports: TCP port numbers 3301 through 3340.
      - Optional Internal Modem Port: TCP port number 3341.

   e) REM Series units:
      - Serial RJ45 Ports: TCP port numbers 3301 through 3304.
      - USB Console Ports: TCP port numbers 3343 and 3351.

   Note: *In order to create a Raw Socket Direct Connection, the "Raw Socket Access" parameter for the Network Port must be enabled as described in Section 7.3.1.1.*

When establishing a Direct Connection, the correct TCP port number must be used. If conditions are acceptable (e.g. Target Port must be free and properly configured), an immediate connection will be made, with one possible exception; password entry may first be required depending on configuration settings.

Note: *When a Direct Connect attempt fails because the Port is busy, the call is rejected at the TCP level.*

Connection Example

1. Assume that Port 8 is configured as described in Appendix D.3.2. If the DSM/CPM's IP address is "1.2.3.4", and you wish to establish a standard Telnet protocol connection with port 8 (TCP Port Number 2108), then on a UNIX system, the connect command would be invoked as follows:

   ```
   $ telnet 1.2.3.4 2108  [Enter]
   ```

2. The DSM/CPM will first send the site ID, Port Number, Port Name, and Telnet Port number, and then once a connection is established, the "Connected" message will be sent.

D.3.4. Terminating a Direct Connect Session

To terminate a Direct Connect session, use the client program's "disconnect" feature. The following will occur immediately upon a client initiated disconnect:

1. The Network port is disconnected from the serial port.
2. The Network session is terminated.
3. The serial port is put to sleep.

Notes:

- *The CLI's Sequence Disconnect Command (defined via the Serial Port Configuration menus), cannot be used to terminate a Direct Connection.*
- *Any DSM/CPM port that allows Administrator or SuperUser level commands can terminate a direct connection at another port by issuing the CLI's /D command or via the Web Browser Interface's Port Control Screen.*
- *Acknowledgment of data received by the DSM/CPM network port does not automatically indicate that the data has been completely sent out the serial port. Data may still be queued in DSM/CPM buffers. Any data queued at the time of a client initiated disconnect is discarded, and is not passed to the attached device.*

D.4. IP Aliasing

In addition to the Direct Connect function described in Appendix D.3, the DSM/CPM also supports IP Aliasing, which provides another method for connecting directly to any serial port on the unit without first accessing the command interface. IP Aliasing allows you to assign an IP address to a DSM/CPM serial port, and then connect to that port directly via Telnet, SSH or Raw Socket.

In order to configure DSM/CPM serial ports for IP Aliasing, you must first access the Serial Port Configuration menu for the desired port(s) as described in Section 7.2. In addition, you must also set the Direct Connect feature to either "On - Password" or "On - No Password".

Once a DSM/CPM serial port has been configured as described above, users can connect to the port in the same manner that would be used to establish a connection with any other IP address. For example, if the serial port IP Alias was set to "1.2.3.4" then users would be able to connect to the port using the following connect command:

`$ telnet 1.2.3.4` **[Enter]**

Notes:

- *The IP Alias feature is only available when the Direct Connect feature is set to "On - Password" or "On - No Password."*
- *To display the IP Alias status via the Web Browser Interface, place the cursor over the "Port Status" link on the left hand side of the screen, wait for the flyout menu to appear and then click on the "Alias Status" link.*
- *To display the assigned IP Alias for each serial port via the CLI, type* **`/SA`** *and press* ***[Enter]****.*

D.5. Creating an Outbound SSH Connection

The DSM/CPM Command Line Interface (CLI) includes an /SSH command that can be used to create an outbound SSH connection. In order to use the /SSH command, you must access the DSM/CPM's CLI using an account that permits SSH Access and Outbound Access, via one of the DSM/CPM's Serial RS232 Ports as described below.

Notes:

- *In order for the /SSH command to function, SSH Access and Outbound Service Access must be enabled for your user account as described in Section 7.5.*
- *The /SSH command is only available via the CLI.*
- *If you have logged in via the Network Port, the /SSH command will not function.*

To create an outbound SSH connection, access the CLI via a free Serial Port, using an account that permits SSH Access and Outbound Access and then invoke the /SSH command using the following format:

`/SSH <ip> -l <username>` [Enter]

Where:

`ip`	Is the target IP address.
`-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.

