IOLAN

SDS/SCS/STS/MDC Command Line Interface Reference Guide

Version 4.6

Part #5500210-48

November 2014

FCC Note The IOLAN Device Server has been 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 instructions in this Guide, 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/her own expense.

EN 55022: 1998, Class A, Note

WARNING This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Caution: the IOLAN Device Server is approved for commercial use only.

WARNING The IOLAN Device Server SDS T models operate in an ambient air temperature above 70 ^{o}C. However, at 70 ^{o}C and above, a burn hazard exists if the metal case is touched without proper hand protection.

Table of Contents

Preface

About This Book

This guide provides the information you need to:

- configure the IOLAN using the Command Line Interface (CLI)

Intended Audience

This guide is for administrators who will be configuring the IOLAN.

Some prerequisite knowledge is needed to understand the concepts and examples in this guide:

- If you are using an external authentication application(s), working knowledge of the authentication application(s).
- Knowledge of TFTP and/or SFTP, the transfer protocols the IOLAN uses.

Typeface Conventions

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Typeface Example	Usage
At the C: prompt, type: `add host`	This typeface is used for code examples and system-generated output. It can represent a line you type in, or a piece of your code, or an example of output.
Set the value to **`TRUE`**.	The typeface used for `TRUE` is also used when referring to an actual value or identifier that you should use or that is used in a code example.
`subscribe` *`project subject`* **`run`** ***`yourcode`*****`.exec`**	The italicized portion of these examples shows the typeface used for variables that are placeholders for values you specify. This is found in regular text and in code examples as shown. Instead of entering *`project`*, you enter your own value, such as `stock_trader`, and for ***`yourcode`***, enter the name of your program.
IOLAN User's Guide	This typeface indicates a book or document title.
See ***About This Book*** for more information.	This indicates a cross-reference to another chapter or section that you can click on to jump to that section.

Contacting Technical Support

Making a Technical Support Query

Who To Contact

Note: Perle offers free technical support to Perle Authorised Distributors and Registered Perle Resellers.

If you bought your product from a registered Perle supplier, you must contact their Technical Support department; they are qualified to deal with your problem.

Have Your Product Information Ready

When you make a technical support enquiry please have the following information ready:

Item	Write Details Here
Product Name	
Problem Description	
Your Name	
Company Name and Address	
Country	
Phone Number	
Fax Number	
Email Address	

Making a support query via the Perle web page

If you have an internet connection, please send details of your problem to Technical Support using the email links provided on the Perle web site in the **Support/Services** area.

Click here to access our website at the following URL:

http://www.perle.com

Repair Procedure

Before sending a IOLAN for repair, you must contact your Perle supplier. If, however, you bought your product directly from Perle you can contact directly.

Customers who are in Europe, Africa or Middle East can submit repair details via a website form. This form is on the Perle website, **www.perle.com**, in the **Support/Services** area.

Click here to access our web site at the following URL:

http://www.perle.com/support_services/rma_form.asp

Feedback on this Manual

If you have any comments or suggestions for improving this manual please email Perle using the following address:

Email: ptac@perle.com

Please include the **title**, **part number** and **date** of the manual (you can find these on the title page at the front of this manual).

Introduction

This book provides the command line interface (CLI) options available for the IOLAN. The commands are grouped by function.

CLI Conventions

This section explains how to interpret the CLI syntax. If you are an existing IOLAN+ customer and would like to configure the IOLAN in the native IOLAN+ interface, you can type the command **`iolan+`** to display and use the native IOLAN+ interface (you must have **User Level Admin**). See your *IOLAN+ User Guide* for information on using the IOLAN+ interface.

Command Syntax

Each command is broken down into several categories:

- **Description**—Provides a brief explanation of how the command is used.
- **User Level**—Shows which user level(s) (Restricted, Normal, and/or Admin) can issue the command. Some commands have options that are available for one user level and not for another level; this usually occurs when a command is valid for both Normal and Admin user levels, where the Admin user level command will have extended options.
- **Syntax**—Shows the actual command line options. The options can be typed in any order on the command line. The syntax explanation will use the following command to break down the command syntax:

  ```
  set service [dhcp/bootp on|off] [telnetd on|off] [httpd on|off]
  [snmpd on|off] [spcd on|off] [syslog on|off] [dmgrd on|off]
  ```

  - Square brackets ([]) show the options that are available for the command. You can type a command with each option individually, or string options together in any order you want. For example,

    `set service dhcp/bootp on telnetd off`

  - Angle brackets (<>) show that the text inside the brackets is a description for a variable value that you must fill in according to your requirements. In the **`set server`** command, you must determine the values for **`domain`**, **`internet`**, **`name`**, **`password-limit`**, and **`subnet-bit-length`**, if you wish to specify them and not use their defaults (default values provided in the **Options** description). The angle brackets can also contain a range that can be used.
  - The pipe (|) shows an 'or' condition. For example, valid values for **`telnetd`** are either **`on`** or **`off`**.
- **Options**—Provides an explanation of each of the options for a command and the default value if there is one. Some commands do not have any options, so this category is absent.

Command Shortcuts

When you type a command, you can specify the shortest unique version of that command or you can press the **ESC** or **TAB** key to complete the command. For example, the following command:

```
set telnet-client map-to-crlf off
```

can be typed as:

```
set tel map off
```

or, you can use the **ESC** key to complete the lines as you go along:

```
set tel<ESC>net-client ma<ESC>p-to-crlf off
```

where the **ESC** key was pressed to complete the option as it was typed.

Command Options

When you are typing commands on the command line (while connected to the IOLAN), you can view the options by typing a question mark (**?**), **ESC**, or **TAB** key after any part of the command to see what options are available/valid. For example:

```
DS$ set vmodem ?
failure-string
host
port
style
success-string
suppress
DS$ set vmodem failure-string ?
<text>                    30 characters maximum
DS$ set vmodem failure-string "Vmodem failed" ?
failure-string
host
port
style
success-string
suppress
Or press Enter to confirm command
DS$ set vmodem failure-string "Vmodem failed"
DS$ show vmodem
Host
Host Port
Success String
Failure String            "Vmodem failed"
Suppress                  Off
Style                     Numeric
DS$
```

User Commands

This chapter defines all the CLI commands available to users who are logged into the IOLAN.

Commands for Users Logged Into the IOLAN

Admin

Description Changes a Normal-level user to the Admin user. When you press **Enter** after you type this command, you will be prompted for the Admin password.
User Level Normal
Syntax `admin`

Help

Description Displays help on using the command line interface (CLI).
User Level Restricted, Normal, Admin
Syntax `help`

Line

Description Displays a menu of configured serial ports.
User Level Admin
Syntax `line`

Kill Line

Description Restarts a line. On IOLANs with more than 1 port, you can specify a port number and then a range of ports; for example, `kill line 4, 10-13, 15`. This command can also be used to reset the internal modem on the IOLAN. The internal modem is addressed as last serial port +1 (i.e., on an SDS 3M, the modem is line 4). On single port models, use the command `kill line`.
User Level Admin
Syntax `kill line *|<number>|<number range>`

Note: the `*` is a wildcard meaning all lines.

Kill Session

Description Kills an active session.
User Level Restricted, Normal, Admin
Syntax `kill session 1|2|3|4`
Options **1|2|3|4**

The number of the session you want to kill.

Logout

Description Logs the user out from the IOLAN.
User Level Restricted, Normal, Admin
Syntax **`logout`**

Menu

Description Switches from a command line based interface to Menu mode of operation.
User Level Restricted, Normal, Admin
Syntax **`menu`**

Ping

Description This command checks to see if a given host is reachable via an IP message. The specific message used is called a ping.
User Level Normal, Admin
Syntax **`ping <`***`hostname/IP_address`***`> [<`***`packet_size`***`>] [<`***`#_of_packets`***`>]`**

Options ***<hostname/IP_address>***

The name (DNS resolvable host name) or IP address of the machine you are trying to ping.

<packet_size>

Enter the number of data bytes to be sent. The default is 100 bytes.

<#_of_packets>

Enter the number of the packets you want to send. The default is 10.

Resume

Description Resumes a started session.
User Level Restricted, Normal, Admin
Syntax **`resume 1|2|3|4`**

Options **1|2|3|4**

The number of the session you want to resume.

Rlogin

Description Starts an rlogin session to the specified host/IP address.
User Level Normal, Admin
Syntax **`rlogin <`***`hostname/IP_address`***`> [termtype <`***`terminal_name`***`>] [user <`***`string`***`>]`**

Options **<***hostname/IP_address***>**

The name of the target host.

termtype

Type of terminal attached to this line; for example, ansi or wyse60.

user

The name of the user logging into the rlogin session.

Screen

Description Switches from a command line based interface to Menu mode of operation.
User Level Restricted, Normal, Admin
Syntax **`screen`**

Set Termtype

Description Sets the type of terminal being used for the current session.

User Level Normal, Admin

Syntax

```
set termtype
wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|
term3
```

Option **wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|term3**

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3** (user-defined terminals)

Set User

Description Sets the current users settings.

User Level Normal, Admin

Syntax

```
set user . [hotkey-prefix <00-7f>] [language english|customlang]
[routing none|send|listen|send-and-listen] [password]
```

Options **hotkey-prefix**

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a number**—To switch from one session to another, press **^a** and then the required session number. For example, **^a 2** would switch you to session 2. Pressing **^a 0** will return you to the IOLAN Menu.
- **^a n**—Display the next session. The current session will remain active. The lowest numbered active session will be displayed.
- **^a p**—Display the previous session. The current session will remain active. The highest numbered active session will be displayed.
- **^a m**—To exit a session and return to the IOLAN. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^r**—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always **Ctrl R**, regardless of the **Hotkey Prefix**.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu or CLI. The IOLAN supports one custom language that must be downloaded to the IOLAN; otherwise, **Customlang** defaults to English.

routing

Determines the routing mode used for RIP packets on the PPP and SLIP interfaces for this user. Values are:

- **None**—RIP packets are neither received nor sent by the IOLAN.
- **Send**—RIP packets can only be sent by the IOLAN.
- **Listen**—RIP packets can only be received by the IOLAN.
- **Send and Listen**—RIP packets are sent and received by the IOLAN.

password

The password the user will need to enter to login to the IOLAN. This case-sensitive field accepts a maximum of 16 characters.

Set User Session

Note: Not all SSH encryption options are available on all formware versions.

Description Sets the current users session settings.

User Level Normal, Admin

Syntax

```
set user . session 1|2|3|4|* [auto on|off]
 [type off|telnet|rlogin|ssh]

set user . session 1|2|3|4|* telnet-options [host <config_host>
 <tunnel_name>] [port <TCP_port>] [termtype <terminal_name>]
 [line-mode on|off] [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>]
 [eof <00-7f>] [erase <00-7f>] [intr <00-7f>] [quit <00-7f>]

set user . session 1|2|3|4|* rlogin-options [host <config_host>
 <tunnel_name>] [termtype <terminal_name>]

set user . session 1|2|3|4|* ssh-options [host <config_host>
 <tunnel_name>]
 [port <TCP_port>] [termtype <terminal_name>]
 [protocol ssh-1|ssh-2|ssh-2/1] [compression on|off]
 [verbose on|off] [auto-login on|off] [name <string>]
 [password <string>] [ssh-1-cipher 3des|des|blowfish]
 [authentication rsa on|off] [authentication dsa on|off]
 [authentication keyboard-interactive
 on|off][strict-host-key-checking on|off]

set user . session 1|2|3|4|* ssh-options
 ssh-2-cipher-list <3des blowfish cast aes arcfour>
```

Options

session

Specifies the session number (or all, *) that you are configuring.

auto

Specify whether or not the session(s) will start automatically when the user logs into the IOLAN.

telnet-options

See ***Set Telnet-Client*** in the *IOLAN User's Guide*.

rlogin-options

See ***Set Rlogin-Client*** in the *IOLAN User's Guide*.

ssh-options

See ***Set SSH-Client*** in the *IOLAN User's Guide*.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

strict-host-key-checking

When enabled, a host public key (for each host you wish to SSH to) must be downloaded into the IOAN.

Default: Enabled

Show Line Users

Description Shows the users who are on the line.
User Level Admin
Syntax **`show line <number> users`**

SSH

Note: Not all SSH encryption options are available on all formware versions.

Description Starts an SSH session to the specified host/IP address.
User Level Normal, Admin
Syntax

```
ssh <hostname/IP_address> [<TCP_port>]
 [termtype <terminal_name>] [authentication rsa on|off]
 [authentication dsa on|off]
 [authentication keyboard-interactive on|off]
 [compression on|off] [protocol ssh-1|ssh-2|ssh-2,1]
 [ssh-1-cipher 3des|des|blowfish]
 [ssh-2-cipher-list <3des blowfish cast aes arcfour> end-list]
 [user <name>] [verbose on|off]
```

Options <*hostname/IP_address*>

The name (resolvable via DNS) or IP address of the host you wish to connect to with SSH.

<*TCP_port*>

The port number the target host is listening on for incoming connections. The default for SSH is port number 22.

termtype

Type of terminal attached to this line; for example, ANSI or WYSE60.

authentication rsa

An authentication method used by SSH version 1 and 2. When enabled, an SSH client session will try to authenticate via RSA.

authentication dsa

An authentication method used by SSH version 2. When enabled, an SSH client session will try to authenticate via DSA.

authentication keyboard-interaction

The user types in a password for authentication.Used for SSH2 only.

compression

Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks.

protocol

Specify whether you are using SSH-1, SSH-2, or a combination of the two protocols, SSH-2, SSH-1.

ssh-1-cipher

Select the encryption method (cipher) that you want to use for your SSH version 1 connection:

- **3DES**
- **Blowfish**

ssh-2-cipher-list

Select the order of negotiation for the encryption method (ciphers) that the IOLAN will use for the SSH version 2 connection:

- **3DES**
- **Blowfish**
- **AES**
- **Arcfour**
- **CAST**

user

The name of the user logging into the SSH session.

verbose

Displays debug messages on the terminal.

Syslog Console

Description Starts/stops or displays the status of the syslog console.
User Level Admin
Syntax

```
syslog console start|stop

syslog console status
```

Options **start|stop**

Start or stop console logging. When console logging is enabled, syslog messages will be echoed to the current console. These messages are filtered based on the level set in the (remote) syslog options.

status

Displays the current console logging status (enabled or disabled).

Show Sessions

Description Shows available sessions.
User Level Restricted, Normal, Admin
Syntax

```
show sessions
```

Show Termtype

Description Shows the terminal type for the current session.
User Level Admin

Syntax `show termtype`

Start

Description Starts a predefined session. Only inactive sessions are displayed.
User Level Restricted, Normal, Admin
Syntax `start 1|2|3|4`

Options **1|2|3|4**

The number of the session that you want to start.

Telnet

Description Starts a telnet session to the specified host/IP address.
User Level Normal, Admin
Syntax

```
telnet <hostname/IP_address> [<TCP_port>]
 [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>] [eof <00-7f>] [erase <00-7f>] [intr <00-7f>]
 [quit <00-7f>] [escape <00-7f>]
```

Options ***<hostname/IP_address>***

The name (resolvable via DNS) or IP address of the host you wish to connect to with Telnet.

<TCP_port>

The port number the target host is listening on for incoming connections. The default for Telnet is port number 23.

termtype

Type of terminal attached to this line; for example, ANSI or WYSE60.

line-mode

When **On**, keyboard input is not sent to the remote host until **Enter** is pressed, otherwise input is sent every time a key is pressed. Default is **Off**.

map-cr-crlf

Maps carriage returns (CR) to carriage return line feed (CRLF). The default value is **Off**.

local-echo

Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can only be used when **Line Mode** is **On**. Default is **Off**.

echo

Defines the echo character. When **Line Mode** is **On**, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal with a default value of **5** (ASCII value **^E**).

eof

Defines the end-of-file character. When **Line Mode** is **On**, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal with a default value of **4** (ASCII value **^D**).

erase

Defines the erase character. When **Line Mode** is **Off**, typing the erase character erases one character. This value is in hexadecimal with a default value of **8** (ASCII value **^H**).

intr

Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of **3** (ASCII value **^C**).

quit

Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal with a default value of **1c** (ASCII value **FS**).

escape

Defines the escape character. Returns you to the command line mode. This value is in hexadecimal with a default value of **1d** (ASCII value **GS**).

Version

Description Displays firmware version and build.
User Level Normal, Admin
Syntax `version`

Configuring Users

Add User

Description For units with 4 or less serial ports, you can configure up to 4 users. For units with 8 or more serial ports, the maximum number of users which can be added is 48. This is in addition to the **admin** user.
User Level Admin
Syntax **add user <***username***>**

Option ***<username>***

The name of the user, without spaces. When you finish the command and press Enter, you will be prompted to enter and re-enter a password for the user.

Delete User

Description Deletes a user.
User Level Admin
Syntax **delete user <***config_user***>**

Option ***<config_user>***

You can see a list of users that can be deleted by typing **delete user ?**. You can not delete the **admin** user.

Set Default User

Description Configures the Default User. When adding a new user, the profile of the default user will be used to assign the values of the various parameters of the new user. For example if you set the **service** parameter of the default user to **ppp**, when a new user is added, their service parameter will be set to **ppp**.

User Level Admin

Syntax

```
set default user [callback on|off] [framed-compression on|off]
[framed-ip <IPv4_address>]
[framed-interface-id <IPv6_interface_id>]
[framed-mtu <64-1500>] [hotkey-prefix <00-7f>]
[idle-timer <0-4294967>]
[host-ip None|<IP_address>|<config_host>]
[language english|customlang]
[level admin|normal|restricted|menu]
[line-access readin|readout|readwrite [on|off]|<line(s)> [0]]
[netmask <IPv4_address>] [phone-number <phone_number>]
[routing none|send|listen|send-and-listen]
[service dsprompt|telnet|tcp-clear|rlogin|ppp|slip|ssh|ssl-raw]
[sess-timer <0-4294967>] [port tcp-clear|telnet|ssh|ssl-raw
<TCP_port>] [access-clustered-ports on|off]
```

Options

callback

When **On**, enter a phone number for the IOLAN to call the user back (the **Callback** parameter is unrelated to the **Line Dial** parameter).

Note: the IOLAN will allow callback only when a user is authenticated. If the protocol over the link does not provide authentication, there will be no callback. Therefore, when the **Line Service** is set to **PPP**, you must use either **PAP** or **CHAP**, because these protocols provide authentication. The default is **Off**.

The IOLAN supports another type of callback, **Roaming Callback**, which is configurable when the **Line Service** is set to **PPP**.

framed-compression

Used for **User Service PPP** or **SLIP**, determines whether Van Jacobsen Compression is used on the link. VJ compression is a means of reducing the standard TCP/IP header from 40 octets to approximately 5 octets. This gives a significant performance improvement, particularly when interactive applications are being used. For example, when the user is typing, a single character can be passed over the link with a packet as small as 5 octets as opposed to 40 octets when no JV compression is used. VJ Compression has little effect on other types of links, such as ftp, where the packets are much larger. The **Framed Compression** value will be used in preference to the **VJ Compression** value set for a **Line**. The default is **Off**.

framed-ip

Used for **User Service PPP** or **SLIP**, sets the IP address of the remote user. Enter the address in dot decimal notation as follows:

- **255.255.255.254** (default)—The IOLAN will use the **Remote IP Address** set in the **PPP** settings for the line.
- **255.255.255.255**—When the **User Service** is **PPP**, the IOLAN will allow the remote machine to specify its IP address (overriding the Remote IP Address configured in the line, **PPP** settings). When the **User Service** is **SLIP**, the IOLAN will use the **Remote IP Address** set for the line (no negotiation).
- **n.n.n.n**—(where **n** is a number) Enter the IP address of your choice. This IP address will then be used in preference to the **Remote IP Address** set for a line.

framed-interface-id

Used for **User Service PPP**, sets the IPv6 address of the remote user.

framed-mtu

Used for **User Service PPP** or **SLIP**, specifies the maximum size of packets, in bytes, being transferred across the link. On noisy links it might be preferable to fragment large packets being transferred over the link, since there will be quicker recovery from errors. Depending on whether you have selected a **User Service** of **SLIP** or **PPP**, details are as follows:

- **PPP**—**Framed MTU** will be the maximum size of packets that the IOLAN port will accept. This value is negotiated between the two ends of the link. The valid range is 64-1500. The default value is **1500** bytes.
- **SLIP**—**Framed MTU** will be the maximum size of packets being sent by the IOLAN. The IOLAN will send SLIP packets in the range 256-1500 bytes. The default value is **256** bytes.

The **Framed MTU** value will be used in preference to the **MTU**/**MRU** values set for a **Line**.

hotkey-prefix

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a number**—To switch from one session to another, press **^a** and then the required session number. For example, **^a 2** would switch you to session 2. Pressing **^a 0** will return you to the IOLAN Menu.
- **^a n**—Display the next session. The current session will remain active. The lowest numbered active session will be displayed.
- **^a p**—Display the previous session. The current session will remain active. The highest numbered active session will be displayed.
- **^a m**—To exit a session and return to the IOLAN. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^r**—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always **Ctrl R**, regardless of the **Hotkey Prefix**.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

idle-timer

The amount of time, in seconds, that the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, because there has been no exchange of data within the specified time, the IOLAN will close the connection. The default value is **0** (zero), meaning that the **Idle Timer** will not expire (the connection is open permanently). The maximum value is 4294967 seconds. The **User Idle Timer** will override the **Line Idle Timer**, with the exception of **reverse SSH** or reverse Telnet sessions.

host-ip

For outbound User Services such as **Telnet**, **Rlogin**, or **SSH**, this is the target host name or IP address. If no IP address is specified, the **Host IP** value in the **Default User** configuration will be used. The default is **0.0.0.0**. or None.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu or CLI. The IOLAN supports one custom language that must be downloaded to the IOLAN; otherwise, **Customlang** defaults to English.

level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the IOLAN. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the IOLAN.
- **Normal**—The Normal level user has limited access to the IOLAN. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings.
- **Restricted**—The Restricted level user can only access predefined sessions or access the Easy Port Access menu.
- **Menu**—The menu level user will only be able to access predefined session or access the Easy Port Access menu. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the IOLAN. Does not have any access to CLI commands.

netmask

This is used for the PPP or SLIP Service types. Only used for IPv4. If the remote user is on a subnet, enter the network's subnet mask. For example, a subnet mask of 255.255.0.0.

line-access

Specifies the user access rights to each IOLAN device line. Options are:

- **Read/Write**—Users are given read and write access to the line.
- **Read In**—Users are given access to read only outbound data, data that is going from the IOLAN to the device.
- **Read Out**—Users are given access to read only inbound data, data that is going from the device to the IOLAN.

Users can read data going in both directions by selecting both the **Read In** and **Read Out** options. The `on|off` option is only for 1-port models. You can disable line access in 2-port + models by specifying `0` (zero).

phone-number

The phone number the IOLAN will dial to callback the user (you must have set **Callback** to **On**). Enter the number without spaces. To change the phone number, overwrite the previous entry; to clear the phone number, set it to **""** (double quotes without a space).

routing

Determines the routing mode used for RIP packets on the PPP and SLIP interfaces for this user. Values are:

- **None**—RIP packets are neither received nor sent by the IOLAN.
- **Send**—RIP packets can only be sent by the IOLAN.
- **Listen**—RIP packets can only be received by the IOLAN.
- **Send and Listen**—RIP packets are sent and received by the IOLAN.

service

The type of service that the user will use.

sess-timer

The amount of time, in seconds, that the **Session Timer** will run. Use this timer to forcibly close a user's session (connection). When the **Session Timer** expires, the IOLAN will end the connection. The default value is **0** (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds. The **User Session Timer** will override the **Line Session Timer**, with the exception of **reverse SSH** or reverse Telnet sessions.

port

.For outbound User Services such as **Telnet**, **SSH**, **TCP clear** or **SSL raw**, this is the target port number. The default value will change based on the type of **Service** selected; the most common known port numbers are used as the default values.

access-clustered-ports

When enabled, allows the user access to IOLANs that have been configured in the clustering group. The default is on.

Set User

Description Sets users settings. Normal-level users can configure only their own settings. Admin-level users can configure any users settings, including their own (with the exception of their User Level, which must stay at Admin).

User Level Normal, Admin

Syntax

```
set user . [hotkey-prefix <00-7f>] [language english|customlang]
 [password] [routing none|send|listen|send-and-listen]
```

Admin User Only

```
set user .|<username>|* [callback on|off]
 [framed-compression on|off] [framed-ip <IPv4_address>]
 [framed-interface-id <IPv6_interface_id>]
 [framed-mtu <64-1500>] [hotkey-prefix <00-7f>]
 [idle-timer <0-4294967>]
 [host-ip None|<IP_address>|<config_host> <tunnel_name>]
 [language english|customlang]
 [level admin|normal|restricted|menu] [password]
 [line-access readin|readout|readwrite [on|off]|<line(s)> [0]]
 [netmask <IPv4_address>] [phone-number <phone_number>]
 [routing none|send|listen|send-and-listen]
 [service dsprompt|telnet|tcp-clear|rlogin|ppp|slip|ssh|ssl-raw]
 [sess-timer <0-4294967>] [port tcp-clear|telnet|ssh|ssl-raw
 <TCP_port>] [access-clustered-ports on|off]
```

Options

callback

When **On**, enter a phone number for the IOLAN to call the user back (the **Callback** parameter is unrelated to the **Line Dial** parameter).

Note: the IOLAN will allow callback only when a user is authenticated. If the protocol over the link does not provide authentication, there will be no callback. Therefore, when the **Line Service** is set to **PPP**, you must use either **PAP** or **CHAP**, because these protocols provide authentication. The default is **Off**.

The IOLAN supports another type of callback, **Roaming Callback**, which is configurable when the **Line Service** is set to **PPP**.

framed-compression

Used for **User Service PPP** or **SLIP**, determines whether Van Jacobsen Compression is used on the link. VJ compression is a means of reducing the standard TCP/IP header from 40 octets to approximately 5 octets. This gives a significant performance improvement, particularly when interactive applications are being used. For example, when the user is typing, a single character can be passed over the link with a packet as small as 5 octets as opposed to 40 octets when no JV compression is used. VJ Compression has little effect on other types of links, such as ftp, where the packets are much larger. The **Framed Compression** value will be used in preference to the **VJ Compression** value set for a **Line**. The default is **Off**.

framed-ip

Used for **User Service PPP** or **SLIP**, sets the IP address of the remote user. Enter the address in dot decimal notation as follows:

- **255.255.255.254** (default)—The IOLAN will use the **Remote IP Address** set in the **PPP** settings for the line.
- **255.255.255.255**—When the **User Service** is **PPP**, the IOLAN will allow the remote machine to specify its IP address (overriding the Remote IP Address configured in the line, **PPP** settings). When the **User Service** is **SLIP**, the IOLAN will use the **Remote IP Address** set for the line (no negotiation).
- **n.n.n.n**—(where **n** is a number) Enter the IP address of your choice. This IP address will then be used in preference to the **Remote IP Address** set for a line.

framed-interface-id

Used for **User Service PPP**, sets the IPv6 address of the remote user.

framed-mtu

Used for **User Service PPP** or **SLIP**, specifies the maximum size of packets, in bytes, being transferred across the link. On noisy links it might be preferable to fragment large packets being transferred over the link, since there will be quicker recovery from errors. Depending on whether you have selected a **User Service** of **SLIP** or **PPP**, details are as follows:

- **PPP**—**Framed MTU** will be the maximum size of packets that the IOLAN port will accept. This value is negotiated between the two ends of the link. The valid range is 64-1500. The default value is **1500** bytes.
- **SLIP**—**Framed MTU** will be the maximum size of packets being sent by the IOLAN. The IOLAN will send SLIP packets in the range 256-1500 bytes. The default value is **256** bytes.

The **Framed MTU** value will be used in preference to the **MTU**/**MRU** values set for a **Line**.

hotkey-prefix

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a number**—To switch from one session to another, press **^a** and then the required session number. For example, **^a 2** would switch you to session 2. Pressing **^a 0** will return you to the IOLAN Menu.
- **^a n**—Display the next session. The current session will remain active. The lowest numbered active session will be displayed.
- **^a p**—Display the previous session. The current session will remain active. The highest numbered active session will be displayed.
- **^a m**—To exit a session and return to the IOLAN. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^r**—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always **Ctrl R**, regardless of the **Hotkey Prefix**.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

idle-timer

The amount of time, in seconds, that the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, because there has been no exchange of data within the specified time, the IOLAN will close the connection. The default value is **0** (zero), meaning that the **Idle Timer** will not expire (the connection is open permanently). The maximum value is 4294967 seconds. The **User Idle Timer** will override the **Line Idle Timer**, with the exception of **reverse SSH** or reverse Telnet sessions.

host-ip

For outbound User Services such as **Telnet**, **Rlogin**, or **SSH**, this is the target host name or IP address. If no IP address is specified, the **Host IP** value in the **Default User** configuration will be used. The default is **0.0.0.0**. or None.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu or CLI. The IOLAN supports one custom language that must be downloaded to the IOLAN; otherwise, **Customlang** defaults to English.

level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the IOLAN. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the IOLAN.
- **Normal**—The Normal level user has limited access to the IOLAN. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings.
- **Restricted**—The Restricted level user can only access predefined sessions or access the Easy Port Access menu.
- **Menu**—The menu level user will only be able to access predefined session or access the Easy Port Access menu. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the IOLAN. Does not have any access to CLI commands.

netmask

This is used for the PPP or SLIP Service types. Only used for IPv4. If the remote user is on a subnet, enter the network's subnet mask. For example, a subnet mask of 255.255.0.0.

password

The password the user will need to enter to login to the IOLAN. This case-sensitive field accepts a maximum of 16 characters.

line-access

Specifies the user access rights to each IOLAN device line. Options are:

- **Read/Write**—Users are given read and write access to the line.
- **Read In**—Users are given access to read only outbound data, data that is going from the IOLAN to the device.
- **Read Out**—Users are given access to read only inbound data, data that is going from the device to the IOLAN.

Users can read data going in both directions by selecting both the **Read In** and **Read Out** options. The `on|off` option is only for 1-port models. You can disable line access in 2-port + models by specifying `0` (zero).

phone-number

The phone number the IOLAN will dial to callback the user (you must have set **Callback** to **On**). Enter the number without spaces. To change the phone number, overwrite the previous entry; to clear the phone number, set it to **""** (double quotes without a space).

routing

Determines the routing mode used for RIP packets on the PPP and SLIP interfaces for this user. Values are:

- **None**—RIP packets are neither received nor sent by the IOLAN.
- **Send**—RIP packets can only be sent by the IOLAN.
- **Listen**—RIP packets can only be received by the IOLAN.
- **Send and Listen**—RIP packets are sent and received by the IOLAN.

service

The type of service that the user will use.

sess-timer

The amount of time, in seconds, that the **Session Timer** will run. Use this timer to forcibly close a user's session (connection). When the **Session Timer** expires, the IOLAN will end the connection. The default value is **0** (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds. The **User Session Timer** will override the **Line Session Timer**, with the exception of **reverse SSH** or reverse Telnet sessions.

port

.For outbound User Services such as **Telnet**, **SSH**, **TCP clear** or **SSL raw**, this is the target port number. The default value will change based on the type of **Service** selected; the most common known port numbers are used as the default values.

access-clustered-ports

When enabled, allows the user access to IOLANs that have been configured in the clustering group. The default is on.

Set User Session

Description Configures a users session settings. See ***Set User Session*** for a description of the options.

User Level Admin

Syntax

```
set user .|<username>|* session 1|2|3|4|* [auto on|off]
 [type off|telnet|rlogin|ssh]

set user .|<username>|* session 1|2|3|4|* telnet-options
 [host <config_host>] [port <TCP_port>]
 [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>] [eof <00-7f>] [erase <00-7f>] [intr <00-7f>]
 [quit <00-7f>]

set user .|<username>|* session 1|2|3|4|* rlogin-options
 [host <config_host>] [termtype <terminal_name>]

set user .|<username>|* session 1|2|3|4|*
 ssh-options [host <config_host>] [port <TCP_port>]
 [termtype <terminal_name>] [protocol ssh-1|ssh-2|ssh-2/1]
 [compression on|off] [verbose on|off] [auto-login on|off]
 [name <string>] [password <string>]
 [ssh-1-cipher 3des|des|blowfish] [authentication rsa on|off]
 [authentication password on|off]
 [authentication keyboard-interactive on|off]

set user .|<username>|* session 1|2|3|4|* ssh-options
 ssh-2-cipher-list <3des blowfish cast aes arcfour>
```

Show Default User

Description Shows the Default Users settings.

User Level Admin

Syntax

```
show default user
```

Show User

Description Shows user configuration settings.

User Level Admin

Syntax **show user <***configured_user***>|.**

Options ***<configured_user>***

Show the settings for the specified user.

Show the settings for the current user.

Server Commands

This chapter defines all the CLI commands associated with configuring the IOLAN server parameters.

Server Commands

Set Console

Description Sets the flow control and baud rate on IOLAN models that have a dedicated console port.

User Level Admin

Syntax

```
set console [flow none|soft|hard]
 [speed 9600|19200|38400|57600|115200]
```

Options

flow

For IOLAN models that have a dedicated console port, defines whether the data flow is handled by using software (**Soft**), hardware (**Hard**), or no (**None**) flow control.

speed

For IOLAN models that have a dedicated console port, specifies the baud rate of the line connected to the console port.

Set Custom-App

Description You can create a custom application that can run on the IOLAN using the Perle SDK.

User Level Admin

Syntax

```
set custom-app server program-command-line <command>
```

Options

program-command-line

The name of the SDK program executable that has been already been downloaded to the IOLAN, plus any parameters you want to pass to the program. Maximum of 80 characters. Use the **`shell`** CLI command as described in the *SDK Programmer's Guide* to manage the files that you have downloaded to the IOLAN. For example, using sample **`outraw`** program, you would type:

```
outraw -s 0 192.168.2.1:10001 Acct:10001
```

if you were starting the application on the Server (notice the **`-s 0`** parameter specifies Line 1).

Set Port-Buffering

Description Configures port buffering.

User Level Admin

Syntax

```
set port-buffering [syslog on|off]
 [keys-stroke-buffering on|off] [mode off|local|remote|both]
 [nfs-directory <text>] [nfs-encryption on|off]
 [nfs-host <config_host> [<tunnel_name>] [time-stamp on|off]
 [view-port-buffer-string <text>]
```

Options

duplicate-nfs-to-syslog

When enabled, buffered data is sent to the syslog host to be viewed on the host's monitor. The default is off.

key-stroke-buffering

When enabled, key strokes that are sent from the network host to the serial device on the IOLAN's serial port are buffered. The default is off.

mode

Specifies where the port buffer log is kept, either **Off**, **Local**, **Remote**, or **Both**. If **Remote** or **Both** is selected, you must specify an NFS server location for the port buffer log.

nfs-directory

The directory and/or subdirectories where the **Remote Port Buffering** files will be created. This field is used when Port Buffering **Mode** is set to **Remote** or **Both**. For multiple IOLANs using the same NFS host, it is recommended that each IOLAN have its own unique directory to house the remote port log files. The default is **`/device_server/portlogs`**.

nfs-encryption

Determines if the data sent to the NFS host is sent encrypted or in the clear across the LAN. The default is set of **Off**.

NOTE: When NFS encryption is enabled, the Decoder utility software is required to be installed on the NFS host for decrypting the data to a readable format. The Decoder utility software can be found on the installation CD-ROM and on the **`www.perle.com`** website.

nfs-host

The NFS host that the IOLAN will use for its **Remote Port Buffering** feature. The IOLAN will open a file on the NFS host for each reverse SSH or reverse Telnet line, and send any port data to be written to those files. The default is **None**. This field is required when **Mode** is set to **Remote** or **Both**.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

time-stamp

Enable/disable time stamping of the port buffer data.

view-port-buffer-string

The string (up to 8 characters) used by a a session connected to a serial port to display the port buffer for that particular serial port. You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, **Escape b** is **<027>b**). The default is **~view**.

Set Server

Description Sets server parameters.
User Level Admin
Syntax

```
set server [active-standby on|off]
set server [auto-obtain-dns on|off] [auto-obtain-gw on|off]
 [auto-obtain-wins on|off]
[set server banner on|off]
set server [break on|off]
set server [bypass-password on|off]
set server [dhcp-update-dns on|off]
set server [data-logging-buffer-size <integer>]
set server [domain <string>]
set server [flush-on-close on|off]
set server [generic-web-login on|off]
set server [incoming-pings enabled|disabled]
set server internet [eth1|eth2] <IPV4_address> [netmask]
set server internet [eth1|eth2] dhcp/bootp on dhcp-update-dns on
 domain-prefix <text>
set server internet [eth1|eth2] dhcp/bootp on dhcp-update-dns off
set server internet [eth1|eth2] mtu <integer>
set server internet [eth1|eth2] dhcp/bootp off <IPV4_address>
 [<netmask>]
set server [ip-filter on|off]
set server [ip-filter-end-address <IPV4_address>]
set server [ip-filter-range on|off]
set server [ip-filter-start-address <IPV4_address>]
set server [line-menu-string <string>]
set server [miimon <milliseconds>]
set server [monitor-connection-every <seconds>]
set server [monitor-connection-number<integer>]
set server [monitor-connection-timeout <seconds>]
set server [name <string>]
set server [oem-login on|off]
set server [password-limit <0-10>]
set server [power-management-menu-string <string>]
set server [pre-v4.3g-data-logging on|off]
set server [prompt-with-name on|off]
set server [session-escape-string <string>]
set server [single-telnet on|off]
set server [netmask <IPV4_address>]
set server [ssl-passphrase <string>]
set server tftp [retry <integer>] [timeout <integer>]
set server [updelay <milliseconds>]

set server [udp-always-arp on|off] (available on one port models)
```

Options

auto-obtain-dns

When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the DNS IP address from the DHCP/BOOTP server.

auto-obtain-gw

When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the Default Gateway IP address from the DHCP/BOOTP server.

auto-obtain-wins

When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the WINS IP address from the DHCP/BOOTP server.

banner

This parameter concerns the banner information (product name/software version). This banner information is presented to a user with a login prompt. For security reasons, you can turn off the display of this information. The default is **Off**.

break

Enables/disables proprietary inband SSH break signal processing as well as the existing Reverse Telnet break signal. This parameter can also enable/disable the out-of-band break signals for TruePort. The default value is **Off**.

bypass-password

When set, authorised users who do not have a password set, with the exception of the Admin user, WILL NOT be prompted for a password at login with **Local Authentication**.

dhcp-update-dns

The DHCP server will update the DNS server when the IOLAN requests a DHCP IP address (the communication between the DNS server and the DHCP server must already be set up in your network).

dhcp/bootp

Enables the DHCP/BOOTP client process in the IOLAN. By default, this is disabled/off. If this is enabled, the server IP address parameter is disabled.

domain

Unique name for your domain, your location in the global network. Like Hostname, it is a symbolic, rather than a numerical, identifier.

domain-prefix

(SCS models only) A domain prefix to uniquely identify the Ethernet interface to the DNS when the IOLAN has two Ethernet interfaces. The format of the Ethernet interface will take the form of <*Server Name*>.<*Domain Prefix*>.<*Domain Name*> or <*Server Name*>.<*Domain Prefix*>, depending on what is configured.

flush-on-close

When enabled, deletes any pending outbound data when a port is closed; as opposed to maintaining the port to send pending data. The default value is **Off**.

internet

The IOLAN's unique IPv4 network IP address. If you are using the IOLAN in an IPv6 network, use the **`set ipv`**6 command.

incoming-pings

The IOLAN will respond to incoming pings. (Available only on the FIPS version of firmware)

Default: Enabled

internet [eth1|eth2]

Dual Ethernet SCS models require that you specify which Ethernet connection you are setting, either **eth1** or **eth2**.

mtu

The Maximum Transmission Unit (MTU) size of an IP frame that will be sent over the network. If your IOLAN has more then one interface, each of the interfaces can be set separately, however only one MTU size can be set for both IPv4 and IPv6 frames.

MTU sizes: 68-1500 bytes

Default size: 1500 bytes

name

You must supply a name for the IOLAN.

netmask

The network subnet mask. For example, 255.255.0.0.

line-menu-string

The string used to access to the Easy Port Access menu without disconnecting the initial reverse SSH or reverse Telnet session.The default string is **~menu**.

monitor-connection-every

Specify how often, in seconds, the IOLAN will send a TCP keepalive. This only applies to line service types that support the keepalive feature.

Default Interval: 180 seconds

monitor-connection-timeout

Sets the maximum time to wait for a response after sending a TCP keepalive message.

Values: 1-32767 seconds

Default: 5 seconds

monitor-connection-number

The number of TCP keepalive retries before the connection is closed.

Values: 1-32767

Default: 5

oem-login

When set, and a custom language file is in use, the login prompt will use the string defined in the language file as the login prompt instead of the default prompt, **`login:`**.

password-limit

The number of attempts a user is allowed to enter a password for a serial port connection from the network, before the connection is terminated and the user has to attempt to login again. For users logging into the serial port, if this limit is exceeded, the serial port is disabled for 5 minutes. A user with Admin level rights can restart the serial port, bypassing the timeout, by issuing a kill on the disabled serial port. The default value is **3**.

prompt-with-name

Displays the **Server Name** field value instead of default product name. When enabled, the **Server Name** is displayed in the IOLAN login prompt, CLI prompt, WebManager login screen, and the heading of the Menu. The default value is **Off**.

ip-filter

A security feature that when enabled, the IOLAN will only accept data from hosts configured in the IOLAN's **Host Table** with an IP address (hosts configured with a Fully Qualified Domain Name, FQDN, will not be able to access the IOLAN when this option is enabled). The default value is **Off**.

ip-filter-end-address

Set the end IPv4 address for the filter.

ip-filter-range

A security feature that when enabled, the IOLAN will only accept data from or send data to hosts configured within this IPv4 address range. The default value is **Off**

ip-filter-start-address

Set the start IPv4 address for the filter.

single-telnet

Sets all reverse connections (raw, SSH, and telnet) to a one connection at a time mode. In this mode of operation, the IOLAN will only allow for a single TCP connection at a time to exist for each serial port configured for a reverse connection type. Subsequent connection attempts will be refused until all of the following conditions are met:

- No active connection to serial port exists and at least 1 second has passed since the last connection was terminated.
- All data from the previous connection on the serial port has been transmitted.

The IOLAN has logic to automatically detect when a reverse connection is no longer active. When this happens, the connection is reset and the server can go back to a listening for an incoming connection state.

Applications using Single Telnet need to be aware that there can be some considerable delay between a network disconnection and the port being available for the next connection attempt; this is to allow any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature. The default value is **Off**.

active-standby

(SCS only) Enables/disables the feature of automatically assigning the Ethernet 1 IP address to Ethernet 2 if Ethernet 1 should fail to communicate to the network.

miimon

(SCS only) The interval in which the active interface is checked to see if it is still communicating. The default is 100 ms.

updelay

(SCS only) The time that the IOLAN will wait to make the secondary interface (Ethernet 2) active after it has been detected as up.

power-management-menu-string

Users accessing the IOLAN through reverse sessions can enter the string to bring up a power bar management menu. This string can be up to 8 characters. Control characters can be specified by putting their decimal value within angled brackets. The default value is **<016>** or **Ctrl-p** on the keyboard.

data-logging-buffer-size

The minimum data buffer size for all models is 1 KB. The maximum data buffer size is 2000 KB for DS1/TS/STS8D models, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.

Data logging is only valid for Trueport and TCP Sockets profiles.

Values: 1-2000 KB (DS1/TS1/STS8D)

Values: 1-4000 KB (all other models)

Default Buffer Size: 4 KB (DS1/TS1/STS8D)

Default Buffer Size: 256 KB (all other models)

pre-v4.3g-data-logging

Enable the data logging feature previous to V4.3 firmware.

Default: Disabled

udp-always-arp

This controls whether the IOLAN will attempt an ARP each time there is data to be transmitted and the ARP table does not have a valid ARP entry for the destination. When set to "off", a new ARP will only be attempted after a timeout period. Any data to be sent before the timeout elapses, will be silently discarded.

Default: Off

session-escape-string

A configurable string that allows access to a port to view the multisession screen options, allowing the various options while accessing the particular port on the IOLAN. You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, **ESC-b** is **<027>b**). The default value is **Ctrl-z s** (**<026>s** in decimal).

retry

The number of times the IOLAN will retry to transmit a TPFT packet to/from a host when no response is received. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the IOLAN will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the IOLAN will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

ssl-passphrase

This is the SSL/TLS passphrase used to generate an encrypted RSA/DSA private key. This private key and passphrase are required for both HTTPS and SSL/TLS connections, unless an unencrpyted private key was generated, then the SSL passphrase is not required. Make sure that you download the SSL private key and certificate if you are using the secure HTTP option (HTTPS) or SSL/TLS. If both RSA and DSA private keys are downloaded to the IOLAN, they need to be generated using the same SSL passphrase for both to work.