For example, to create an outbound SSH connection to a device at IP Address 255.255.255.255, with the username "employee", access the CLI via a free DSM/CPM Serial Port using an account that permits SSH Access and Outbound Access and invoke the SSH command as follows:

`/SSH 255.255.255.255 -l employee` [Enter]

D.6. Creating an Outbound Telnet Connection

The DSM/CPM Command Line Interface (CLI) includes a /TELNET command, that can be used to create an outbound Telnet connection. In order to use the /TELNET command, you must access the DSM/CPM's CLI using an account that permits Telnet Access and Outbound Access, via one of the DSM/CPM's Serial Ports as described below.

Notes:

- *In order for the /TELNET command to function, Telnet Access and Outbound Service Access must be enabled for your user account as described in Section 7.5.*
- *The /TELNET command is only available via the CLI.*
- *If you have logged in via the Network Port, the /TELNET command will not function unless Outbound Access has been enabled.*

To create an outbound Telnet connection, access the CLI via a free Serial Port, using an account that permits Telnet Access and Outbound Access and then invoke the /TELNET command using the following format:

`/TELNET <ip> [port] [raw]` [Enter]

Where:

`ip`	Is the target IP address.
`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`**".

For example, to create a raw socket, outbound Telnet connection to port 2000 at IP Address 255.255.255.255, access the CLI via a free DSM/CPM Serial Port using an account that permits Telnet Access and Outbound Access and invoke the TELNET command as follows:

`/TELNET 255.255.255.255 2000 raw` [Enter]

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 as described in Section 7.1.1., 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 as described in Section 7.3.1.8 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 WTI Device, 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 7.10 is triggered.

Appendix F. SNMP Traps

The SNMP Trap function allows the WTI Device to send Alarm Notification messages to two different SNMP managers, each time one of the Alarms discussed in Section 7.10 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.*
- *For further instructions regarding setting up the Buffer Threshold Alarm to send SNMP Traps, please refer to Section 7.10.9.*

F.1. Alarm Notification via SNMP Traps

Note: *When setting up the Buffer Threshold Alarm (DSM, CPM and REM Series units only,) please refer to Appendix F.2 for further instructions.*

For most of the available WTI Device 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 WTI Device will send an SNMP Trap each time an alarm is triggered.

F.2. SNMP Trap Notification for the Buffer Threshold Alarm

Notes:

- *The Buffer Threshold Alarm is only available on WTI DSM Series, CPM Series and REM Series products.*
- *Please refer to Section 7.10.9 for further instructions regarding enabling and configuring the Buffer Threshold alarm.*

To configure the Buffer Threshold Alarm to generate an SNMP Trap whenever data in a given Serial Port buffer exceeds the user-defined trigger level, proceed as follows:

1. Access the user interface using an account that permits access to Administrator level commands.
2. **Serial Port Configuration:** Access the Serial Port Configuration menu for the desired serial port and set the following:
   a) **Port Mode:** Make certain that Port Mode is set to Buffer Mode.
   b) **Buffer Threshold:** Set the Buffer Threshold to the desired value. The Buffer Threshold determines how much data must accumulate in a given port buffer in order to trigger the Buffer Threshold alarm.
3. **SNMP Trap Parameters:** Access the Network Configuration menu's SNMP Traps submenu and set the following parameters:
   a) **SNMP Managers 1 through 4:** The address(es) that will receive SNMP Traps generated by the Buffer Threshold Alarm. 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:

- *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 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.*

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

Once the Buffer Threshold level and SNMP Trap parameters have been defined and the Buffer Threshold Alarm has been enabled, the WTI Device will send an SNMP Trap each time the amount of data in the buffer for the target serial port exceeds the defined Buffer Threshold level.

Appendix G. Operation via SNMP

If SNMP Access Parameters have been defined as described in Section 7.3.1.9, then you will be able to manage user accounts, control power and reboot switching and display unit status via SNMP. This section describes SNMP communication with the WTI Device, and lists some common commands that can be employed to manage users, control switching and reboot actions and display unit status.

G.1. WTI Device SNMP Agent

The WTI Device's SNMP Agent supports various configuration, control, status and event notification capabilities. Managed objects are described in the follow two files, both of which are available via the Downloads page at **https://www.wti.com**:

- **WTI-CONSOLE-MIB.TXT -** DSM Series Console Server products and CPM Series Console Server + Power Control Combo products.
- **WTI-POWER-MIB.TXT -** VMR, NPS, NBB and RPC Series Power Control products.

These MIB documents can be compiled for use with your SNMP client.

Notes:

- *The WTI Device 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 WTI Device 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 WTI Device supports either MD5 or SHA1.