Set SSL Server

Description Sets the default SSL/TLS parameters for the server.
User Level Admin

Syntax

```
set ssl server [version any|tslv1|sslv3] [type client|server]
 [verify-peer on|off]
 [validation-criteria
   country <code>|state-province <text>|locality <text>
   |organisation <text>|organisation-unit <text>
   |common-name <text>|email <email_addr>]
```

Options

version

Specify whether you want to use:

- **Any**—The IOLAN will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try an SSLv2 connection.
- **TLSv1**—The connection will use only TLSv1.
- **SSLv3**—The connection will use only SSLv3.

The default is **Any**.

type

Specify whether the IOLAN will act as an SSL/TLS client or server. The default is **Client**.

verify-peer

Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.

validation-criteria

Any values that are entered in the validation criteria must match the peer certificate for an SSL connection; any fields left blank will not be validated against the peer certificate.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

Set Service

Description Sets server service parameters.

User Level Admin

Syntax

```
set service [routed on|off] [telnetd on|off] [sshd on|off]
 [httpd on|off] [snmpd on|off] [spcd on|off] [sntp on|off]
 [httpsd on|off] [syslog on|off] [dmgrd on|off] [modbusd on|off]
 [ipsec on|off]
```

Options

routed

Route daemon process in the IOLAN on port 520/521.

telnetd

Telnet daemon process in the IOLAN on port 23.

sshd

SSH daemon process in the IOLAN on port 22.

httpd

HTTP daemon process in the IOLAN on port 80.

snmpd

SNMP daemon process in the IOLAN on port 161.

spcd

SPC (TruePort) daemon process in the IOLAN that supports TruePort Full Mode on UDP port 668. You can still communicate with the IOLAN in Lite Mode when this service is disabled.

sntp

Simple Network Time Protocol client process in the IOLAN.

httpsd

Secure HTTP daemon process in the IOLAN on port 443.

syslog

Syslog client process in the IOLAN.

dmgrd

DeviceManager daemon process in the IOLAN. If you disable this service, you will not be able to connect to the IOLAN with the DeviceManager application. DeviceManagerD listens on port 33812 and sends on port 33813.

modbusd

Modbus daemon process in the IOLAN on port 502.

ipsec

IPsec daemon process in the IOLAN listening and sending on UDP port 500. This is disabled by default.

Set Web Manager

Description Sets Web Manager caching on or off.
User Level Admin
Syntax `set web-manager disable caching [on|off]`

Show Console

Description For IOLAN models that have a dedicated console port, this command displays the configured parameters of the console port.
User Level Admin
Syntax `show console`

Show Custom-App

Description Shows the custom application server settings.
User Level Admin
Syntax `show custom-app server`

Show Server

Description Shows the parameters set for the server.
User Level Admin, Normal
Syntax `show server`

Show Port-Buffering

Description Shows the port buffering settings.
User Level Normal, Admin
Syntax `show port-buffering`

Show Modbus

Description Shows the Modbus settings for the gateway.
User Level Normal, Admin
Syntax `show modbus gateway`

Show Web-Manager

Description Shows Web Manager caching
User Level Admin
Syntax `show web-manager`

Hardware Commands

Set Ethernet

Description Sets the hardware configuration for the Ethernet port(s).
User Level Admin
Syntax
```
set ethernet [eth1|eth2] speed-and-duplex
 auto|10-half|10-full|100-half|100-full|1000-full
```

Options **eth1|eth2**

You must specify the Ethernet interface if you have an SCS model with dual Ethernet.

auto|10-half|10-full|100-half|100-full|1000-full

Define the Ethernet connection speed at one of the following (desktop models don't support 1000 Mbps):

- **auto**—automatically detects the Ethernet interface speed and duplex
- **10 Mbps Half Duplex**
- **10 Mbps Full Duplex**
- **100 Mbps Half Duplex**
- **100 Mbps Full Duplex**
- **1000 Mbps Full Duplex**

Show Hardware

Description Shows the hardware resources, Ethernet link status, date and time.
User Level Normal, Admin
Syntax
```
show hardware
```

SSH Server Commands

Set SSH-Server

Note: Not all SSL/TLS encryption options are available on all firmware versions.

See ***Keys and Certificates*** in the *IOLAN User's Guide* for information about the keys and certificates that need to be uploaded or downloaded with the IOLANs SSH server.

Description Configures the IOLANs SSH server.
User Level Admin
Syntax
```
set ssh-server [authentication rsa on|off]
 [authentication dsa on|off] [authentication password on|off]
 [authentication keyboard-interactive on|off]
 [break-string <text>] [compression on|off] [ssh1 on|off]
 [verbose on|off][login-timeout <seconds>]

set ssh-server cipher [3des on|off] [blowfish on|off]
 [cast on|off] [aes on|off] [arcfour on|off]
```

Options **authentication rsa**

An authentication method used by SSH version 1 and 2. Use RSA authentication for the SSH session.

authentication dsa

An authentication method used by SSH version 2. Use DSA authentication for the SSH session.

authentication password

The user types in a password for authentication.

authentication keyboard-interactive

The user types in a password for authentication.Used for SSH2 only.

compression

Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks.

verbose

Displays debug messages on the terminal.

break-string

The break string used for inband SSH break signal processing. A break signal is generated on a specific serial port only when the server's break option is enabled and the user currently connected using reverse SSH has typed the break string exactly. The default is set to **~break**, where **~** is tilde; the break string can be up to eight characters.

ssh1

Allows the user's client to negotiate an SSH-1 connection, in addition to SSH-2.

cipher

Specify which ciphers the IOLAN's SSH server can use to negotiate data encryption with an SSH client session.

login-timeout

Set the time to wait for the SSH client to complete the login. If the timer expires before the login is completed, the session is terminated.

Default: 120 seconds

Values: 1-600 seconds

Show SSH-Server

Description Shows the SSH server settings.
User Level Admin
Syntax `show ssh-server`

SSL/TLS Commands

Set SSL Server

Description Sets the default SSL/TLS parameters for the server.

User Level Admin

Syntax

```
set ssl server [version any|tslv1|sslv3] [type client|server]
 [verify-peer on|off]
 [validation-criteria
   country <code>|state-province <text>|locality <text>
   |organisation <text>|organisation-unit <text>
   |common-name <text>|email <email_addr>]
```

Options

version

Specify whether you want to use:

- **Any**—The IOLAN will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try an SSLv2 connection.
- **TLSv1**—The connection will use only TLSv1.
- **SSLv3**—The connection will use only SSLv3.

The default is **Any**.

type

Specify whether the IOLAN will act as an SSL/TLS client or server. The default is **Client**.

verify-peer

Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.

validation-criteria

Any values that are entered in the validation criteria must match the peer certificate for an SSL connection; any fields left blank will not be validated against the peer certificate.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

Set SSL Server Cipher-suite

Note: Not all SSL/TLS encryption options are available on all firmware versions.

Description Sets the default SSL/TLS cipher suite parameters.

User Level Admin

Syntax

```
set ssl server cipher-suite
 option1|option2|option3|option4|option5
 encryption any|aes|3des|des|arcfour|arctwo|none
 min-key-size 40|56|64|128|168|256
 max-key-size 40|56|64|128|168|256
 key-exchange any|rsa|edh-rsa|edh-dss|adh
 hmac any|sha1|md5
```

Options **option1|option2|option3|option4|option5**

Sets the priority of the cipher suite, with **option1** being highest priority and **option5** lowest priority.

encryption

Select the type of encryption that will be used for the SSL connection:

- Any—Will use the first encryption format that can be negotiated.
- AES
- 3DES
- DES
- ARCFOUR
- ARCTWO
- None—Removes any values defined for the cipher option.

The default value is **Any**.

min-key-size

The minimum key size value that will be used for the specified encryption type. The default is **40**.

max-key-size

The maximum key size value that will be used for the specified encryption type. The default is **256**.

key-exchange

The type of key to exchange for the encryption format:

- **Any**—Any key exchange that is valid is used (this does not, however, include ADH keys).
- **RSA**—This is an RSA key exchange using an RSA key and certificate.
- **EDH-RSA**—This is an EDH key exchange using an RSA key and certificate.
- **EDH-DSS**—This is an EDH key exchange using a DSA key and certificate.
- **ADH**—This is an anonymous key exchange which does not require a private key or certificate. Choose this key if you do not want to authenticate the peer device, but you want the data encrypted on the SSL/TLS connection.

The default is **Any**.

hmac

Select the key-hashing for message authentication method for your encryption type:

- Any
- MD5
- SHA1

The default is **Any**.

Show SSL

Description Shows the SSL/TLS settings/information.
User Level Normal, Admin
Syntax `show ssl`

Modbus Commands

Set Modbus Gateway

Description Sets the Modbus parameters for the IOLAN when it is operating as a Modbus Gateway.

User Level Admin

Syntax

```
set modbus gateway [addr-mode embedded|re-mapped]
set modbus gateway [broadcast on|off]
set modbus gateway [char-timeout <number>]
set modbus gateway [req-next-delay <number>]
set modbus gateway [exceptions on|off]
set modbus gateway [idle-timer <number>]
set modbus gateway [mess-timeout <number>]
set modbus gateway [port <TCP/UDP_port>]
set modbus gateway [req-queuing on|off]
set modbus gateway [remapped-id <1-247>]
set modbus gateway [ssl on|off]
set modbus gateway [ip-aliasing]
```

Options

addr-mode

Determines if the original UID address will be embedded in the transmission header or if a specified (remapped) UID will be embedded in the transmission header.

broadcast

When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. The default is **Off**.

char-timeout

Used in conjunction with the Modbus RTU protocol, specifies how long to wait, in milliseconds, after a character to determine the end of frame. The default is **30** ms.

req-next-delay

A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. The default is **50** ms.

exceptions

When enabled, an exception message is generated and sent to the initiating Modbus device when any of the following conditions are encountered: there is an invalid UID, the UID is not configured in the Gateway, there is no free network connection, there is an invalid message, or the target device is not answering the connection attempt. The default is **On**.

idle-timer

Specifies the number of seconds that must elapse without any network or serial traffic before a connection is dropped. If this parameter is set to 0 (zero), a connection will not be dropped (with the following exceptions: the TCP KeepAlive causes the connection to be dropped or the Modbus device drops the connection). The default is **10** seconds.

mess-timeout

Time to wait, in milliseconds, for a response message from a Modbus TCP or serial slave (depending if the Modbus Gateway is a Master Gateway or Slave Gateway, respectively) before sending a Modbus exception. The default is **1000** ms.

port

The network port number that the Slave Gateway will listen on for both TCP and UDP messages. The default is **502**.

req-queuing

When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception. The default is **On**.

remapped-id

Specify the UID that will be inserted into the message header for the Slave Modbus serial device. Valid values are 1-247.

ssl

When enabled, messages over the TCP connection are encrypted via SSL/TLS.

ip-aliasing

When enabled, allows for multiple requests to serial slaves (from an Ethernet Master/s) to be processed simultaneously.

Default: Off

Show Modbus

Description Displays the Modbus Gateway parameters.
User Level Admin
Syntax **`show modbus gateway`**

`show modbus slave|master <`*`line_number`***`>`**

Authentication Commands

Set Authentication

Description Sets the authentication method for the IOLAN.

User Level Admin

Syntax

```
set authentication type primary|secondary
 none|local|radius|kerberos|ldap|tacacs+|securid|nis
 [secondary-as-backup on|off] [auth-admin-user-local on|off]
```

Options

primary

The first authentication method that the IOLAN attempts. Some type of authentication must be done by the IOLAN, therefore, **None** is not a valid option for the **Primary Authentication Method**.

secondary

If the **Primary Authentication Method** fails, the next authentication method that the IOLAN attempts. You can choose to use authentication methods in combination. For example, you can specify the **Primary Authentication Method** as **Local** and the **Secondary Authentication Method** as **RADIUS**. Therefore, some users can be defined in the IOLAN (**Local**) others in **RADIUS**.

none|local|radius|kerberos|ldap|tacacs+|securid|nis

Specify the authentication method that the IOLAN will use to authenticate users (this must already be set up in your network).

secondary-as-backup

When enabled, the Secondary Authentication method will be tried only when the IOLAN cannot communicate with the Primary Authentication server.

auth-admin-user-local

When enabled, the IOLAN will only authenticate the admin user in the local user database, regardless of any external authentication methods configured. When disabled, a user called admin must exist when only external authentication methods are configured, or you will not be able to access the IOLAN as the admin user, except through the console port. The default is **on**.

Set Authentication Local

Description Configures local authentication settings. When you configure the IOLAN to authenticate users locally, you can require that the users be configured in the User table. You can also enable the **Guest** mode. This mode allows users to log into the IOLAN using any user name, but they will only get authenticated if they match the password configured for the **Guest** account.

User Level Admin

Syntax

```
set authentication local [guest-mode on|off] [password
 <text>][login-once on|off][password-rules on|off]
[account-lockout on|off]
```

Options

guest-mode

Allow users who are not defined in the **User** database to log into the IOLAN with any user ID and the specified password. **Guest** users inherit their settings from the **Default User**'s configuration.

password

The password that **Guest** users must use to log into the IOLAN.

Enable Login Once

When this option is selected, only one user with the same username can be signed in at one time. Should the same user with the same username attempt to sign in again, their first session will be terminated and they will gain entry to their new session.

Enable Password Rules

When this option is selected, the following password rules will apply. The password must be 8 characters long and contain at least one number.

Enable Account Lockout

When this option is selected, the IOLAN's internal local user database will provide a 10 second delay after each invalid attempt. If 5 invalid attempts are made within 1 minute the user will be locked out from further attempts for 5 minutes.

Set Authentication Kerberos

Description Configures Kerberos authentication settings.

User Level Admin

Syntax

```
set authentication kerberos [kdc-domain <string> <tunnel_name>]
 [port <TCP_port>] [realm <string>]
```

Options

kdc-domain

The name of a host running the KDC (Key Distribution Center) for the specified realm. The host name that you specify must either be defined in the IOLAN's **Host Table** (with an IP address) or be resolvable by a DNS server.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

port

The port that the Kerberos server listens to for authentication requests. If no port is specified, the default port 88 is used.

realm

The Kerberos realm is the Kerberos host domain name, in upper-case letters.

Set Authentication LDAP/Active Directory

Description Configures LDAP/Active Directory authentication settings.

User Level Admin

Syntax

```
set authentication ldap [base <string>]
 [client |append-base on|off |authenticate on|off
 |name <string> |password <string>] [encrypt-password on|off]
 [host <hostname/IP_addr> <tunnel_name>] [port <TCP_port>] [tls
 on|off]
 [tls-port <TCP_port>] [user-attribute other|<string>
 |sAMAccountName|uid
```

Options

base

The domain component (dc) that is the starting point for the search for user authentication.

client

Enables/disables appending the base domain component (dc) to the client name field. Enables/disables whether the IOLAN will authenticate itself to the LDAP Server. The name to be used by the IOLAN to authenticate to the LDAP Server. The password to be used when authenticating to the LDAP Server

host

The name or IP address of the LDAP/Active Directory host. If you use a host name, that host must either have been defined in the IOLAN's **Host Table** (with an IP address) or be resolvable by a DNS server. If you are using **TLS**, you must enter the same string you used to create the LDAP certificate that resides on your LDAP server.

port

The port that the LDAP/Active Directory host listens to for authentication requests. The default port is 389.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

encrypt-password

When enabled, the IOLAN will encrypt the user's and the IOLAN's password strings using MD5 digest.

tls

Enables/disables the Transport Layer Security (TLS) with the LDAP/Active Directory host.

tls-port

Specify the port number that LDAP/Active Directory will use for **TLS**. The default is port 636.

user-attribute

Specify whether you want to use:

- **Other** - specify a user attribute to be used when authenticating.
- **sAMAccountName** - When enabled, the IOLAN will use the Microsoft Active Directory attribute sAMAccountName for the user name.
- **uid** - When enabled, the IOLAN will use the OpenLDAP attribute uid for the user name.

The default is **uid**.

Set Authentication NIS

Description Sets NIS authentication parameters.

User Level Admin

Syntax **set authentication nis [domain <***string***>] [primary <***config_host***> <tunnel_name>]**
[secondary <*config_host***>]**

Options **domain**

The NIS domain name.

primary

The primary NIS host that is used for authentication.

secondary

The secondary NIS host that is used for authentication, should the primary NIS host fail to respond.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Add RADIUS

Description Adds an accounting or authentication RADIUS host.

User Level Admin

Syntax

```
add radius accounting-host <config_host> secret
add radius auth-host <config_host> <tunnel_name> secret
```

Options

accounting-host

The first time this command is entered, this is the name of the primary RADIUS accounting host.

The second time this command is entered, this is the name of the secondary RADIUS authentication host.

auth-host

The first time this command is entered, this is the name of the primary RADIUS authentication host.

The second time this command is entered, this is the name of the secondary RADIUS authentication host, should the first RADIUS host fail to respond.

secret

The secret (password) shared between the IOLAN and the RADIUS authentication host.

After typing the command **secret** and pressing **Enter**, you will be prompted to enter the secret and then re-enter the secret.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Delete RADIUS

Description Deletes an accounting or authentication RADIUS host.

User Level Admin

Syntax

```
delete radius accounting <accounting_host>
delete radius authentication <authentication_host>
```

Options

accounting

Deletes the specified accounting host from the RADIUS authentication settings.

authentication

Deletes the specified authentication host from the RADIUS authentication settings.

Set Authentication RADIUS

Description Sets RADIUS parameters.

User Level Admin

Syntax
```
set authentication radius [accounting on|off]
 [acct-authenticator on|off] [acct-port <UDP_port>]
 [auth-port <UDP_port>] [nas-identifier <nas_id>]
 [nas-ip-address auto|specify <ipv4_address>]
 [nas-ipv6-address auto|specify <ipv6_address>] [retry <integer>]
 [timeout <integer>]
```

Options

accounting

Enables/disables RADIUS accounting.

acct-authenticator

Enables/disables whether or not the IOLAN validates the RADIUS accounting response.

acct-port

The port that the RADIUS host listens to for accounting requests. The default port is 1813.

auth-port

The port that the RADIUS host listens to for authentication requests. The default port is 1812.

nas-identifier

This is the string that identifies the Network Address Server (NAS) that is originating the Access-Request to authenticate a user.

Field Format: Maximum 31 characters, including spaces

nas-ip-address auto

When specified, the IOLAN will send the IOLAN's Ethernet 1 IPv4 address to the RADIUS server. This is the default.

nas-ip-address specify *<ipv4_address>*

When specified, the IOLAN will send the specified IPv4 address to the RADIUS server. The default is 0.0.0.0.

nas-ipv6-address auto

When specified, the IOLAN will send the IOLAN's IPv6 address to the RADIUS server. This is the default.

nas-ipv6-address specify *<ipv6_address>*

When specified, the IOLAN will send the specified IPv6 address to the RADIUS server.

retry

The number of times the IOLAN tries to connect to the RADIUS server before erroring out. Valid values are 0-255. The default is **5**.

timeout

The time, in seconds, that the IOLAN waits to receive a reply after sending out a request to a RADIUS accounting or authentication host. If no reply is received before the timeout period expires, the IOLAN will retry the same host up to and including the number of retry attempts. Valid values are 1-255. The default is **3** seconds.

Set Authentication TACACS+

Description Configures TACACS+ authentication settings.

User Level Admin

Syntax

```
set authentication tacacs+ [port <TCP_port>]
 [primary <config_host>] [secondary <config_host>]<tunnel_name>
 [secret <string>][alternate-service-names
 <on|off>][authorization <on|off>][accounting
  <on|off>] [acct-port <TCP_port>] [acct-primary <config_host>]
  acct-secondary <config_host>] acct-secret <string>]
```

Options

port

The port number that TACACS+ listens to for authentication requests. The default port number is 49.

primary

The primary TACACS+ host that is used for authentication.

secondary

The secondary TACACS+ host that is used for authentication, should the primary TACACS+ host fail to respond.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

secret

The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.

alternate-service-name

The TACACS+ service name Telnet or SSH is normally “raccess”. The service name for Web Manager or Device Manager is “EXEC”. In some cases, these service names conflicted with services used by Cisco devices. If this is the case, checking this field will cause the service name for Telnet or SSH to be “perlecli” and the service name for Web Manager or Device Manager to be “perleweb”.

authorization

Enables authorization on the TACACS+ host, meaning that IOLAN-specific parameters set in the TACACS+ configuration file can be passed to the IOLAN after authentication.

Default: Disabled

accounting

Enables/disables TACACS+ accounting.

Default: Disabled

acct-port

The port number that TACACS+ listens to for accounting requests. The default port number is 49.

acct-primary

The primary TACACS+ host that is used for accounting.

Default: None

acct-secondary

The secondary TACACS+ host that is used for accounting, should the primary accounting TACACS+ host fail to respond.

Default: None

acct-secret

The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.

Set Authentication SecurID

Description Configures SecurID authentication settings.

User Level Admin

Syntax

```
set authentication securid primary [host <config_host>]
 <tunnel_name>
 [port <TCP_port>] [encryption des|sdi] [legacy on|off]

set authentication securid replica [host <config_host>]
 [port <TCP_port>] [encryption des|sdi] [legacy on|off]

set authentication securid reset secret
```

Options

primary host

The first SecurID server that is tried for user authentication.

replica host

If the first SecurID server does not respond to an authentication request, this is the next SecurID server that is tried for user authentication.

port

The port number that SecurID listens to for authentication requests. The default port number is 5500.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

encryption

You can specify either **SDI** or **DES** encryption for SecurID server communication. The default is **SDI** encryption.

legacy

If you are running SecurID 3.x or 4.x, you need to run in **Legacy Mode**. If you are running SecurID 5.x or above, do not select **Legacy Mode**.

reset secret

Resets the SecurID secret (password) in the IOLAN.

Show Authentication

Description Shows the authentication settings. If you type just the **`show authentication`** command, the configured primary and secondary authentication methods are displayed.

User Level Admin

Syntax

```
show authentication radius|ldap|tacacs+|nis|kerberos|securid
```

Option **`radius|ldap|tacacs+|nis|kerberos|securid`**

Displays the authentication settings for the specified authentication method.

TruePort Baud Commands

Set TruePort Remap-Baud

Description This command allows for the remapping of the baud rate being specified by the Serial application to a different value on the physical serial port on the IOLAN.

User Level Admin

Syntax

```
set trueport remap-baud
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|
   38400
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|
   38400|57600|115200|230400|28800|[custom <baud_rate]
```

Options **50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|38400**

The configured baud rate of the TruePort client.

50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|38400|57600|115200|230400|28800|[custom <*baud_rate*>]

The actual baud rate that runs between the IOLAN and the connected serial device. You can also specify a custom baud rate; valid values are 50 - 1843200.

Show TruePort

Description Shows the IOLAN TruePort remapping table.

User Level Normal, Admin

Syntax

```
show trueport
```

Email Commands

Set Email-Alert Server

Description Configures email alert settings for the server.

User Level Admin

Syntax

```
set email-alert server [from <email_addr>]
[level emergency|alert|critical|error|warning|notice|info|debug]
[mode on|off] [to <email_addr>] [reply-to <email_addr>]
[smtp-host <string>] [subject <string>][encryption
none|tls|ssl]{verify-peer off|on][tcp-port <number>][domain
<text>]
```

Options

from

This will be the contents of the from field in the generated email.

This field will be specified in the **from** field of the email message sent by the IOLAN.

level

Choose the event level that triggers an email notification:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

The list is in decreasing order of priority (**Emergency** has the highest priority). You are selecting the lowest notification level; therefore, when you select **Debug**, you will get an email notification for all events that trigger a message.

mode

Determines whether or not email notification is turned on. Default is **Off**.

to

An email address or list of email addresses that will receive the email notification.

reply-to

The email address to whom all replies to the email notification should go.

smtp-host

The SMTP host (email server) that will process the email notification request. This can be either a host name defined in the IOLAN host table or the SMTP host IP address.

subject

A text string, which can contain spaces, that will display in the **Subject** field of the email notification.

If the text string contains spaces, enclose the string in quotes.

encryption

Choose the type of encryption to be used.

Valid options:

None- All information is sent in the clear.

SSL -Select this if you r email server requires SSL.

TLS - Select this if your email server requires TLS.

verify-peer

Enable the validation of the certificate presented by the email server. To validate the certificate, you will need to download the appropriate CA list into the IOLAN. If the certificate is not found to be valid the communications with the email server will be terminated. No authentication will take place and the email message will not be forwarded to the email server. If this option is not checked, the certificate validaation will still be attempted but if it fails, a syslog message will be generated but the authentication and forwarding of the email will still take place.

Default: Enable if SSL or TLS encryption is selected. Disabled if no encryption is selected.

tcp-port

This is the TCP port used to communicate with the email server.

Default: 25 for non-SSL, 465 if SSL/TLS is used.

domain

This field is only used if SPA authentication is performed with the email server. It may or may not be required. If the email server does not expect this field, it can be left blank.

Show Email-Alert Server

Description Shows how the server email alert is configured.
User Level Admin
Syntax `show email-alert server`

Clustering Commands

Add Clustering Slave-IP

Description Adds a slave IOLAN to the clustering group.
User Level Admin
Syntax
```
add clustering slave-ip <IPv4_address>
 number-of-ports 1|2|4|8|16|24|32|48 [protocol telnet|ssh]
 [starting-master-tcp-port <10001-65535>]
 [starting-slave-ds-port <10001-65535>]
```

Options ***<IPv4_address>***

Specify the IP address of the clustering slave you wish to modify. This clustering slave must already exist in the clustering group. The IP address must be in a valid IPv4 format.

number-of-ports

Specify the port number that you wish to modify on this clustering slave.

protocol

Specify the protocol that will be used to access the Slave IOLAN port, SSH or Telnet.

starting-master-tcp-port

Specify this parameter if you wish to change the name associated with this slave port.

starting-slave-ds-port

Specify this parameter if you wish to change the slave-ds-port associated with this slave port. This should match the port number configured for this port on the salve IOLAN.

Delete Clustering Slave-IP

Description Deletes a Slave IOLAN from the clustering group. Type **`delete clustering slave-ip ?`** to get a list of Slave IOLAN IP addresses.
User Level Admin
Syntax
```
delete clustering slave-ip <IPv4_address>
```
Option ***<IPv4_address>***

Specify the IP address of the clustering slave you wish to modify. This clustering slave must already exist in the clustering group. The IP address must be in a valid IPv4 format.

Set Clustering Slave-IP

Description Modify the parameter associated with a specific port in a clustering group.
User Level Admin
Syntax
```
set clustering slave-ip <IPv4_address> port <number>
 [master-tcp-port <10001-65535>] [name <port_name>]
 [protocol telnet|ssh|not-used] [slave-ds-port <10001-65535>]
```

Options ***<IPv4_address>***

Specify the IP address of the clustering slave you wish to modify. This clustering slave must already exist in the clustering group. The IP address must be in a valid IPv4 format.

port

Specify the port number that you wish to modify on this clustering slave.

master-tcp-port

Specify this parameter if you wish to change the name associated with this slave port.

name

Specify this parameter if you wish to change the name associated with this slave port.

protocol

Specify this parameter if you wish to change the protocol used to access this slave port. Valid options are SSH, Telnet or not used if you wish to disable access to this port.

slave-ds-port

Specify this parameter if you wish to change the slave-ds-port associated with this slave port. This should match the port number configured for this port on the salve IOLAN.

Show Clustering Slave-IP

Description Show a Slave IOLANs clustering group settings. Type **`show clustering slave-ip ?`** to get a list of Slave IOLAN IP addresses.

User Level Admin

Syntax **`show clustering slave-ip <`***`IPv4_address`***`> [get-port-names] [get-port-names-and-save]`**

Options ***<IPv4_address>***

Specify the IP address of the clustering slave you wish to modify. This clustering slave must already exist in the clustering group. The IP address must be in a valid IPv4 format.

get-port-names

Retrieves the port/line names from the specified Slave IOLAN.

get-port-names-and-save

Retrieves the port/line names from the specified Slave IOLAN and saves them in the Slave IOLAN clustering configuration.

Dynamic DNS Commands

Set Dynamic-DNS

Description Configures the dynamic DNS parameters.

User Level Admin

Syntax

```
set dynamic-dns [on|off]
 [connection-method http|http-port-8245|https]
 [hostname <hostname>] [username <username>]
 [password <password>] [system-type dynamic|static|custom]
 [wildcard enable|disable|nochange]
```

Options

connection-method

Specify how the IOLAN is going to connect to the DynDNS.org server, via HTTP, HTTP through Port 8245, or HTTPS.

hostname

Specify the registered hostname with DynDNS.org that will be updated with the IOLAN's IP address should it change. Put in the full name; for example, mydeviceserver.dyndns.org.

username

Specify the user name used to access the DynDNS.org server.

password

Specify the password used to access the DynDNS.org server.

system-type

Specify how your account was set up with DynDNS.org, using a Dynamic, Static, or Custom IP address schema.

wildcard

Adds an alias to **`*.yourhost.ourdomain.ext`** pointing to the same IP address as entered for **`yourhost.ourdomain.ext`**.

Set Dynamic-DNS SSL

Description Sets the SSL/TLS parameters for the connection between the IOLAN and the DNS server.

User Level Admin

Syntax

```
set dynamic-dns ssl [verify-peer on|off]
 [validation-criteria
   country <code>|state-province <text>|locality <text>
   |organisation <text>|organisation-unit <text>
   |common-name <text>|email <email_addr>]
```

Options

verify-peer

Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.

validation-criteria

Any values that are entered in the validation criteria must match the peer certificate for an SSL connection; any fields left blank will not be validated against the peer certificate.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

Set Dynamic-DNS SSL Cipher-Suite

Note: Not all SSL/TLS encryption options are available on all firmware versions.

Description Sets the SSL/TLS cipher suite parameters for the connection between the IOLAN and the DNS server.

User Level Admin

Syntax

```
set dynamic-dns ssl cipher-suite
 option1|option2|option3|option4|option5
 encryption any|aes|3des|des|arcfour|arctwo|none
 min-key-size 40|56|64|128|168|256
 max-key-size 40|56|64|128|168|256
 key-exchange any|rsa|edh-rsa|edh-dss|adh
 hmac any|sha1|md5
```

Options **option1|option2|option3|option4|option5**

Sets the priority of the cipher suite, with **`option1`** being highest priority and **`option5`** lowest priority.

encryption

Select the type of encryption that will be used for the SSL connection:

- Any—Will use the first encryption format that can be negotiated.
- AES
- 3DES
- DES
- ARCFOUR
- ARCTWO
- None—Removes any values defined for the cipher option.

The default value is **Any**.

min-key-size

The minimum key size value that will be used for the specified encryption type. The default is **40**.

max-key-size

The maximum key size value that will be used for the specified encryption type. The default is **256**.

key-exchange

The type of key to exchange for the encryption format:

- **Any**—Any key exchange that is valid is used (this does not, however, include ADH keys).
- **RSA**—This is an RSA key exchange using an RSA key and certificate.
- **EDH-RSA**—This is an EDH key exchange using an RSA key and certificate.
- **EDH-DSS**—This is an EDH key exchange using a DSA key and certificate.
- **ADH**—This is an anonymous key exchange which does not require a private key or certificate. Choose this key if you do not want to authenticate the peer device, but you want the data encrypted on the SSL/TLS connection.

The default is **Any**.

hmac

Select the key-hashing for message authentication method for your encryption type:

- Any
- MD5
- SHA1

The default is **Any**.

Show Dynamic-DNS

Description Shows the dynamic DNS settings.
User Level Admin
Syntax `show dynamic-dns`

PCI Commands

Set PCI

Description Sets the type of card in the PCI slot.
User Level Admin
Syntax
```
set pci card none|modem|wireless-wan|fiber-lan|usb
set pci fiber-lan model kg-500f-gigabit|sfm-gls-10-a-fast
```

Option **card | fiber-lan model**

Specify the type of card which is inserted in the PCI slot. Choices are **modem** for an IOLAN modem card, **wireless-wan** for a wireless WAN card, **usb** for a usb modem stick or **fiber-lan** for a fiber LAN card. Choose **none** or leave the default modem if no card is inserted in the PCI slot.

Show PCI

Description Displays the PCI line settings.
User Level Admin
Syntax
```
show pci
```

Set PCI Wireless-WAN

Description Configures the wireless WAN parameters.
User Level Admin
Syntax
```
set pci wireless-wan [access-point-name <name>]
 [init-string <modem_init_string>]
 [model sierra-wireless-aircard-881|sony-ericsson-pc300|sierra|
        sony-ericsson|standard|custom]
 [password <password>][phone-number <phone_number>]
 [user <username>]
```

Options **access-point-name**

Specify the APN required by your internet provider to access their network. See the internet provider documentation for more information.

init-string

Specify the initialisation string required by your internet service provider for your wireless WAN card.

model

Specify the wireless WAN card you are using. If the wireless WAN card you are using is not listed, try the standard driver. If that does not work, look at the Perle website for a custom driver.

password

Specify the password required by your internet provider to access their network.

phone-number

Specify the phone number provided by your service provider to access their wireless network. The phone number will probably take a format similar to ***99***1#**.

user

Specify the name required by your internet provider to access their network.

Show Wireless-WAN

Description Displays the wireless WAN settings.
User Level Admin
Syntax **`show wireless-wan`**

Set pci usb

Description Configures the usb modem stick parameters.
User Level Admin
Syntax
```
set pci usb [access-point-name <name>]
 [init-string <modem_init_string>]
 [user <username>]
 [password <password>]
 [phone-number <phone_number>]
 [pin <pin>]
```

Options

access-point-name

Specify the APN required by your internet provider to access their network. See the internet provider documentation for more information.

init-string

Specify the initialisation string required by your internet service provider for your usb modem stick.

user

Specify the name required by your internet provider to access their network.

password

Specify the password required by your internet provider to access their network.

phone-number

Specify the phone number provided by your service provider to access their wireless network. The phone number will probably take a format similar to **`*99***1#`**.

pin

If you have locked you SIM using a PIN, you must enter this PIN here in order to allow the IOLAN to access it. If you have never locked your SIM, leave this field blank. You can enter up to 8 digits for the PIN.

Usb show modem

Description Displays the status of the usb modem including parameters detected by the driver and the current state of the modem.
User Level Admin
Syntax **`usb show modem`**

Usb create modem-file

Description Adds the device type parameter to the "usb_modem" file.
User Level Admin
Syntax **`usb create modem [device <name>]`**

device

This command will enable you to specify the "device name" which the driver uses to communicate with your usb modem. The device name would be (ttyUSBx or ttyACMx). x is in the range of 1-4. This should only be needed if the usb modem is not working and you suspect that the device name is wrong. Use the CLI command "usb show modem" to obtain an indication whether this could be the reason the USB modem is not working.

Usb delete modem-file

Description Deletes the "usb_modem" file. This will remove any custom parameters entered by the user such as device name. Deleting this file will cause the code to go back to a fully automatic mode of operation using parameters that it detected.

User Level Admin

Syntax `usb delete modem-file`

IPv6 Commands

Set IPv6

Description Configures the basic IPv6 settings.
User Level Admin
Syntax

```
set ipv6 [dhcpv6-settings ipv6-address on|off]
 [dhcp-settings network-prefix on|off]
 [auto-obtain-dns-ipv6 on|off] [eth1|eth2]
 [enable-ipv6-addressing on|off] [obtain-using auto-ipv6|dhcpv6]
```

Options **dhcpv6-settings**

Determines the types of information that the IOLAN will accept from the DHCPv6 server, IPv6 address(es) and/or network prefix(es).

ivp6-address

When enabled, the IOLAN will accept IPv6 address(es) from the DHCPv6 server. This is **`off`** by default.

network-prefix

When enabled, the IOLAN will accept the network prefix from the DHCPv6 server. This is **`off`** by default.

eth1|eth2

Configures the IPv6 settings for the IOLAN's Ethernet interface 1 and/or Ethernet interface 2 (SCS models only) connection(s).

enable-ipv6-addressing

When enabled, you can configure the IOLAN to obtain the IPv6 address(es) using IPv6 Autoconfiguration or a DHCPv6 server.

Default: Enabled

obtain-using auto-ipv6|dhcpv6

- **auto-ipv6**—When enabled, the IOLAN will send out a Router Solicitation message. If a Router Advertisement message is received, the IOLAN will configure the IPv6 address(es) and configuration parameters based on the information contained in the advertisement. If no Router Advertisement message is received, the IOLAN will attempt to connect to a DHCPv6 server to obtain IPv6 addresses and other configuration parameters. This is the default.
- **dhcpv6**—When enabled, requests IPv6 address(es) and configuration information from the DHCPv6 server.

Show IPv6

Description Shows the IPv6 settings.
User Level Admin
Syntax

```
show ipv6 [eth1|eth2]
```

Option **eth1|eth2**

Displays the configuration IPv6 information for the specified Ethernet interface.

Add Custom-IPv6

Description

User Level Admin

Syntax

```
add custom-ipv6 [eth1|eth2] method auto
 network-prefix <network_prefix>
 [prefix-bits <0-64>] [router-advertisement on|off]

add custom-ipv6 [eth1|eth2] method manual
 ipv6-address <ipv6_address> [prefix-bits <0-128>]
 [router-advertisement on|off]
```

Options

eth1|eth2

Configures the custom IPv6 settings for the IOLAN's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

method auto

When this option is specified, the IOLAN will derive an IPv6 address from the entered network prefix and the IOLAN's MAC address. This is the default option.

network-prefix

Specify the IPv6 network prefix. The IOLAN will derive the complete IPv6 address from the entered network prefix and the IOLAN's MAC address.

prefix-bits (auto)

Specify the network prefix bits for the IPv6 address.

Range: 0-64

Default: 64

method manual

Specify this option when you want to enter a specific IPv6 address.

ipv6-address

Specify the complete IPv6 address.

Field Format: IPv6 address

prefix-bits (manual)

Specify the network prefix bits for the IPv6 address.

Range: 0-128

Default: 64

router-advertisement

When enabled, the IPv6 address is advertised when the IPv6-router-advertisement parameter is enabled.

Set Custom-IPv6

Description Configures custom IPv6 network and IP addresses.

User Level Admin

Syntax

```
set custom-ipv6 [eth1|eth2] <config_ipv6_address> method auto
 network-prefix <network_prefix>
 [prefix-bits <0-64>] [router-advertisement on|off]

set custom-ipv6 [eth1|eth2] <config_ipv6_address> method manual
 ipv6-address <ipv6_address> [prefix-bits <0-128>]
 [router-advertisement on|off]
```

Options **eth1|eth2**

Configures the custom IPv6 settings for the IOLAN's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

method auto

When this option is specified, the IOLAN will derive an IPv6 address from the entered network prefix and the IOLAN's MAC address. This is the default option.

network-prefix

Specify the IPv6 network prefix. The IOLAN will derive the complete IPv6 address from the entered network prefix and the IOLAN's MAC address.

prefix-bits (auto)

Specify the network prefix bits for the IPv6 address.

Range: 0-64

Default: 64

method manual

Specify this option when you want to enter a specific IPv6 address.

ipv6-address

Specify the complete IPv6 address.

Field Format: IPv6 address

prefix-bits (manual)

Specify the network prefix bits for the IPv6 address.

Range: 0-128

Default: 64

router-advertisement

When enabled, the IPv6 address is advertised when the IPv6-router-advertisement parameter is enabled.

Delete Custom-IPv6

Description Deletes the specified custom IPv6 address. To see a list of configured IPv6 addresses, type the command **`delete custom-ipv6 ?`**.

User Level Admin

Syntax

```
delete custom-ipv6 <config_ipv6_address> [eth1|eth2]
```

Option **eth1|eth2**

Deletes the specified custom IPv6 address. You must specify the Ethernet interface for SCS models.

IPv6 Router Advertisements

Set IPv6-Router-Advertisement

Description Configures IPv6 router advertisements.
User Level Admin
Syntax `set ipv6-router-advertisement [eth1|eth2] on|off [dhcpv6 off|on] [dhcpv6-cfg-options off|on]`
Options **ipv6-router-advertisement**

When enabled, the IOLAN will periodically send IPV6 Router Advertisement messages and respond to Router Solicitation messages. The Router Advertisement message can be configured to contain any of the following information:

- **DHCPv6**—Use the DHCPv6 server to obtain additional IPV6 address(es) and configuration parameters.
- **DHCPv6 Configuration Options**—Use DHCPv6 server to obtain additional configuration parameters.
- **Network Prefixes**—Advertise the selected custom configured network prefixes.

Default: Disabled

eth1|eth2

Configures the IPv6 router advertisement settings for the IOLAN's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

dhcpv6

When enabled, the Router Advertisement message indicates to use the DHCPv6 server for obtaining additional IPv6 addresses and configuration parameters.

Default: Disabled

dhcpv6-cfg-options

When enabled, the Router Advertisement message indicates to use the DHCPv6 server to obtain additional configuration parameters.

Default: Disabled

Show IPv6-Router-Advertisement

Description Displays the IPv6 router advertisement settings.
User Level Admin
Syntax `show ipv6-router-advertisement [eth1|eth2]`
Option **eth1|eth2**

Displays the IPv6 router advertisement settings for the IOLAN's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

Line Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's line parameters.

1-Port vs. 2-Port+ Line Commands

If you are using a 1-port IOLAN, the admin user does not have the option of using the number or all (*) options in the line commands, as there is only one line. In a 2-port+ IOLAN, the admin user must specify**.** (current line), <***number***> (line number), or ***** (sets value for all lines) when configuring lines.

Line Commands

Set Line

Description Configures line parameters. The `set line` command does not work on modem ports/lines on models that have an internal modem.

User Level Normal, Admin, Elevated User

Syntax

```
set line . speed
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19,200|38
 ,400|57,600|115,200|230,400|28,800|custom
[data-bits 5|6|7|8]
 [connection-method dial-in|dial-out|dial-in-out|direct-connect|
    ms-direct-host|ms-direct-guest]
 [idle-timer <0-4294967>] [line-name <name>]
 [modem-name <config_modem>] [pages 1|2|3|4|5|6|7]
 [parity none|even|odd|mark|space] [phone-number <phone_number>]
 [rev-sess-security on|off] [send-name on|off] [sess-timer
 <0-4294967>]
 [session-strings |delay <0-65535> |initiate <text> |terminate
 <text> timer <0-4294967>]
 [stop-bits 1|2|1.5] [termtype wyse60|vt100|ansi|dumb|tvi925|
 ibm3151te|vt320|hp700|term1|term2|term3][break on|off]
 [break-length <0-65535>] [break-delay <0-65535>]
 [discard-characters-received-with-error on|off]
```

Admin User Only

```
set line .|<number>|* speed
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19,200|38
 ,400|57,600|115,200|230,400|28,800|custom
  [mode enabled|disabled] [map-cr-crlf on|off] [data-logging
 on|off] [flowin on|off] [flowout on|off] [hotkey-prefix <00-7f>]
 [initial cli|menu] [keepalive on|off] [lock on|off]
 [microsoft-sac-support on|off] [motd on|off]
 [multisessions <integer>] [reset on|off] [dial-timeout <number>]
 [dial-retries <number>] [user <name>] [nouser]
 [line-termination on|off] [internet-address <IPv4_address>]
```

Elevated User

```
set line .|<number>|* speed
50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19,200|38
,400|57,600|115,200|230,400|28,800|custom

Note: The save command must be executed by an admin user in order
 for this parameter to be permanently saved.
```

Options

mode

Enables/disables a line (available only on 2-port+ models). The default is enabled.

data-bits

Specifies the number of bits in a byte. The default is **8**.

connection-method

Determines how a modem will work on the line. Select from the following options:

- **Direct Connect**—Indicates that there is not a modem on the line. This is the default.
- **Dial In**—Specify this option when a user is remote and will be dialing in via modem or ISDN TA.
- **Dial Out**—Specify this option when a modem is attached to the serial port and is being used to dial out.
- **Dial In/Out**—Specify this option when the IOLAN is being used as a router (depending on which end of the link your IOLAN is situated and how you want to initiate the communication).
- **MS Direct-Host**—Specify this option when the serial port is connected to a Microsoft Guest device. **Line Service** must be set to **PPP** for this option.
- **MS Direct-Guest**—Specify this option when the serial port is connected to a Microsoft Host device. **Line Service** must be set to **PPP** for this option.

idle-timer

Enter a time period, in seconds, for which the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, the IOLAN will end the connection. The maximum value is 4294967 seconds (about 49 days). The default value of **0** (zero) means the **Idle Timer** will not expire, so the connection is permanently open.

line-name

Provide a name for the line so it can be easily identified. The **Remote Port Buffering** logging feature uses the **Line Name** when creating a file on the remote NFS server.

modem-name

The name of the predefined modem that is used on this line.

pages

For **DSLogin** line service, this is the number of video pages the terminal supports. Valid values are 1-7. The default is **5** pages.

parity

Specifies if you are using **Even**, **Odd**, or **No parity** on the line. If you want to force a parity type, you can specify **Mark** for 1or **Space** for 0.

phone-number

The phone number to use when **Connection Method** is set to **Dial Out**.

rev-sess-security

Enables/disables login/password authentication, locally or externally, on reverse Telnet connections. The default is **Off**.

port-name

When enabled, the port name will be sent to the host upon session initiation.
Default: Disabled

sess-time

Enter a time, in seconds, for which the **Session Timer** will run. Use this timer to forcibly close the session (connection). When the **Session Timer** expires, the IOLAN will end the connection. The default value is **0** seconds so the port will never timeout. The maximum value is 4294967 seconds (about 49 days).

session strings

Controls the sending of ASCII strings to serial devices at session start and session termination as follows;

- **Send at Start**—If configured, this string will be sent to the serial device when the serial device is detected (i.e. signals come up). The maximum size of this field is 128 bytes/characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).
- **Send at End**—If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. The maximum size of this field is 128 bytes/characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).
- **Delay after Send**—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.