G.3. Configuration via SNMP

WTI Device 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`** – (WTI Power Control Products and WTI Console Server + Power Control Combo Products only) A string of up to 16 characters, with one character for each of the 16 possible plugs/circuits on the WTI Device. A '`0`' indicates that the account does not have access to the plug/circuit, and a '`1`' indicates that the user does have access to the plug/circuit.
- **`userTable::userPortAccess`** – (DSM and CPM Series products only) A string of up to 41 characters, with one character for each of the possible serial ports on the WTI Device. A '`0`' indicates that the account does not have access to the port, and a '`1`' indicates that the user does have access to the port.

  Note: *The number of ports specified in the userPortAccess string must not exceed the number of serial ports available on your WTI Device. If the userPortAccess string specifies more serial ports than are available on the unit, an error message will be generated.*
- **`userTable::userGroupAccess`** – (WTI Power Control products and WTI Console Server + Power Control Combo products only) A string of 54 characters, with one character for each of the 54 possible plug/circuit groups in the system. A '`0`' indicates that the account does not have access to the plug/circuit group, and a '`1`' indicates that the user does have access to the plug/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. Plug/Circuit Control via SNMP

G.4.1. Controlling Plugs/Circuits

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

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 plug/circuit's ID
- **`plugTable::plugName`** - String indicating the plug/circuit's user-defined name.
- **`plugTable::plugStatus`** – Current state of the plug/circuit
  - **`0`** – Plug/circuit is OFF
  - **`1`** – Plug/circuit is ON
- **`plugTable::plugAction`** – Action to be taken on plug/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 Plug/Circuit Groups

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

ON, OFF, BOOT, and DEFAULT commands can be issued for plug groups (or circuit groups) via SNMP. Plug groups and Circuit Groups are arranged in a table of 54 rows, one row for each plug/circuit group in the system. Plug/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

Note: *The Serial Port management functions described here are only available on DSM Series and CPM Series products.*

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 WTI Device can be retrieved via SNMP. Plug/Circuit Status, and Environmental Status are currently supported.

G.6.1. System Status - Ethernet Port MAC Addresses

Note: Ethernet Port 1 (eth1) is only available on WTI Devices that include the optional, secondary Ethernet Port. To display the Ethernet Port MAC Address for units that include only one Ethernet Port, use the environmentMacEth0 option.

The MAC Address for Ethernet Port 0 (eth0) and Ethernet Port 1 (eth1) can be displayed using the command below:

- **`environmentUnitTable::environmentMacEth0`** - The MAC Address for Ethernet Port 0 (eth0.)
- **`environmentUnitTable::environmentMacEth1`** - The MAC Address for Ethernet Port 1 (eth1.)

G.6.2. Power Input Status

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

- **`environmentUnitTable::environmentInputPower1`** - Status of the first power input
- **`environmentUnitTable::environmentInputPower2`** - Status of the second power input (WTI Devices with Dual or Quad Power Inlets Only.)
- **`environmentUnitTable::environmentInputPower3`** - Status of the third power input (WTI Devices with Quad Power Inlets Only.)
- **`environmentUnitTable::environmentInputPower4`** - Status of the fourth power input (WTI Devices with Quad Power Inlets Only.)

G.6.3. Plug/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 WTI Device. The environmentUnitTable contains one row.

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

G.6.5. Serial Number

Displays the serial number of the WTI Device.

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

G.6.6. Alarm Status

The status of the WTI Device'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 WTI Device. 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 WTI Device can send an SNMP trap to notify you when any of the available WTI Device 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 7.10.

- **`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.
- **plugCurrentSetTrap** - (CPM-C Series Units Only) Indicates that the Plug Current Alarm has been triggered.
- **plugCurrentClearTrap** - (CPM-C Series Units Only) Indicates that the Plug Current Alarm has been Cleared.
- **plugCurrentSetTrap** - (Products with Current Monitoring Capabilities Only) Indicates that the Plug Current Alarm has been triggered.
- **plugCurrentClearTrap** - (Products with Current Monitoring Capabilities Only) Indicates that the Plug Current Alarm has been cleared.
- **lostOptoVoltageSetTrap** - (Units with Two or More Power Inlets Only) Indicates that the Lost Voltage Alarm has been triggered at a unit that includes opto sensors.
- **lostOptoVoltageClearTrap** - (Units with Two or More Power Inlets Only) Indicates that the Lost Voltage Alarm has been cleared at a unit that includes opto sensors.

- **`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..

February 2021
Part Number: 14527, Revision: C

Trademarks and Copyrights Used in this Manual

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