  Range: 0-65535 ms

  Default: 10 ms

break

Specifies how a break is interpreted:

- **off**—The IOLAN ignores the break key completely and it is not passed through to the host. This is the default setting.
- **local**—The IOLAN deals with the break locally. If the user is in a session, the break key has the same effect as a hot key.
- **remote**—When the break key is pressed, the IOLAN translates this into a telnet break signal which it sends to the host machine.
- **break-interrupt**—On some systems such as SunOS, XENIX, and AIX, a break received from the peripheral is not passed to the client properly. If the client wishes to make the break act like an interrupt key (for example, when the stty options **`-ignbrk`** and **`brkintr`** are set).

break-length

The length of time (in milliseconds) for which the break signal will be asserted on the serial port. Valid values are 0-65535.
Default is 1000 ms
A value of 0 will cause the "request to send a break signal" to be ignored.

break-delay

The length of time (in milliseconds) to delay after a break signal is sent before the IOLAN sends data. Valid values are 0-65535.
Default: 0 ms (no delay)

map-cr-crlf

When **Line Service Printer** is selected, defines the default end-of-line terminator as CR-LF (ASCII carriage-return line-feed) when enabled. Default is **Off**.

flowin

Determines if input flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

flowout

Determines if output flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

data-logging

When enabled, serial data will be buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data will be sent to its destination.

Note: A kill line or a reboot of the IOLAN causes all buffered data to be lost.

The minimum data buffer size for all models is 1 KB. The maximum data buffer is 2000 KB for DS1//TS1/STS8D, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.

Some profile features are not compatible when using the Data Logging feature. See *Data Logging Appendix J* in the *IOLAN User's Guide* for more information.

Values: 1-2000 KB (DS1/TS1/STS8D)

Values: 1-4000 KB (all other models)

Default: Disabled

hotkey-prefix

The prefix that a user types to lock a line or redraw the Menu. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^r**—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always **Ctrl R**, regardless of the **Hotkey Prefix**.

You can use the **Hotkey Prefix** key to lock a line only when the **Line Lock** parameter is **On**.

initial

Specifies the initial interface a user navigates when logging into the line; either the **Menu** or a prompt for the **CLI**. The default is **CLI**.

keepalive

Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.

This parameter needs to be used in conjunction with server parameter, monitor-connection-every. The interval determines how long the IOLAN will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.

lock

When enabled, the user can lock his terminal with a password using the **Hotkey Prefix** (default Ctrl-a) **^a l** (lowercase L). The IOLAN prompts the user for a password and a confirmation.

microsoft-sac-support

When enabled, a user can access SAC (the interface of the Microsoft Emergency Management Systems utility) through EasyPort Web when the IOLAN's serial port is connected to a Microsoft Server 2003 or Microsoft Server 2008 host. The default is off.

motd

Enables/disables the message of the day on the line.

multisessions

This parameter defines the maximum number of additional reverse sessions which will be allowed for this line allowing more control as to how the total reverse sessions are allocated. This is on top of the main reverse session to the line.

The total number of reverse sessions on the IOLAN are dependent on the model:

- **1-port:** 0-3
- **2-port:** (4 x *#-of-ports*) -1
- **STS/SDS/MDC 4+ ports:** (2 x *#-of-ports*) -1
- **SCS 4+ ports:** (2 x (*#-of-ports* + 1)) -1

user

For **DSLogin** line service, makes this a line that is dedicated to the specified user. Only this user will be able to log in on this line and they won't need to enter their login name - just their password. When the **Line Service** is set to **Direct** or **Silent Rlogin**, the **User** parameter is used as the Rlogin user name (since Rlogin will not prompt you for a user name).

nouser

Blanks out the User parameter, in case you want to change a dedicated user line to an undedicated line.

reset

Resets the terminal type connected to the line when a user logs out.

dial-timeout

The number of seconds the IOLAN will wait to establish a connection to a remote modem. The default value is **45** seconds.

dial-retries

The number of times the IOLAN will attempt to re-establish a connection with a remote modem. The default value is **2**.

stop-bits

Specifies the number of stop bits that follow a byte. The 1.5 option is only available on the 1-port and 2-port models, but not on the modem of the SDS1M or SDS3M models.

term-type

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3** (user-defined terminals)

line-termination

Used with **EIA-422** and **EIA-485** on SDS 8-port+ IOLAN models, specifies whether or not the line requires termination. When termination is required, you need to terminate the line at both ends of the connection.

internet-address

Used with reverse sessions, users can access serial devices connected to the IOLAN by the specified Internet Address (or host name that can be resolved by a DNS). You must reboot the IOLAN for the **Internet Address** to take affect (the kill line option does not apply to this parameter). This parameter must be in IPv4 format.

break-delay

The length of time (in milliseconds) to delay after a break signal is sent before the IOLAN sends data. Valid values are 0-65535.
Default: 0 ms (no delay)

break-length

The length of time (in milliseconds) for which the break signal will be asserted on the serial port. Valid values are 0-65535.
Default is 1000 ms
A value of 0 will cause the "request to send a break signal" to be ignored.

discard-characters-received-with-error

When enabled, the IOLAN will discard characters received with a parity or framing error.
Default: Disabled

Set Line Interface

The SCS, STS, and MDC IOLAN models support the EIA-232 interface only. Therefore, you do not need to specify **interface eia-232** in the command syntax; you only need to specify the command options (e.g., **monitor-dcd**).

Description Configures line interface (hardware) parameters.

User Level Admin

Syntax

```
set line .|<number>|* interface eia-232 [monitor-dcd on|off]
 [monitor-dsr on|off] [flow none|soft|hard|both]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|
   19200|38400|57600|115200|230400|28800|custom <baud_rate>]

set line .|<number>|* interface eia-422
 [flow none|soft|hard|both]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|
   custom <baud_rate>]

set line .|<number>|* interface eia-485-half-duplex
 [tx-driver-control auto|rts] [flow none|soft]
 [echo-suppression on|off]]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|custom <baud_rate>]

set line .|<number>|* interface eia-485-full-duplex
 [tx-driver-control auto|rts] [flow none|soft]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|custom <baud_rate>]
```

Options

eia-232 | eia-422 | eia-485-half-duplex|eia-485-full-duplex

Specifies the type of serial line that is being used with the IOLAN. Specify either EIA-232, EIA-422, EIA-485-half-duplex, or EIA-485-full-duplex. The STS, SCS, and MDC models support only EIA-232.

monitor-dcd

Specifies whether the RS-232 signal DCD (Data Carrier Detect) should be monitored. This is used with modems or any other device that sends a DCD signal. When it is monitored and the IOLAN detects a DCD signal, the line service is started. Default is **Off**. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

monitor-dsr

Specifies whether the RS-232 signal DSR (data set ready) should be monitored. This is used with modems or any device that sends a DSR signal. When it is monitored and the IOLAN detects a DSR signal, the line service is started. Default is **Off**. The **Monitor DSR** parameter is not available for medical unit models. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

flow

Defines whether the data flow is handled by the software (**Soft**), hardware (**Hard**), **Both**, or **None**. If you are using **SLIP**, set to **Hard** only. If you are using **PPP**, set to either **Soft** or **Hard** (**Hard** is recommended). If you select **Soft** with **PPP**, you must set the **ACCM** parameter when you configure **PPP** for the **Line**.

tx-driver-control

Used with a **EIA-485** serial interface, if your application supports **RTS** (Request To Send), select this option. Otherwise, select **Auto**. Default is **Auto**.

duplex

Specify whether the line is **Full Duplex** (communication both ways at the same time) or **Half Duplex** (communication in one direction at a time).

echo-suppression

This parameter applies only to **EIA-485 Half Duplex** mode. All characters will be echoed to the user and transmitted across the serial ports. Some EIA-485 applications require local echo to be enabled in order to monitor the loopback data to determine that line contention has occurred. If your application cannot handle loopback data, echo suppression should be **On**. The default is echo suppression **Off**.

speed

Specifies the baud rate of the line; keep in mind that speed is affected by the length of the cable. You can also specify a custom baud rate; valid values are 50 - 1843200.

Set Line Service

Description Sets the service for the line. For services that need further configuration, see ***Line Service Commands*** to find the Line Service that you want to configure. SSL/TLS can be enabled for the following Line Services: DSLogin, Raw, Bidir, VModem, Server Tunnel, Client Tunnel, Modbus Master, Custom App, and TruePort.

User Level Admin

Syntax

```
set line .|<number>|* service bidir <config_host> <server_port>
<host_port> <tunnel_name>

set line .|<number>|* service direct|silent rlogin <config_host>
<tunnel_name>

set line .|<number>|* service direct raw <config_host>
<host_port> <tunnel_name>

set line .|<number>|* service silent raw <config_host>
<host_port> <tunnel_name>
[multihost all|backup <config_backup_host> <host_port>|none]

set line .|<number>|* service direct|silent telnet|ssh
<config_host> [<host_port> <tunnel_name>]

set line .|<number>|* service reverse raw [multihost on|off]|
ssh|telnet <server_port> <tunnel_name>

set line .|<number>|* service client-tunnel <config_host>
<host_port> <tunnel_name>

set line .|<number>|* service server-tunnel <server_port>

set line .|<number>|* service dslogin|printer|ppp|slip|udp|
vmodem|modbus-master|modbus-slave|custom-app|power-management

set line .|<number>|* service trueport client-initiated off
<config_host> <host_port> [signal-active on|off]
[multihost all|backup <config_backup_host> <host_port>|none
<tunnel_name>]

set line .|<number>|* service trueport client-initiated on
<server_port> [signal-active on|off] [multihost on|off]
```

Options **bidir**

This service allows the IOLAN listen for incoming TCP connection and if needed, initiate a TCP connection.

<config_host>

The name of the target host. The host must exist in the IOLAN host table.

<server_port>

The IOLAN port number.

<host_port>

The port number the target host is listening on for incoming connections.

direct

Direct connections bypass the IOLAN, enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the IOLAN is not required. It is also recommended where multiple sessions are not a requirement. The message **`Press return to continue`** is displayed on the users screen. The user must press a key to display the host login prompt. The message is redisplayed on logout.

silent

Silent connections are the same as direct connections, except they are permanently established. The host login prompt is displayed on the screen. Logging out redisplays this prompt. Silent connections, unlike direct connections, however, make permanent use of pseudo tty resources and therefore consume host resources even when not in use.

rlogin

Sets the line for a remote login connection.

raw

Creates a connection where no authentication takes place and data is passed unchanged.

telnet

Sets the line for a telnet connection.

ssh

Sets the line for an SSH connection.

reverse

Enables a TCP/IP host to establish a login connection on an external machine attached to a port. For example, to access machines like protocol converters, statistical multiplexors, or machines like routers, firewalls, servers, etc.

client-tunnel

Sets the line for a client tunnel connection.

dslogin

The default connection. The IOLAN displays a login on that line. For example, **DSLogin** is used when a System Administrator configures the IOLAN, providing authentication of a user before starting a **User Service** of **SLIP**, or users starts a session(s) from the IOLAN to hosts.

printer

Using the IOLAN as a printer server. For example, remote printing using LPD (port 515) or RCP (port 514).

ppp

Sets the port to a dedicated PPP line.

slip

Sets the port in SLIP mode.

udp

Sets the line to listen for and/or send UDP data.

vmodem

The IOLAN port behaves as if it were a modem to the attached device.

server-tunnel

Sets the line for a server tunnel connection.

modbus-master

Sets the line to act as a Modbus master.

custom-app

Sets the line to use the custom application created with the SDK.

power-management

Indicates that there is a power bar connection to this serial line.

trueport

Sets the line to communicate with the TruePort utility. You must install the TruePort utility on the host machine.

client-initiated

When this option is turned on, the IOLAN will wait for a connection from the TruePort host (see the TruePort documentation for information on how to set up this feature on the TruePort host). When this option is turned off, the IOLAN will initiate the connection to the TruePort host. The default is off.

signal-active

This option has the following impact based on the state of the TruePort connection:

- **TruePort Lite Mode**—When enabled, the EIA-232 signals remain active before, during, and after the TruePort connection is established. When disabled, the EIA-232 signals remain inactive when there is no TruePort connection and active when there is a TruePort connection.
- **TruePort Full Mode**—When enabled, the EIA-232 signals remain active before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection. When disabled, the EIA-232 signals remain inactive before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection.

Default: Enabled

multihost

Used for connections coming from the network to the serial port for TruePort or Raw services, allows multiple hosts to connect to the serial device.

multihost all|backup <*config_backup_host*> <*tcp_port*>|none

Used for connections going from the serial port to the network for TruePort or Silent Raw services, allows the serial device to communicate to either all the hosts in the multihost list or a primary/backup host schema (see *Configuring Multiple Hosts* in the *IOLAN User's Guide* for a more detailed explanation).

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Set Modem

Description Sets the modem initialization strings for a defined modem. If you wish to add a new modem, use the **`add modem`** command.

User Level Admin

Syntax **`set modem <`***`modem_name`***`> <`***`init_string`***`>`**

Options ***<modem_name>***

Predefined modem name.

<init_string>

Specify the initialization string for the modem. This can be up to 60 characters long, but cannot include spaces.

Set Termtype

Description Sets the terminal type for the current terminal session. term1, term2, and term3 refer to the user-uploadable custom terminal definitions. If these are not present, the default is wyse60.

User Level Restricted, Normal, Admin

Syntax **`set termtype [wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|term3]`**

Option **wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|term3**

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3** (user-defined terminals)

Show Line

Description Shows the line settings/information.

User Level Admin

Syntax **`show line <`***`number`***`>|*`**

Line Service Commands

Set Custom-App

Description You can create a custom application that can run on a specific serial line in IOLAN using the Perle SDK.

User Level Admin

Syntax **`set custom-app line .|<`***`number`***`>|* program-command-line <`***`command`***`>`**

Options **program-command-line**

The name of the SDK program executable that has been already been downloaded to the IOLAN, plus any parameters you want to pass to the program. Maximum of 80 characters. Use the **`shell`** CLI command as described in the *SDK Programmer's Guide* to manage the files that you have downloaded to the IOLAN. For example, using sample **`outraw`** program, you would type:

```
outraw -s 0 192.168.2.1:10001 Acct:10001
```

if you were starting the application on the Server (notice the **`-s 0`** parameter specifies Line 1).

Set Rlogin-Client

Description Configures the Rlogin parameters for the specified line. When the IOLAN initiates an rlogin connection to a host, it is acting as a rlogin client.

User Level Normal, Admin

Syntax **`set rlogin-client line .|<`***`number`***`>|* termtype <`***`terminal_name`***`>`**

Option **termtype**

Type of terminal attached to this line; for example, ansi or wyse60.

Set Telnet-Client

Description Configures the Telnet parameters for the specified line. When the IOLAN initiates a Telnet connection to a host, it is acting as a Telnet client.

User Level Normal, Admin

Syntax

```
set telnet-client line .|<number>|* [termtype <terminal_name>]
 [line-mode on|off] [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>] [eof <00-7f>] [erase <00-7f>] [intr <00-7f>]
 [quit <00-7f>] [escape <00-7f]
```

Options **termtype**

Type of terminal attached to this line; for example, ANSI or WYSE60.

line-mode

When **On**, keyboard input is not sent to the remote host until **Enter** is pressed, otherwise input is sent every time a key is pressed. Default is **Off**.

map-cr-crlf

Maps carriage returns (CR) to carriage return line feed (CRLF). The default value is **Off**.

local-echo

Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can only be used when **Line Mode** is **On**. Default is **Off**.

echo

Defines the echo character. When **Line Mode** is **On**, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal with a default value of **5** (ASCII value **^E**).

eof

Defines the end-of-file character. When **Line Mode** is **On**, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal with a default value of **4** (ASCII value **^D**).

erase

Defines the erase character. When **Line Mode** is **Off**, typing the erase character erases one character. This value is in hexadecimal with a default value of **8** (ASCII value **^H**).

intr

Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of **3** (ASCII value **^C**).

quit

Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal with a default value of **1c** (ASCII value **FS**).

escape

Defines the escape character. Returns you to the command line mode. This value is in hexadecimal with a default value of **1d** (ASCII value **GS**).

Set SSH-Client

Description Configures the SSH parameters for the specified line. When the IOLAN initiates a SSH connection to a host, it is acting as a SSH client.

User Level Normal, Admin

Syntax

```
set ssh-client line .|<number>|* [termtype <terminal_name>]
 [protocol ssh-1|ssh-2|ssh-2/1] [compression on|off]
 [verbose on|off] [auto-login on|off] [name <string>]
 [password <string>] [ssh-1-cipher 3des|des|blowfish]
 [authentication rsa on|off] [authentication dsa on|off]
 [authentication keyboard-interactive on|off]
 [strict-host-key-checking on|off]

set ssh-client line .|<number>|*
 ssh-2-cipher-list <3des blowfish cast aes arcfour>
```

Options

termtype

Type of terminal attached to this line; for example, ANSI or WYSE60.

protocol

Specify the SSH protocol you want to use for the connection, SSH-1, SSH-2, or either, SSH2/1.

compression

Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks.

verbose

Displays debug messages on the terminal.

auto-login

Creates an automatic SSH login, using the **Name** and **Password** values.

name

The user's name when **Auto Login** is enabled.

password

The user's password when **Auto Login** is enabled.

ssh-1-cipher

Select the encryption method (cipher) that you want to use for your SSH version 1 connection:

- **3DES**
- **Blowfish**

ssh-2-cipher-list

Select the order of negotiation for the encryption method (ciphers) that the IOLAN will use for the SSH version 2 connection:

- **3DES**
- **Blowfish**
- **AES**
- **Arcfour**
- **CAST**

authentication rsa

An authentication method used by SSH version 1 and 2. When enabled, an SSH client session will try to authenticate via RSA.

authentication dsa

An authentication method used by SSH version 2. When enabled, an SSH client session will try to authenticate via DSA.

authentication keyboard-interactive

The user types in a password for authentication.Used for SSH2 only.

strict-host-key-checking

When enabled, a host public key (for each host you wish to SSH to) must be downloaded into the IOLAN.

Set PPP

Description Configures the Lines PPP settings.

User Level Admin

Syntax

```
set ppp wireless-wan|line .|<number>|* [accm <8_hex_digits>]
 [address-comp on|off] [auth-tmout <integer>]
 [challenge-interval <integer>] [cr-retry <integer>]
 [cr-timeout <integer>] [ipaddr-neg on|off]
 [ipv6-global-network-address <IPv6_network_prefix>]
 [ipv6-local-interface <interface_id>]
 [ipv6-remote-interface <interface_id>]
 [lipaddr <IPV4_address>] [magic-neg on|off] [mru <64-1500>]
 [nak-retry <integer>] [netmask <IPV4_address>]
 [password <string>] [proto-comp on|off] [ripaddr <IPV4_address>]
 [roaming-callback on|off] [authentication none|pap|chap]
 [routing none|send|listen|send-and-listen] [rpassword <string>]
 [ruser <string>] [tr-retry <integer>] [tr-tmout <integer>]
 [user <string>] [vj-comp on|off]
```

Options

accm

Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream. This is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). So entering the value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected **Soft Flow Control** on the **Line**, you must enter a value of at least **000a0000** for the **ACCM**. The default value is **00000000**, which means no characters will be escaped.

address-comp

This determines whether compression of the **PPP Address** and **Control** fields take place on the link. The default is **On**. For most applications this should be enabled.

auth-tmout

The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when **PAP** or **CHAP** is turned **On**). If the timer expires before the remote end has been authenticated successfully, the link will be terminated.

challenge-interval

The interval, in minutes, for which the IOLAN will issue a CHAP re-challenge to the remote end. During CHAP authentication, an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if re-challenges are disabled. Some PPP client software does *not* work with CHAP re-challenges, so you might want to leave the parameter disabled in the IOLAN. The default value is **0** (zero), meaning CHAP re-challenge is disabled.

cr-retry

The maximum number of times a **`configure request`** packet will be re-sent before the link is terminated.

cr-timeout

The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a **`configure request`** packet to have been lost.

ipaddr-neg

Specifies whether or not IP address negotiation will take place. IP address negotiation is where the IOLAN allows the remote end to specify its IP address. The default value is **Off**. When **On**, the IP address specified by the remote end will be used in preference to the **Remote IP Address** set for a **Line**. When **Off**, the **Remote IP Address** set for the **Line** will be used.

ipv6-global-network-prefix

You can optionally specify an IPv6 global network prefix that the IOLAN will advertise to the device at the other end of the PPP link. Enter the IPv6 network prefix in the **`aaaa:bbbb:cccc:dddd::`** format.

ipv6-local-interface

The local IPv6 interface identifier of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly. The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.

ipv6-remote-interface

The remote IPv6 interface identifier of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you set the **PPP** parameter **IP Address Negotiation** to **On**, the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Interface-ID** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.

lipaddr

The IPV4 IP address of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.

magic-neg

Determines if a line is looping back. If enabled (**On**), random numbers are sent on the link. The random numbers should be different, unless the link loops back. The default is **Off**.

mru

The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the IOLAN's port will accept. Enter a value between 64 and 1500 bytes; for example, 512. The default value is **1500**. If your user is authenticated by the IOLAN, the **MRU** value will be overridden if you have set a **Framed MTU** value for the user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-MTU** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

nak-retry

The maximum number of times a **`configure NAK`** packet will be re-sent before the link is terminated.

netmask

The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Netmask** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

password

This field defines the password which is associated with the user defined by the **user** parameter. It is used to authenticate a user connecting to the IOLAN. You can enter a maximum of 16 alphanumeric characters.

proto-comp

This determines whether compression of the PPP Protocol field takes place on this link. The default is **On**.

ripaddr

The IPV4 IP address of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you set the PPP parameter IP Address Negotiation to On, the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Address** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. The exception to this rule is a **Framed-Address** value in the RADIUS file of **255.255.255.254**; this value allows the IOLAN to use the remote IP address value configured here.

roaming-callback

A user can enter a telephone number that the IOLAN will use to callback him/her. This feature is particularly useful for a mobile user. Roaming callback can only work when the **User Callback** parameter is set to **On**. Roaming callback therefore overrides (fixed) **User Callback**.To use **Roaming Callback**, the remote end must be a Microsoft Windows OS that supports Microsoft's Callback Control Protocol (CBCP). The user is allowed 30 seconds to enter a telephone number after which the IOLAN ends the call. The default is **Off**.

routing

Determines the routing mode (RIP, Routing Information Protocol) used on the **PPP** interface as one of the following options:

- **None**—Disables RIP over the PPP interface.
- **Send**—Sends RIP over the PPP interface.
- **Listen**—Listens for RIP over the PPP interface.
- **Send and Listen**—Sends RIP and listens for RIP over the PPP interface.

This is the same function as the **Framed-Routing** attribute for RADIUS authenticated users. Default is **None**.

rpassword

The **rpassword** is the password which is associated with the user defined by **ruser**. It is used to authenticate a user connecting to the IOLAN. You can enter a maximum of 16 alphanumeric characters.

ruser

This field is used to authenticate a user connecting to this line. It is used in conjunction with the **rpassword** field. By specifying a name here, this line becomes dedicated to that user only. If left blank, the internal user database will be used to authenticate the connection and any user configured will be able to access this line. You can enter a maximum of 254 alphanumeric characters.

This option does not work with external authentication.

authentication

The type of authentication that will be done on the link:

None, **PAP**, or **CHAP**. The default is **CHAP**. You can use **PAP** or **CHAP** (MD5CHAP, MSCHAP and MSCHAPv2) to authenticate a port or user on the IOLAN, from a remote location, or authenticate a remote client/device, from the IOLAN.

PAP is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.

CHAP challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated. MD5CHAP and Microsoft's MSCHAP/MSCHAPv2 are supported. The IOLAN will attempt MSCHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use

When setting either **PAP** and **CHAP**, make sure the IOLAN and the remote client/device have the same setting. For example, if the IOLAN is set to **PAP**, but the remote end is set to **CHAP**, the connection will be refused.

tr-retry

The maximum number of times a **`terminate request`** packet will be re-sent before the link is terminated.

tr-tmout

The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a **`terminate request`** packet to have been lost.

user

This field is used by a remote peer to authenticate a PPP connection on this line. It is used in conjunction with the **password** field. You can enter a maximum of 254 alphanumeric characters.

vj-comp

This determines whether Van Jacobson Compression is used on this link. The default is **On**. If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set the **User Framed Compression On**. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Compression** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

Set PPP Dynamic-DNS

Description This option is only available when IP address negotiation (**ipaddr-neg**) is **on**. When enabled, the IOLAN will automatically update the DNS server with the specified host name and negotiated IP address for the PPP session.

User Level Admin

Syntax
```
set ppp line .|<number>|* dynamic-dns [on|off]
 [hostname <hostname>] [username <username>]
 [password <password>]
```

Options

hostname

Specify the host name that will be updated with the PPP session's IP address on the DynDNS.org server.

username

Specify the user name used to access the DynDNS.org server.

password

Specify the password used to access the DynDNS.org server.

Set SLIP

Description Configures the lines SLIP settings.

User Level Admin

Syntax
```
set slip line .|<number>|* [lipaddr <IPV4_address>]
 [mtu <256-1006>] [netmask <IPV4_address>]
 [ripaddr <IPV4_address>] [vj-comp on|off]
 [routing none|send|listen|send-and-listen]
```

Options

lipaddr

The IPv4 address of the IOLAN end of the SLIP link. For routing to work you must enter an IP address in this field. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.

mtu

The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1500. The default value is **256**. If your user is authenticated by the IOLAN, this MTU value will be overridden when you have set a **Framed MTU** value for the user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-MTU** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

netmask

The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Netmask** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

ripaddr

The IPv4 address of the remote end of the SLIP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If your user is authenticated by the IOLAN, this remote IP address will be overridden if you have set a **Framed IP Address** for the user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Address** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

vj-comp

This determines whether Van Jacobson compression is used on this link; that is, whether you are using SLIP or C-SLIP (compressed SLIP). The choices are **On** (C-SLIP) or **Off** (SLIP). The default is **On**. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin.

If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set a **Framed Compression** value for a user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Compression** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.

routing

Determines the routing mode (RIP, Routing Information Protocol) used on the **SLIP** interface as one of the following options:

- **None**—Disables RIP over the SLIP interface.
- **Send**—Sends RIP over the SLIP interface.
- **Listen**—Listens for RIP over the SLIP interface.
- **Send and Listen**—Sends RIP and listens for RIP over the SLIP interface.

This is the same function as the **Framed-Routing** attribute for RADIUS authenticated users. Default is **None**.

Set UDP

Description Configures the UDP settings for the serial line.

User Level Normal, Admin

Syntax

```
set udp line .|<number>|* entry 1|2|3|4
 both auto-learn|specific <UDP_port> <tunnel_name>
 [<start_IP_address>] [<end_IP_address>]

set udp line .|<number>|* entry 1|2|3|4 in
 any-port|auto-learn|specific <UDP_port> [<start_IP_address>]
 [<end_IP_address>]

set udp line .|<number>|* entry 1|2|3|4 out <UDP_port>
 <tunnel_name> [<start_IP_address>] [<end_IP_address>]

set udp line .|<number>|* entry 1|2|3|4 none
```

Options **entry 1|2|3|4**

Selects which of the 4 available entries we wish to define/modify. For each entry the user can specify a different IP address range, UDP port and direction of data flow.

both|in|out|none

The direction in which information is received or relayed:

- **None**—UDP service not enabled.
- **In**—LAN to serial. The IOLAN will listen on port value configured in the **DS Port** parameter for messages coming from the learned or configured port.
- **Out**—Serial to LAN. The IOLAN will forward data received on the serial port to the IP address range, UDP port configured for this entry.
- **Both**—Messages are relayed in both directions. For messages coming from the LAN to the serial device, IOLAN will listen on the port value configured in the **DS Port** parameter for messages coming from the learned or configured port. For messages going from the serial device to the LAN, the IOLAN will forward the data to the IP address range and UDP port configured for this entry. If **auto-learn** is enabled, the IOLAN must receive a UDP message before it can send one, since the UDP port number is learned from the received message.

auto-learn

The IOLAN will only listen to the first port that it receives a UDP packet from. Applicable when set to **In** or **Both**.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

any-port

The IOLAN will receive messages from any port sending UDP packets. Applicable when set to **In**.

specific

The port that the IOLAN will use to relay messages to servers/hosts or the port from which the IOLAN will receive messages to be forwarded to the serial port.. This option works with any setting except **None**. The IOLAN will listen for UDP packets on the port configured by the **DS Port** parameter.

<start_IP_address>

The first host IP address in the range of IP addresses (for IPV4 or IPV6) that the IOLAN will listen for messages from and/or send messages to.

<end_IP_address>

The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the IOLAN will listen for messages from and/or send messages to.

Set Vmodem

Description Configures the vmodem settings for the serial line. SSL/TLS can be enabled and configured for this Line Service.

User Level Admin

Syntax

```
set vmodem line .|<number>|* [echo on|off]
 [failure-string <string>] [host <config_host>]
 [init-string <string>] [mode auto|manual]
 [port <TCP_port>|0] [response-delay <time_ms>]
 [signals dcd always-high|follow-connection]
 [signals dtr always-high|represent-dcd|represent-ri]
 [signals rts always-high|represent-dcd|represent-ri]
 [style numeric|verbose] [success-string <string>]
 [suppress on|off]
```

Options

echo

When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Disabled by default.

failure-string

String that is sent to the serial device when a connection fails. If no string is entered, then the string **`NO CARRIER`** will be sent.

host

The target host name.

init-string

You can specify additional vmodem commands that will affect how vmodem starts. The following commands are supported: ATQn, ATVn, ATEn, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, and ATDS1.

See *VModem Initialization Commands* in the *IOLAN User's Guide* for a more detailed explanation of the support initialization commands.

mode

Auto mode establishes the connection when the line becomes active. You must supply the AT command or phone number that will start the connection; see ***Set Vmodem-Phone*** for the command parameters to set the AT command or phone number.

port

The port number the target host is listening on for messages.

response-delay

The amount of time, in milliseconds, before an AT response is sent to the requesting device. The default is 250 ms.

signals dcd

Controls the state of the DCD signal.

- always-high = DCD signal will always stay high.
- follow-connection = DCD signal will be high when an end to end connection is established and low when it is not.

Since the IOLAN does not have a physical DCD pin, you need to re-map the DTR or RTS signal to DCD to have the signal present. (see next option).

signals dtr

You can specify how the DTR signal pin acts during your modem application connection, as itself (DTR), as DCD, or as RI.

signals rts

You can specify how the RTS signal pin acts during your modem application connection, as itself (RTS), as DCD, or as RI.

style

One of the following:

- **Verbose**—Return codes (strings) are sent to the connected device.
- **Numeric**—The following characters can be sent to the connected device:

  0 OK

  1 CONNECTED

  2 RING

  3 NO CARRIER

  4 ERROR

  6 ITERFACE DOWN

  7 CONNECTION REFUSED

  8 NO LISTNER

success-string

String that is sent to the serial device when a connection succeeds. If no string is entered, then the string **`CONNECT`** will be sent with the connecting speed, for example **`CONNECT 9600`**.

suppress

When enabled, the connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed. The default is disabled.

Set Vmodem-Phone

Description This command associates a phone number with an IP address and TCP port. This enables the existing modem application to issue a dial command with a phone number. The phone number will be searched for in this table and if an exact match is found, the associated IP address and TCP port will be used to establish the connection. This is a universal command, meaning that all VModem lines will have access to the entries defined here. 1-port models support up to 4 entries, all other desktop models support up to 8 entries, and rack mount and medical unit models support up to 48 entries.

User Level Admin

Syntax

```
set vmodem-phone entry <number> phone-number <string> [ip_address
 <number>|host <string>][port <TCP_port>] [<tunnel_name>]

set vmodem-phone entry <number> delete
```

Options

entry

Specify the entry number in the vmodem phone number table.

phone-number

Specify the phone number that your application uses to connect to remote location. Enter the number exactly as it is issued by your application.

<ip_*address*>

Specify the IP address of the remote host that is receiving the vmodem connection.

<host>

Select the host (from the host table) of the remote host that is receiving the vmodem connection.

<port>

Specify the TCP port that the remote host is listening on for the vmodem connection.

delete

Deletes the specified entry from the phone number table.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Set SSL Line

Description Sets the SSL/TLS parameters for the line. SSL/TLS can be enabled for the following Line Services: DSLogin, Raw, Bidir, VModem, Server Tunnel, Client Tunnel, Modbus Master, Custom App and Trueport.

User Level Admin

Syntax

```
set ssl line .|<number>|* [enable on|off] [use-server on|off]
 [version any|tslv1|sslv3] [type client|server]
 [verify-peer on|off] [validation-criteria
 country <code>|state-province <text>|locality <text>
 |organisation <text>|organisation-unit <text>
 |common-name <text>|email <email_addr>]
```

Options

enable

Activates the SSL/TLS settings for the line.

use-server

Uses the SSL/TLS server configuration for the line.

version

Specify whether you want to use:

- **Any**—The IOLAN will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try an SSLv2 connection.
- **TLSv1**—The connection will use only TLSv1.
- **SSLv3**—The connection will use only SSLv3.

The default is **Any**.

type

Specify whether the IOLAN will act as an SSL/TLS client or server. The default is **Client**.

verify-peer

Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.

validation-criteria

Any values that are entered in the validation criteria must match the peer certificate for an SSL connection; any fields left blank will not be validated against the peer certificate.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

Set SSL Line Cipher-suite

Note: Not all SSH encryption options are available on all formware versions.

Description Sets the SSL/TLS cipher suite parameters for the line.

User Level Admin

Syntax

```
set ssl line .|<number>|* cipher-suite
 option1|option2|option3|option4|option5
 encryption any|aes|3des|des|arcfour|arctwo|none
 min-key-size 40|56|64|128|168|256
 max-key-size 40|56|64|128|168|256
 key-exchange any|rsa|edh-rsa|edh-dss|adh
 hmac any|sha1|md5
```

Options **option1|option2|option3|option4|option5**

Sets the priority of the cipher suite, with **option1** being highest priority and **option5** lowest priority.

encryption

Select the type of encryption that will be used for the SSL connection:

- Any—Will use the first encryption format that can be negotiated.
- AES
- 3DES
- DES
- ARCFOUR
- ARCTWO
- None—Removes any values defined for the cipher option.

The default value is **Any**.

min-key-size

The minimum key size value that will be used for the specified encryption type. The default is **40**.

max-key-size

The maximum key size value that will be used for the specified encryption type. The default is **256**.

key-exchange

The type of key to exchange for the encryption format:

- **Any**—Any key exchange that is valid is used (this does not, however, include ADH keys).
- **RSA**—This is an RSA key exchange using an RSA key and certificate.
- **EDH-RSA**—This is an EDH key exchange using an RSA key and certificate.
- **EDH-DSS**—This is an EDH key exchange using a DSA key and certificate.
- **ADH**—This is an anonymous key exchange which does not require a private key or certificate. Choose this key if you do not want to authenticate the peer device, but you want the data encrypted on the SSL/TLS connection.

The default is **Any**.

hmac

Select the key-hashing for message authentication method for your encryption type:

- Any
- MD5
- SHA1

The default is **Any**.

Set Modbus-Slave Line

Description Sets the Modbus slave parameters for the line.

User Level Admin

Syntax

```
set modbus-slave line .|<number>|* [crlf on|off]
 [protocol rtu|ascii] [uid-range <uid_range>]
```

Options

crlf

When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

protocol

Specify the protocol that is used between the Modbus Master(s) and Modbus Slave(s), either RTU or ASCII.

uid-range

You can specify a range of UIDs (1-247), in addition to individual UIDs. The format is comma delimited; for example, 2-35, 50, 100-103.

Set Modbus-Master Line

Description Sets the Modbus master parameters for the line. SSL/TLS can be enabled and configured for this Line Service.

User Level Admin

Syntax

```
set modbus-master line .|<number>|* [crlf on|off]
 [protocol rtu|ascii]
 [[entry <number> [port <port>] [protocol udp|tcp]
  [range-mode gateway|host] [slave-ip <IP_address>]
  [uid-range <start_uid> <end_uid>]]
```

Options

crlf

When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

protocol

Specify the protocol that is used between the Modbus Master(s) and Modbus Slave(s), either RTU or ASCII.

entry

You can specify up to 16 Modbus Slave Remote IP Mapping entries (the UIDs must not overlap).

port

The destination port of the remote Modbus TCP Slave that the IOLAN will connect to.

protocol

Specify the protocol that is used between the Modbus Master and Modbus Slave(s), either TCP or UDP.

range-mode

If you specify **Host**, the IP address is used for the first UID specified in the range. The last octect in the IPv4 address is then incremented for subsequent UID's in that range. The **Host** option is not applicable for IPv6 addresses. If you specify **Gateway**, the Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range.

slave-ip

The IP address of the TCP/Ethernet Modbus Slave.

uid-range

When **Range Mode** is **Host** and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range and the IOLAN will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the IOLAN will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.

Set Power-Management Line

Description Configures the power management settings for the line.

User Level Admin

Syntax

```
set power-management line .|<number>|*
 [model rps820|rps830|rps1620|rps1630] [name <bar_name>]

set power-management line .|<number>|* plug <1-8|1-16>
 [default-state on|off] [name <plug_name>]
 [power-up-interval .5|1|2|5|15|30|60|120|180|300]
 [serial-line <number>] [monitor |delay <length> <number> |mode
 on|off |notify-email on|off |notify- serial on|off [host <none |
 hostname |interval <number> |timeout<number> |retries  <number>]
```

Options

model

Specify the power bar model, either RPS820, RPS830, RPS1620, RPS1630.

name (power bar name)

Specify a name for the RPS.

plug

Specify the power bar plug number you are configuring.

default-state

Sets the default state of the plug, either **on** or **off**. The default is **off**.

name (plug name)

Specify a name for the plug to make it easier to recognize and manage.

power-up-interval

Specify the amount of time, in seconds, that the power bar will wait before powering up a plug. This can be useful if you have peripherials that need to be started in a specific order.

serial-line

Associate a serial line(s) connected to a serial device that is plugged into the power bar on that plug.

- **delay**

  length - Specify a delay (in minutes) before cycling the power on the plug.

  mode - Selects whether the delay feature is enabled or disabled

  notify-email - Send an email using parameters as pre-defined under email alert

  notify-serial - Send a message to the serial port associated with this power plug. This is usually the console port on the host being monitored.

Default : 5 minutes

- **host -** This is the hostname which is to be monitored via PINGs. If the host stops responding to the PINGs, the power on that plug will be cycled in an attempt to recover the host.

Default: None

- **interval -S**pecify the frequency (in minutes) at which the configured host will be PING'ed.
- **retries -**Specify the number of times to re-try the PING when the host doeas not reply. This is in addition to the orginial PING request.

Default: 2

- **timeout** - Specify the length of time (in seconds) to wait for a reply from the host

Default: 60 seconds

Set Multihost Line

Description Configures multiple hosts or a primary/backup host schema for Silent Raw, Reverse Raw, or Client-Initiated TruePort service types (multihost must be enabled by the line service type for this to take effect, see ***Set Line Service*** for the command to enable multihost).

User Level Admin

Syntax

```
set multihost line <number> entry <number> host <host>
 <tunnel_name><TCP_port>

set multihost line <number> entry <number> delete
```

Options

entry

You can specify up to 100 hosts in the multihost table.

host <*host*>

Specify the preconfigured host that will be in the multihost list.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

<TCP_port>

Specify the TCP port that the IOLAN will use to communicate to the **Host**.

delete

Deletes the specified entry from the multihost table.

Set Line Initiate-Connection

Description Determines how the connection is initiated for Direct Telnet, Direct SSH, Direct Raw, and Direct Rlogin.
User Level Admin
Syntax **`set line <number>|* initiate-connection any-char|specific-char <hex>`**
Options **any-char**

Initiates a connection to the specified host when any data is received by the serial port.

specific-char <*hex*>

Initiates a connection to the specified host only when the specified character is received by the serial port.

Show Custom-App

Description Shows the custom application line settings.
User Level Admin
Syntax **`show custom-app line .|<number>|*`**

Show Interface

Description Shows the network interface information.
User Level Admin
Syntax **`show interface [brief|ppp|slip|ethernet]`**

Show Power-Management

Description Shows the power management settings for a line.
User Level Admin
Syntax **`show power-management line <number>`**

Show PPP

Description Shows the PPP line settings.
User Level Admin
Syntax **`show ppp line <number>|wireless-wan`**

Show Rlogin-Client

Description Show the rlogin-client settings for the line.
User Level Normal, Admin
Syntax **`show rlogin-client line <number>`**

Show SLIP

Description Show the SLIP settings for the line.
User Level Admin
Syntax **`show slip line <number>`**

Show SSH-Client

Description Shows the SSH client settings for the line.
User Level Admin
Syntax **`show ssh-client line <number>`**

Show Telnet-Client

Description Shows the telnet client settings for a line.
User Level Admin
Syntax **`show telnet-client line <`***`number`***`>`**

Show Modbus

Description Shows the Modbus settings for a line.
User Level Admin
Syntax **`show modbus master|slave <`***`number`***`>`**

Show UDP

Description Shows the UDP settings for the line.
User Level Admin
Syntax **`show udp line <`***`number`***`>`**

Show Vmodem

Description Show the vmodem settings for the line.
User Level Normal, Admin
Syntax **`show vmodem line <`***`number`***`>`**

Show Vmodem-Phone

Description Show the vmodem-phone entries.
User Level Normal, Admin
Syntax **`show vmodem-phone`**

Modem Commands

Add Modem

Description Adds a modem.
User Level Admin
Syntax **`add modem <`***`modem_name`***`> <`***`initialization_string`***`>`**

Options ***<modem_name>***

The name of the modem. Do not use spaces.

<initialization_string>

The initialisation string of the modem; see your modem's documentation.

Delete Modem

Description Deletes a modem.
User Level Admin
Syntax **`delete modem <`***`config_modem_name`***`>`**

Option ***<config_modem_name>***

You can see a the list of modems that can be deleted by typing **`delete modem ?`**.

Set Modem

Description Sets the modem initialization strings for a defined modem. If you wish to add a new modem, use the **add modem** command.
User Level Admin
Syntax **set modem <***modem_name***> <***init_string***>**

Options ***<modem_name>***

Predefined modem name.

<init_string>

Specify the initialization string for the internal modem.

Show Modems

Description Shows the IOLAN modem table.
User Level Normal, Admin
Syntax **show modems**

Email Commands

Set Email-Alert Line

Description This command configures email alert parameters for the line.
User Level Admin
Syntax
```
set email-alert line <number>|* [from <email_addr>]
 [level emergency|alert|critical|error|warning|notice|info|debug]
 [mode on|off] [to <email_addr>] [reply-to <email_addr>]
 [smtp-host <string>] [subject <string>] [use-server on|off]
```

Options **from**

This field will be specified in the **from** field of the email message sent by the IOLAN.

level

Choose the event level that triggers an email notification:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

The list is in decreasing order of priority (**Emergency** has the highest priority). You are selecting the lowest notification level; therefore, when you select **Debug**, you will get an email notification for all events that trigger a message.

mode

Determines whether or not email notification is turned on. Default is **Off**.

to

An email address or list of email addresses that will receive the email notification.

reply-to

The email address to whom all replies to the email notification should go.

smtp-host

The SMTP host (email server) that will process the email notification request. This can be either a host name defined in the IOLAN host table or the SMTP host IP address.

subject

A text string, which can contain spaces, that will display in the **Subject** field of the email notification.

use-server

Determines whether you want the **Line** to inherit the **Email Alert** settings from the **Server Email Alert**. If this is enabled, **Server** and **Line** notification events will have the same **Email Alert** setting.

Show Email-Alert Line

Description Shows how the line email alert is configured.
User Level Admin
Syntax **show email-alert line <*number*>**

Packet Forwarding Commands

Set Packet-Forwarding Line

Description The Packet Forwarding feature allows you to control how the data coming from a serial device is packetized before forwarding the packet onto the LAN network. This command configures packet forwarding options for serial devices attached to the serial line. The command is broken up into logical flows that can be configured; if you configure both the packet options and the frame definition options, the frame definition options will take precedence. If any of the packet options that are configured are met, the packet transmission is triggered.

User Level Admin

Syntax

```
set packet-forwarding line <number>|* mode minimize-latency

set packet-forwarding line <number>|* mode
 optimize-network-throughput

set packet-forwarding line <number>|* mode
 prevent-message-fragmentation delay-between-messages <0-65535>

set packet-forwarding line <number>|*
 mode custom-on-specific-events [enable-end-trigger1 on|off]
 [enable-end-trigger2 on|off] [end-trigger1 <0x0-FF>]
 [end-trigger2 <0x0-FF>] [force-transmit-timer <number>]
 [forwarding-rule trigger1|trigger+1|trigger+2|strip-trigger]
 [idle-timer <number>] [packet-size <number>]

set packet-forwarding line <number>|*
 mode custom-on-frame-definition [enable-eof1 on|off]
 [enable-eof2 on|off] [enable-sof1 on|off] [enable-sof2 on|off]
 [eof1 <0x0-FF>] [eof2 <0x0-FF>]
 [forwarding-rule trigger|trigger+1|trigger+2|strip-trigger]
 [sof1 <0x0-FF>] [sof2 <0x0-FF>] [start-frame-transmit on|off]
```

Options **minimize-latency**

This option ensures that any data received on the serial port will immediately be forwarded to the LAN. Select this option for timing-sensitive applications.

optimize-network-throughput

This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN.

prevent-message-fragmentation

This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages.

delay-between-messages

The minimum time, in milliseconds, between messages that must pass before the data is forwarded by the IOLAN. The range is 0-65535. The default is 250 ms.

custom-on-specific-events

This section allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, if you set a **Force Transmit Timer** of **1000** ms and a **Packet Size** of **100** bytes, whichever criteria is met first is what will cause the packet to be transmitted.

custom-on-frame-definition

This section allows you to control the frame that is transmitted by defining the start and end of frame character(s). If the internal buffer (1024 bytes) is full before the EOF character(s) are received, the packet will be transmitted and the EOF character(s) search will continue. The default frame definition is SOF=00 and EOF=00.

enable-end-trigger1

Enable or disable the end trigger1 hex character.

enable-end-trigger2

Enable or disable the end trigger2 hex character.

enable-end-eof1

Enable or disable the eof1 (end of frame) hex character.

enable-end-eof2

Enable or disable the eof2 (end of frame) hex character.

enable-end-sof1

Enable or disable the sof1 (start of frame) hex character.

enable-end-sof2

Enable or disable the sof2 (start of frame) hex character.

end-trigger1

When enabled, specifies the character that when received will define when the packet is ready for transmission. The transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

end-trigger2

When enabled, creates a sequence of characters that must be received to specify when the packet is ready for transmission (if the End Trigger1 character is not immediately followed by the End Trigger2 character, the IOLAN waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

eof1

Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

eof2

When enabled, creates a sequence of characters that must be received to define the end of the frame (if the EOF1 character is not immediately followed by the EOF2 character, the IOLAN waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

force-transmit-timer

When the specified amount of time, in milliseconds, elapses after the first character is received from the serial port, the packet is transmitted. After a packet is transmitted, the next character received starts the timer again. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.

forwarding-rule

Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options:

- **Strip-Trigger**—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.
- **Trigger**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.
- **Trigger+1**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger.
- **Trigger+2**—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger.

idle-timer

The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.

packet-size

The number of byte that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-1024 bytes. The default is 0.

sof1

When enabled, the Start of Frame character defines the first character of the frame, any character(s) received before the Start of Frame character is ignored. Valid values are in hex 0-FF. The default is 0.

sof2

When enabled, creates a sequence of characters that must be received to create the start of the frame (if the SOF1 character is not immediately followed by the SOF2 character, the IOLAN waits for another SOF1 character to start the SOF1/SOF2 character sequence). Valid values are in hex 0-FF. The default is 0.

start-frame-transmit

When enabled, the SOF1 or SOF1/SOF2 characters will be transmitted with the frame. If not enabled, the SOF1 or SOF1/SOF2 characters will be stripped from the transmission.

Show Packet-Forwarding Line

Description Shows the packet-forwarding settings for the line.
User Level Admin
Syntax **`show packet-forwarding line <`***`number`***`>`**

5 Network Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's network parameters.

SNMP Commands

Add Community

Description Adds an SNMP community (version 1 and version 2).

User Level Admin

Syntax **`add community <`***`community_name`***`> <`***`config_host`***`>|<`***`IP_address`***`> none|readonly|readwrite`**

Options ***<community_name>***

The name of the group that devices and management stations running SNMP belong to.

<config_host>|<IP_address>

The host name of the SNMP community that will send requests to the IOLAN.

The IPv4 or IPv6 address of the SNMP manager that will send requests to the IOLAN. If the address is **`0.0.0.0`**, any SNMP manager with the **Community Name** can access the IOLAN. If you specify a network address, for example **`172.16.0.0`**, any SNMP manager within the local network with the **Community Name** can access the IOLAN.

none|readonly|readwrite

Permits the IOLAN to respond to SNMP requests by:

- **None**—There is no response to requests from SNMP.
- **Readonly**—Responds only to Read requests from SNMP.
- **Readwrite**—Responds to both Read and Write requests from SNMP.

Add Trap

Description Adds an SNMP host to which trap messages will be sent. The IOLAN supports SNMP traps for restart and SNMP community authentication error.

User Level Admin

Syntax **`add trap <`***`config_host`***`>|<`***`IP_address`***`> <version> <type> <tunnel_name> <`***`Community`***`>`**

Options ***<Community>***

The trap receiver is the network management system (NMS) that should receive the SNMP traps. This NMS must have the same SNMP community string as the trap sender.

<config host>|<IP address>

Defines the hosts (by IPv4 or IPv6 address) that will receive trap messages generated by the IOLAN. Up to four trap hosts can be defined.

<version>

Select the version of trap you want the IOLAN to send. Valid options are v1, v2c and v3.

<type>

Select trap or inform. Inform requires the receiving host to acknowledge receipt of the trap.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Delete Community

Description Deletes an SNMP community (version 1 and version 2).
User Level Admin
Syntax **`delete community <`***`config_community_number`***`>`**

Option ***<config_community_number>***

When you add an SNMP community, it gets assigned to a number. To delete the SNMP community, you need to specify the number of the community that you want to delete. To see which community is assigned to what number, type the **`show snmp`** command.

Delete Trap

Description Deletes an SNMP trap host.
User Level Admin
Syntax **`delete trap <`***`config_trap_number`***`>`**

Option ***<config_trap_number>***

When you add an SNMP trap host, it gets assigned to a number. To delete the SNMP trap host, you need to specify the number of the trap host that you want to delete. To see which trap host is assigned to what number, type the **`show snmp`** command.

Set SNMP

Description Configures SNMP settings.
User Level Admin
Syntax **`set snmp [contact <`***`string`***`>] [location <`***`string`***`>] [readonly user <`***`username`***`>] [readwrite user <`***`username`***`>] [trap user <`***`username`***`>]`**

Options **contact**

The name and contract information of the person who manages this SMNP node.

location

The physical location of the SNMP node.

readonly user

(SNMP version 3) Specify the name of the read only user.

readwrite user

(SNMP version 3) Specify the name of the read/write user.

trap user

(SNMP version 3) Specify the name of the trap user.

Set SNMP V3-Security

Description Configures SNMP settings for the Version 3 read-write, read-only and trap user(s).

User Level Admin

Syntax

```
set snmp v3-security [type readonly|readwrite|trap]
 [security-level none|auth/nopriv|auth/priv][auth-algorithm
 md5|sha1][auth-password][privacy-algorithm des|aes]
 [privacy-password]
```

Options

type

Select the user type you wish to configure. The options are readonly, readwrite and trap.

security-level

Select the security level for the user type being defined. The valid options are:

none- no security or authentication will be used.

auth/nopriv - authentication but no privacy will be used.

auth/priv - both authentication and privacy will be used.

auth-algorithm

Specify the authentication algorithum that will be used for this user. The options are md5 or sha1

The default is md5.

auth-password

After pressing <enter> you will be prompted for the authentication password. The password must be a minimum of 8 characters long. You will be prompted to re-enter the password to ensure accuracy.

privacy-algorithm

Specify the privacy (encryption) algorithum that will be used for this user. The options are des or aes.

The default is des.

privacy-password

After pressing <enter> you will be prompted for the privacy password. The password must be a minimum of 8 characters long. You will be prompted to re-enter the password to ensure accuracy.

Set SNMP engine-id-string

Description Configures SNMP v3 Engine ID.
User Level Admin
Syntax **`set snmp engine-id-string <string>`**

Options **string**

The string entered in this field will be combined with the defined string in hex of 800007AE04 to form the engine-id. Ensure each string is unique for each IOLAN on your network. The default engine-id uses the MAC address of the Ethernet interface on your IOLAN to ensure that the Engine-id is unique to this agent. To set the engine id back to default, enter a null <"">.

Set SNMP inform-timeout

Description Configures SNMP inform traps timeout value.
User Level Admin
Syntax **`set snmp inform-timeout <number>`**
Options **number**

This is the length of time in seconds, that the IOLAN will wait for the acknowledgement of the trap. If no ACK is received within this time, the trap will be resent. The default is 1 second.

Set SNMP inform-retries

Description Configures SNMP inform traps number of retires.
User Level Admin
Syntax **`set snmp inform-retires <number>`**
Options **number**

This is the number of times the IOLAN will resend a trap which has not been acknowledged by the receiving end. Once the retry count is exhausted, no further attempts will be made to deliver the trap. The default is 3 retries.

Show SNMP

Description Shows SNMP settings, including communities and traps.
User Level Admin
Syntax **`show snmp`**

TFTP Commands

Set Server TFTP

Description Configures the IOLANs TFTP client settings.
User Level Admin
Syntax **`set server tftp [retry <`*`integer`*`>] [timeout <`*`integer`*`>]`**

Options **retry**

The number of times the IOLAN will retry to transmit a TPFT packet to/from a host when no response is received. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the IOLAN will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the IOLAN will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

SFTP Commands

Set Server SFTP

Description Configures the IOLANs SFTP client settings.
User Level Admin
Syntax

```
set server sftp [host <config host>][authentication rsa on|off]
 [authentication dsa on|off] [authentication keyboard-interactive
 on|off]] [auto-login on|off] [name <string>] [password <string>]
 [compression on|off] [protocol ssh1|ssh2|ssh2-1] [ssh-1-cipher
 3des|blowfish] [ssh-2-cipher-list
 3des|blowfish|aes|cast|arcfour]
```

Options **host**

This is the name of the SFTP host. The name must come from the IOLAN host table. You can see a list of hosts available for selection by typing `? after host.`

authentication

You can individually enable/disable each of the three available authentication methods. They are rsa, dsa or keyboard-interactive. At least one method must be enabled. The default is to have all enabled.

auto-login

You can have the **IOLAN** automatically login to the SFTP server. When set, it will use the “Name” and “Password” configured using these keywords.

`name`

This is the name that will be used when automatically logging into the SFTP host.

`password`

This is the password that will be used when automatically logging into the SFTP host.

compression

Enables compression of all data. Compression is desirable on slow connections but may actually slow things down on fast network connections.

protocol

Select the protocol you are willing to use with the SFTP server. You can enable SSH1, SSH2 or both. At least one protocol must be enabled.

`ssh-1-cipher`

Select the encryption cipher to be used with SSH1. The options are "3des" or "blowfish". You must select one of the two if you enable the SSH1 protocol.

`ssh-2-cipher-list`

Select the list of encryption cipher(s) to be used with SSH2. The options are 3des, blowfish, aes, cast and arcfour. The list is in order of preference with the first cipher being the most desirable and the fifth being the least desirable. At least one of the ciphers needs to be included in the list if the SSH2 protocol is enabled.

Show SFTP

Description Shows the SFTP settings.
User Level Admin
Syntax `show sftp`

Hosts Commands

Add Host

Description Adds a host to the IOLAN host table.
User Level Admin
Syntax **add host <***hostname***> <***IP_address***>**

add host <*hostname***> fqdn <***text***>**

Options ***<hostname>***

The name of the host.

<IP_address>

The host IPv4 or IPv6 address.

fqdn

When you have DNS defined in the IOLAN, you can enter a DNS resolvable fully qualified domain name (note: FQDN's are excluded as accessible hosts when **IP Filtering** is enabled).

Delete Host

Description Deletes a host from the IOLAN host table.
User Level Admin
Syntax **delete host <***config_host***>**

Option ***<config_host>***

You can see a list of hosts that can be deleted by typing **delete host ?**.

Set Host

Description Configures a host in the IOLAN host table.
User Level Admin
Syntax **set host <***config_host***> <***IP_address***>**

set host <*config_host***> fqdn <***text***>**

Options ***<config_host>***

The name of the host.

<IP_address>

The host IPv4 or IPv6 address.

fqdn

When you have DNS defined in the IOLAN, you can enter a DNS resolvable fully qualified domain name (note: FQDN's are excluded as accessible hosts when **IP Filtering** is enabled).

Show Hosts

Description Shows the IOLAN host table.
User Level Normal, Admin
Syntax **show hosts**

DNS/WINS Commands

Add DNS

Description Adds a DNS entry.
User Level Admin
Syntax **`add dns <`***`IP_address`***`>`**

Option **<***IP_address***>**

You can specify the IPv4 or IPv6 addresses for up to four DNS (Domain Name Servers) hosts in your network.

Add WINS

Description Adds a WINS entry.
User Level Admin
Syntax **`add wins <`***`IP_address`***`>`**

Option **<***IP_address***>**

You can specify the IPv4 addresses for up to four WINS (Windows Internet Naming Service) hosts in your network.

Delete DNS

Description Deletes a DNS entry.
User Level Admin
Syntax **`delete dns <`***`config_dns_addr`***`>`**

Option **<***config_dns_addr***>**

You can view a list of configured DNS server IP addresses to choose from by typing **`delete dns ?`**.

Delete WINS

Description Deletes a WINS entry.
User Level Admin
Syntax **`delete wins <`***`config_wins_addr`***`>`**

Option **<***config_wins_addr***>**

You can view a list of configured WINS server IP addresses to choose from by typing **`delete wins ?`**.

Show DNS

Description Shows all DNS entries, even those supplied by DHCP/BOOTP when applicable.
User Level Admin, Normal
Syntax **`show dns`**

Show Server

Description Shows the server configuration, including configured WINS or DNS servers.
User Level Admin, Normal
Syntax **`show server`**

Show WINS

Description Shows all WINS entries, even those supplied by DHCP/BOOTP when applicable.
User Level Admin, Normal
Syntax **show wins**

Gateway Commands

Add Gateway

Description Adds a gateway. You can configure up to twenty gateways.
User Level Admin
Syntax

```
add gateway <config_host> default

add gateway <config_host> host <dest_IP_addr>

add gateway <config_host> network
 <dest_IPv4_addr>|<dest_IPv6_addr>
 [<subnet_bits_0-32>|<prefix_bits_0-128>]

add gateway specify-gateway ipv6tunnel <tunnel_name> default|
 host <dest_IP_addr>|
 network <dest_IPv4_addr>|<dest_IPv6_addr>
 [<subnet_bits_0-32>|<prefix_bits_0-128>]

add gateway specify-gateway serial-port ppp <line_name>|
 slip <line_name> default|
 host <dest_IP_addr>|
 network <dest_IPv4/IPv6_addr>
 [<subnet_bits_0-32>|<prefix_bits_0-128>]
```

Options ***<config_host>***

You can specify up to 20 hosts on desktop models and 49 hosts on rack mount and medical unit models to act as gateways in your network. Each gateway host must be defined in the IOLAN's host table.

default|host|network

Specify the type of gateway:

- **Default**—A gateway which provides general access beyond your local network.
- **Host**—(Default) A gateway reserved for accessing a specific host external to your local network.
- **Network**—A gateway reserved for accessing a specific network external to your local network.

ipv6tunnel *<tunnel_name>*

Specify the configured IPv6 tunnel that you want to use as the gateway to the destination.

serial-port ppp|slip *<line_name>*

Specify the PPP or SLIP configured line that you want to use as the gateway to the destination.

<dest_IP_addr>

When the gateway is a **Host** or **Network** gateway, you must specify the IPv4 or IPv6 address of the target host machine/network.

<subnet_bits>|<prefix_bits>

When the gateway is a **Network** gateway, you must specify the network's subnet mask (IPv4) or prefix bits (IPv6).

Delete Gateway

Description Deletes a gateway.
User Level Admin
Syntax **`delete gateway <`***`config_gateway_host`***`>`**
Option ***<config_gateway_host>***

You can view the configured gateways that can be deleted by typing **`delete gateway ?`**.

Set Gateway

Description Configures the gateway.
User Level Admin
Syntax

```
set gateway <config_gateway_host> default

set gateway <config_gateway_host> host <destination_ip>

set gateway <config_gateway_host>
 network <dest_IPv4_addr>|<dest_IPv6_address> <prefixbits_mask>
```

Options ***<config_gateway_host>***

You can view the configured gateways that can be deleted by typing **`delete gateway ?`**.

default|host|network

Specify the type of gateway:

- **Default**—A gateway which provides general access beyond your local network.
- **Host**—(Default) A gateway reserved for accessing a specific host external to your local network.
- **Network**—A gateway reserved for accessing a specific network external to your local network.

<destination_ip>

When the gateway is a **Host** or **Network** gateway, you must specify the IPv4 or IPv6 address of the target host machine/network.

<prefixbits_mask>

When the gateway is a **Network** gateway, you must specify the network's subnet mask for an IPv4 destination IP address (the address is in the form of 123.123.123.123) or prefix bits for an IPv6 destination IP address (valid values are 0-128).

Show Gateways

Description Shows configured gateways.
User Level Normal, Admin
Syntax **`show gateways`**

Logging Commands

Set Syslog

Description Configures the system log.
User Level Admin
Syntax

```
set syslog
 [level emergency|alert|critical|error|warning|notice|info|debug]
 [primary-host <config_host>] [secondary-host
 <config_host>]<tunnel_name>
```

Options **level**

Choose the event level that triggers a syslog entry:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

When you select a **Level**, all the levels that appear above it in the list also trigger a syslog entry. For example, if you select **Error**, all **Error**, **Critical**, **Alert**, and **Emergency** events will be logged.

primary-host

The first preconfigured host that the IOLAN will attempt to send system log messages to; messages will be displayed on the host's monitor.

secondary-host

If the IOLAN cannot communicate with the primary host, then the IOLAN will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Show Syslog

Description Shows the syslog settings.
User Level Admin
Syntax

```
show syslog
```

RIP Commands

Add RIP

Description Adds a RIP MD5 key. After pressing **Enter**, you will be prompted for the MD5 key value.

User Level Admin

Syntax **add rip md5 <***integer_md5_id***> <***start_date***> <***start_time***> <***end_date***> <***end_time***>**

Options **<***integer_md5_id***>**

The **MD5** identification key.

<*start_date***>**

The start date that the MD5 key becomes valid. The date format is dependent on your system's settings.

<*start_time***>**

The time that the MD5 key becomes valid. The time format is dependent on your system's settings.

<*end_date***>**

The last day that the MD5 key is valid. The date format is dependent on your system's settings.

<*end_time***>**

The time that the MD5 key becomes invalid. The time format is dependent on your system's settings.

Delete RIP

Description Deletes a RIP MD5 key.

User Level Admin

Syntax **delete rip md5 <***integer_md5_id***>**

Option **<***integer_md5_id***>**

You can see a list of MD5 IDs available for deletion by typing **delete rip md5 ?**.

Set RIP

Description Configures the RIP MD5 key. After pressing Enter, you will be prompted for the MD5 key value.

User Level Admin

Syntax

```
set rip [authentication none|password|md5]
 [ethernet-mode none|send|listen|send-and-listen]

set rip password

set rip md5 <config_md5_id> [end <date> <time>]
 [start <date> <time>] [key]
```

Options **authentication**

Specify the type of RIP authentication:

- **None**—No authentication for RIP.
- **Password**—Simple RIP password authentication.
- **MD5**—Use MD5 RIP authentication.

ethernet-mode

Enable/disable RIP (Routing Information Protocol) mode for the Ethernet interface with one of the following options:

- **None**—Disables RIP over the Ethernet interface.
- **Send**—Sends RIP over the Ethernet interface.
- **Listen**—Listens for RIP over the Ethernet interface.
- **Send and Listen**—Sends RIP and listens for RIP over the Ethernet interface.

password

When you type the **`set rip password`** command and press **Enter**, you will be prompted to type in a password and then re-enter that password.

<*configured_md5_id*>

The **MD5** identification key.

end <*date*> <*time*>

The last day that the MD5 key is valid. Specify as ***dd/mm/yyyy***.

The time that the MD5 key becomes invalid. Specify as ***hh:mm***:[***ss***].

start <*date*> <*time*>

The start date that the MD5 key becomes valid. Specify as ***dd/mm/yyyy***.

The time that the MD5 key becomes valid. Specify as ***hh:mm***:[***ss***].

key

When you press **Enter** after typing the **`key`** command, you will be prompted to enter the MD5 key value and then re-enter the key value.

Show RIP

Description Shows the RIP settings.
User Level Normal, Admin
Syntax **`show rip`**

Show RIP Peers

Description Shows current information about IPv4 or IPv6 RIP peers.
User Level Normal, Admin
Syntax **`show rip peers [ipv6]`**

IPsec Commands

Once there is an active VPN tunnel, the IOLAN expects all connections to be established through a VPN tunnel. To allows hosts to connect outside of the VPN tunnel, you must configure VPN exceptions, see ***VPN Exceptions*** for the command syntax.

Add IPsec

Description Adds an IPsec tunnel.
User Level Admin
Syntax **add ipsec <***tunnel_name***>**

Option ***<tunnel_name>***

The name of an IPsec VPN tunnel. You can configure up to 64 VPN tunnels.

Set IPsec

Description Configures the IPsec tunnel.
User Level Admin
Syntax

```
set ipsec <config_tunnel_name>
 [authentication-method shared-secret|rsa-signature|x.509-certificate]
 [boot-action start|add|ignore] [local-device left|right]
 [local-external-ip-address <IPv4/IPv6_address/FQDN>]
 [local-host-network <IPv4_addr> <subnet_mask>|
                     <IPv6_address> <prefix_bits>]
 [local-ip-address <IPv4/IPv6_address/FQDN>]
 [local-next-hop <IPv4/IPv6_address>]
 [remote-external-ip-address <IPv4/IPv6_address/FQDN>]
 [remote-host-network <IPv4_addr> <subnet_mask>|
                     <IPv6_address> <prefix_bits>]
 [remote-ip-address <IPv4/IPv6_address/FQDN>]
 [remote-next-hop <IPv4/IPv6_address>]
 [remote-validation-criteria
   country <code>|state-province <text>|locality <text>
   |organisation <text>|organisation-unit <text>
   |common-name <text>|email <email_addr>]

set ipsec <config_tunnel_name> secret <text>

set ipsec use-nat-traversal enabled|disabled
```

Options **authentication-method**

Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.

Data Options:

- **Shared Secret**—A text-based secret that is used to authenticate the IPsec tunnel (case sensitive).
- **RSA Signature**—RSA signatures are used to authenticate the IPsec tunnel. When using this authentication method, you must download the IPsec RSA public key to the IOLAN and upload the IPsec RSA public key from the IOLAN to the VPN gateway.
- **X.509 Certificate**—X.509 certificates are used to authenticate the IPsec tunnel. When using this authentication method, you must include the signing authority's certificate information in the SSL/TLS CA list and download it to the IOLAN.

The default is shared secret.

boot-action

Determines the state of the VPN network when the IOLAN is booted.

- **Start**—Starts the VPN network, initiating communication to the remote VPN.
- **Add**—Adds the VPN network, but doesn't initiate a connection to the remote VPN.
- **Ignore**—Maintains the VPN network configuration, but the VPN network is not started and cannot be started through the IPsec command option.

When defining peer VPN gateways, one side should be defined as **Start** (initiate) and the other as **Add** (listen). It is invalid to define both gateways as **Add**. VPN connection time can take longer when both gateways are set to **Start**, as both sides will attempt to initiate the same VPN connection.

The default is start.

local-device

When the VPN tunnel is established, one side of the tunnel is designated as Right and the other as Left. You are configuring the IOLAN-side of the VPN tunnel. The default is left.

local-external-ip-address

When **NAT Traversal (NAT_T)** is enabled, this is IOLAN's external IPv4 or IPv6 address or FQDN. When the IOLAN is behind a NAT router, this will be its public IP address.

local-host-network

The IPv4 or IPv6 address of a specific host, or the network address that the IOLAN will provide a VPN connection to.

local-ip-address

The IPv4 or IPv6 address or FQDN of the IOLAN. You can specify **`%defaultroute`** when the IP address of the IOLAN is not always known (for example, when it gets its IP address from DHCP). When **`%defaultroute`** is used, a default gateway must be configured in the route table.

local-next-hop

The IPv4 or IPv6 address of the router/gateway that will forward data packets to the remote VPN (if required). The router/gateway must reside on the same subnet at the IOLAN. Leave this parameter blank if you want to use the **Default Gateway** configured in the IOLAN.

remote-external-ip-address

When **NAT Traversal (NAT_T)** is enabled, the remote VPN's public external IPv4 or IPv6 address or FQDN. If you want to accept a VPN connection from any host/network, you can enter **`%any`** in this field.

remote-host-network

The IPv4 or IPv6 address of a specific host or the network address that the IOLAN will provide a VPN connection to. If the IPsec tunnel is listening for connections (**Boot Action** set to **Add**), and the field value is left at **`0.0.0.0`**, any VPN peer with a private remote network/host that conforms to RFC 1918 (10.0.0.0/8, 172.16.0.0./12, 192.168.0.0/16) will be allowed to use this tunnel if it successfully authenticates.

remote-ip-address

The IPv4 or IPv6 address or FQDN of the remote VPN peer. If you want to accept a VPN connection from any VPN peer, you can enter **`%any`** in this field.

remote-next-hop

The IPv4 or IPv6 address of the router/gateway that will forward data packets to the IOLAN (if required). The router/gateway must reside on the same subnet at the remote VPN.

remote-validation-criteria

Any values that are entered in the remote validation criteria must match the remote X.509 certificate for a succsessful connection; any fields left blank will not be validated against the remote X.509 certificate. Note that all validation criteria must be configured to match the X.509 certificate. An asterick (*) is valid as a wildcard.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

secret

When the **Authentication Method** is set to **Shared Secret**, enter the case-sensitive secret word. Maximum of 16 characters, spaces not allowed. The secret is shared for all IPsec and L2TP/IPsec tunnels.

use-nat-traversal

NAT Traversal should be enabled when the IOLAN is communicating through a router/gateway to a remote VPN that also has NAT Traversal enabled. By default, this is enabled.

Show IPsec

Description Displays an IPsec tunnel.
User Level Admin
Syntax `show ipsec <config_tunnel_name>`
Option ***<config_tunnel_name>***

Displays the configuration information for the specified IPsec tunnel.

IPsec

Description Controls the state of all IPsec tunnels.
User Level Admin
Syntax `ipsec start|stop|restart|status`
Options **start**

Starts all IPsec VPN tunnels.

stop

Stops all IPsec VPN tunnels.

restart

Stops and then starts all IPsec VPN tunnels.

status

Used strictly for debugging, displays trace data for all IPsec tunnels.

IPv6 Tunnels

Add IPv6tunnel

Description Adds a new IPv6 tunnel.
User Level Admin
Syntax `add ipv6tunnel <tunnel_name>`
Option ***<tunnel_name>***

Adds the specified IPv6 tunnel.

Set IPv6tunnel

Description Configures the specified IPv6 tunnel.
User Level Admin
Syntax `set ipv6tunnel <config_tunnel_name> [mode manual|teredo|6to4] [gateway <interface>] [remote-host <config_host>]`

Options **mode**

The method or protocol that is used to create the IPv6 tunnel.

- **Manual**—When enabled, the IOLAN will manually create the IPv6 tunnel to the specified **Remote Host** through the specified **Interface**.
- **6to4**—When enabled, the IOLAN will broadcast to the multicast address 192.88.99.1 through the specified **Interface**. When the closest 6to4 router responds, it will create the IPv6 tunnel, encapsulating and decapsulating IPv6 traffic sent to and from the IOLAN.
- **Teredo**—When enabled, the Teredo protocol encapsulates the IPv6 packet as an IPv4 UDP message, allowing it to pass through most network address translator (NAT) boxes and create an IPv6 tunnel to the specified **Remote Host** (a Teredo server) through the specified **Interface**.

Default: Manual

gateway

The interface that the IOLAN is going to use to access the Remote Host. The list is comprised of the Ethernet interface(s) and serial ports configured PPP or SLIP.

Default: ethernet_1

remote-host

The IPv4 host that can access the IPv6 network when the **Mode** is **Manual**.

The Teredo server when the **Mode** is **Teredo**.

Default: None

Show IPv6tunnel

Description Shows the specified IPv6 tunnel settings.
User Level Admin
Syntax `show ipv6tunnel <config_tunnel_name>`

Delete IPv6tunnel

Description Controls the state of all IPsec tunnels.
User Level Admin
Syntax `delete ipv6tunnel <config_tunnel_name>`
Options *<config_tunnel_name>*

Deletes the specified IPv6 tunnel. If a tunnel is associated with a gateway, it cannot be deleted until the gateway is either changed or deleted.

L2TP/IPsec

Once L2TP/IPsec is enabled, the IOLAN expects all connections to be established through a VPN tunnel. To allows hosts to connect outside of the VPN tunnel, you must configure VPN exceptions, see ***VPN Exceptions*** for the command syntax.

Set L2TP

Description

User Level Admin

Syntax

```
set l2tp listen-for-l2tp on|off

set l2tp authentication-method shared-secret [secret <text>]

set l2tp authentication-method x.509-certificate
 remote-validation-criteria  [country <code>]
 [state-province <text>] [locality <text>] [organisation <text>]
 [organisation-unit <text>] [common-name <text>]
 [email <email_addr>]

set l2tp [ipsec-local-ip-address <ipv4_addr>]
 [local-ip-address <ipv4_addr>]
 [remote-ipv4-start-address <start_ip>]
 [remote-ipv4-end-address <end_ip>]
 [authentication-type pap|chap|both]
```

Options

listen-for-l2tp

When enabled, allows L2TP/IPsec VPN connections. Note: to allow non-VPN connections to the IOLAN, you must create entries in the VPN Exceptions list. The default is **off**.

authentication method shared-secret|x.509-certificate

Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.

Data Options:

- **Shared Secret**—A text-based secret that is used to authenticate the IPsec tunnel (case sensitive).
- **X.509 Certificate**—X.509 certificates are used to authenticate the IPsec tunnel. When using this authentication method, you must include the signing authority's certificate information in the SSL/TLS CA list and download it to the IOLAN.

Default: Shared Secret

secret

When the **Authentication Method** is **Secret**, enter the case-sensitive secret word. Maximum of 16 characters, spaces not allowed. The secret is shared for all IPsec and L2TP/IPsec tunnels.

remote-validation-criteria

Any values that are entered in the remote validation criteria must match the remote X.509 certificate for a succsessful connection; any fields left blank will not be validated against the remote X.509 certificate. Note that all validation criteria must be configured to match the X.509 certificate. An asterick (*) is valid as a wildcard.

country

A two character country code; for example, US. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

state-province

Up to a 128 character entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

locality

Up to a 128 character entry for the location; for example, a city. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

organisation

Up to a 64 character entry for the organisation; for example, Accounting. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

organisation-unit

Up to a 64 character entry for the unit in the organisation; for example, Payroll. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

common-name

Up to a 64 character entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

email

Up to a 64 character entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the remote X.509 certificate. An asterisk (*) works as a wildcard.

ipsec-local-ip-address

The IPv4 address that the IOLAN will listen on for L2TP/IPsec connections. If the default value (0.0.0.0) is kept, the IOLAN will use the **Default Gateway** value (if no **Default Gateway** is specified, L2TP/IPsec VPN connections will error out).

Default: 0.0.0.0

local-ip-address

Specify the unique IPv4 address that hosts accessing the IOLAN through the L2TP tunnel will use.

Field Format: IPv4 address

local-ipv4-start-address

Specify the first IPv4 address that can be assigned to incoming hosts through the L2TP tunnel.

Field Format: IPv4 address

local-ipv4-end-address

Specify the end range of the IPv4 addresses that can be assinged to incoming hosts through the L2TP tunnel.

Field Format: IPv4 address

authentication-type

Specify the authentication method that will be used for the L2TP tunnel.

Data Options: CHAP, PAP, Both

Default: Both

Show LT2P

Description Shows the L2TP settings.
User Level Admin
Syntax **`show l2tp`**

VPN Exceptions

VPN exceptions allows specific hosts or any host in a network to connect to the IOLAN outside of a VPN tunnel.

Add VPN Exception

Description Adds a VPN exception.
User Level Admin
Syntax **`add vpn-exception network-ip <`***`ipv4_net_ip`***`> <`***`network_subnet`***`>|`**
`<`*`ipv6_net_ip`***`> <`***`prefix_bits`***`>`**

`add vpn-exception host-ip <`*`ipv4/ipv6_address`***`>`**

Options **network-ip <*ipv4_net_ip*> <*network_subnet*>|<*ipv6_net_ip*> <*prefix_bits*>**

The network address that will communicate with the IOLAN outside of the VPN tunnel. If the address is IPv4, you can supply the subnet mask for the network (the default is 0.0.0.0). If the address is IPv6, you can supply the prefix bits for the network (the default is 64, the range is 0-128).

host-ip <*ipv4/ipv6_address*>

The IP address of the host that will communicate with the IOLAN outside of the VPN tunnel.

Field Format: IPv4 or IPv6 address

Set VPN Exception

Description Configures an existing VPN exception.
User Level Admin
Syntax **`set vpn-exception <`***`config_vpn_except`***`>`**
`network-ip <`*`ipv4_address`***`> <`***`network_subnet`***`>|`**
`<`*`ipv6_address`***`> <`***`prefix_bits`***`>`**

`set vpn-exception <`*`config_vpn_except`***`> host-ip <`***`ipv4/ipv6_address`***`>`**

Options **network-ip <*ipv4_net_ip*> <*network_subnet*>|<*ipv6_net_ip*> <*prefix_bits*>**

The network address that will communicate with the IOLAN outside of the VPN tunnel. If the address is IPv4, you can supply the subnet mask for the network (the default is 0.0.0.0). If the address is IPv6, you can supply the prefix bits for the network (the default is 64, the range is 0-128).

host-ip <*ipv4/ipv6_address*>

The IP address of the host that will communicate with the IOLAN outside of the VPN tunnel.

Field Format: IPv4 or IPv6 address

Delete VPN Exception

Description Deletes a VPN exception. To see a list of configured VPN exceptions, type **`delete vpn-exception ?`**
User Level Admin
Syntax **`delete vpn-exception <`***`config_vpn_except`***`>`**

Show VPN Exception

Description Shows the configured VPN exceptions.
User Level Admin
Syntax **`show vpn-exception`**

HTTP Tunnel Commands

Add http-tunnel

Description Adds an http-tunnel or connection.
User Level Admin
Syntax **`add http-tunnel [`***`tunnel <text>|connection <1-100> <text> tcp <text>|udp <text> <number> local-port<number> ipalias <ipv4address> |limit-access on|off]`***
Options **text**

Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer IOLAN DS.

Range: 0-15 alpha-numeric characters.

connection

The number of the connection.
Range: 1-100.

tcp

Use TCP protocol.

text

The IPV4/IPV6 address or host name of the final destination host.

Field Format: IPV4/IPV6 address or host name)

udp

Use UDP protocol.

text

The IPV4/IPV6 address or host name of the final destination host.

Field Format: IPV4/IPV6 address or host name)

remote number

The port number of the application on the final destination host.

local-port

The local port on the IOLAN that will send and receive data.

ipalias
Users can access the HTTP tunnel through this IP address. Typically this field is only needed if the IOLAN has a listener on the same local TCP port. If not entered, the IP address of the IOLAN is used.

Field Format: IPV4/IPV6 address.

limit-access
Allow only attached serial devices to connect to this destination.

Field Format: off or on

Set http_tunnel

Description Configures an existing http tunnel.
User Level Admin
Syntax

```
set http_tunnel [proxy domain<text> host<text> keepalive<1-255>
 maximum-connection-age<1-65535> password<text> port<1-65535>
 user<text>]

set http-tunnel [tunnel <tunnel_name> https <off|on> limit-access
 <off|on> listen-ip <internet address> mode <connect <text> |
 listen>]
```

Options

proxy

If a proxy server is being used, proxy specific paramters can be configured.

domain

Specific the domain name of the proxy server.

host

The host/IP address of the proxy server.

keepalive

Specify the number of seconds between sending keepalives for HTTP connections.

maximum-connection-age

The maximum amount of time an HTTP connection will stay open.

Field Format: 1-65535
Default: 1440 mins (1 day)

password

The "password" which will be used by the IOLAN to authenticate with the proxy server.

port
The HTTP port number of the Proxy server

Default: 8080

user

The "username" which will be used by the IOLAN to authenticate with the proxy server.

tunnel-name

Select an exisiting tunnel. This tunnel must match the tunnel name on the tunnel peer IOLAN DS

https
The IOLAN will use secure access (HTTPS) mode to connect to the listening IOLAN DS.

limit-access
Allow only attached serial devices to connect to this destination.

Field Format: off or on

listen-ip
Provide the IP address of the listening Terminal Server DS.

mode

Connect or listen

connect

Provide the Host name or IP address of the listening IOLAN DS.

listen

Listen for connection requests generated from the connecting IOLAN DS.

Delete HTTP Tunnel

Description Deletes a HTTP tunnel connection.
User Level Admin
Syntax `delete http-tunnel [connection <number> | tunnel <tunnel_name>]`

Show HTTP Tunnel

Description Shows the configured HTTP tunnels.
User Level Admin
Syntax `show http-tunnel tunnel`

Time Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's time parameters.

Server Commands

Set Time

Description Sets the IOLAN's system clock.
User Level Admin
Syntax **`set time <`***`hh:mm[:ss]`***`>`**

Option **<*hh*:*mm*[:*ss*]>**

Sets the IOLAN's system time, using the 24-hour clock time format (00:00-23:59).

Set Timezone

Description Sets the IOLAN's time zone name and its offset from Greenwich Mean Time (UTC).
User Level Admin
Syntax **`set timezone [name <`***`string`***`>] [offset +|-<`***`hh[:mm]`***`>]`**

Options <*name*>

The name of the time zone to be displayed during standard time. Maximum 4 characters and minimum 3 characters (do not use angled brackets < >).

offset

The offset from UTC for your local time zone. Specify in the format of hours *hh* (valid -12 to +14) and minutes *mm* (valid 0 to 59 minutes) for the offset from UTC.

Show Time

Description Shows the IOLAN's system clock.
User Level Normal, Admin
Syntax **`show time`**

Show Timezone

Description Shows the time zone settings.
User Level Admin
Syntax **`show timezone`**

SNTP Commands

Add SNTP

Description Adds an SNTP server.
User Level Admin
Syntax **`add sntp [server-1 <`*`config_host`*`>] [server-2 <`*`config_host`*`>]`**

Options **server-1**

The name of the primary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

server-2

The name of the secondary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

Delete SNTP

Description Deletes an SNTP server.
User Level Admin
Syntax **`delete sntp server-1|server-2`**

Options **server-1**

The name of the primary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

server-2

The name of the secondary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

Set SNTP

Description Configures an SNTP server.
User Level Admin
Syntax **`set sntp mode none|unicast|anycast|multicast [server-1 <`*`config_host`*`>] [server-2 <`*`config_host`*`> <tunnel_name>] [version 1|2|3|4][server-authentication on|off] [keyid-1 <1-65534>] [keyid-2 <1-65534>]`**

Options **mode**

The SNTP mode. Valid modes are:

- **None**—SNTP is turned off.
- **Unicast**—Sends a request packet periodically to the Primary host. If communication with the Primary host fails, the request will be sent to the Secondary host.
- **Multicast**—Listen for any broadcasts from an NTP/SNTP server and then synchronizes its internal clock to the message.
- **Anycast**—Sends a request packet as a broadcast on the LAN to get a response from any NTP/SNTP server. The first response that is received is used to synchronize its internal clock and then operates in **Unicast** mode with that NTP/SNTP server.

server-1

The name of the primary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

server-2

The name of the secondary NTP/SNTP server from the IOLAN host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the IOLAN will only accept broadcasts from the specified host NTP/SNTP server.

version

Version of SNTP. Valid values are 1 to 4. Default value is **4**.

server-authentication

Sets NTP/SNTP server authentication On or Off.

Default: Off

keyid-1/keyid-2

Specify the key id associated with this ntp/sntp server (1 or 2). This key must exist in the ntp/sntp (symmetric key) file that was downloaded to the IOLAN.

Valid keyids: 1-65534

(**Note:** the structure for the ntp/sntp (symmetric key) file can be found in your *IOLAN User's Guide - Appendix L*)

Show SNTP

Description Shows the SNTP settings.
User Level Admin
Syntax `show sntp`

Show SNTP-Info

Description Shows current SNTP information.
User Level Admin
Syntax `show sntp-info`

Time/Date Setting Commands

Set Date

Description Sets the IOLAN's system clock.
User Level Admin
Syntax `set date <dd/mm/yyyy>`

Set Summertime

Description Sets the summertime clock.
User Level Admin
Syntax `set summertime [mode none|fixed|recurring] [name <text>] [offset <minutes>]`

Options **mode**

You can configure the summer time to take effect:

- **None**—No summer time change.
- **Fixed**—The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 pm.
- **Recurring**—The summer time changes goes into effect every year at same relative time. For example, on the third week in April on a Tuesday at 1:00 pm.

<*name***>**

The name of the configured summer time zone; this will be displayed during the summer time setting. Maximum 4 characters and minimum 3 characters (do not use angled brackets < >). If this parameter is not set, then the summertime feature will not work.

offset

The offset from standard time in minutes. Valid values are 0 to 180 minutes.

Set Summertime Fixed

Description Sets the summertime clock to start on the same date each year, for example, April 15 at 1:00 pm.

User Level Admin

Syntax

```
set summertime fixed
 [start-date january|february |...  <0-31>] [start-time <hh:mm>]
 [end-date january|february|... <0-31>] [end-time <hh:mm>]
```

Options **start-date**

The date to change to summer time and end standard time.

start-time <*hh***:***mm***>**

The time to change to summertime. Valid values are 00:00 to 23:59.

end-date

The date to end summer time and start standard time.

end-time <*hh***:***mm***>**

The time to change to standard time. Valid values are 00:00 to 23:59.

Set Summertime Recurring

Description Sets the summertime clock to start at the same relative time each year; for example, on the third week in April on a Tuesday at 1:00 pm.

User Level Admin

Syntax

```
set summertime recurring [start-day monday|tuesday|...]
 [start-month january|february|...] [start-time <hh:mm>]
 [start-week 1|2|3|4|5|last] [end-day monday|tuesday|...]
 [end-month january|february|...] [end-time <hh:mm>]
 [end-week 1|2|3|4|5|last]
```

Options **start-day**

The day to change to summer time from standard time.

start-month

The month to change to summer time from standard time.

start-time

The time to change to summer time from standard time; uses the format hh:mm for a 24-hour clock (00:00-23:59).

start-week

The week to change to summer time from standard time.

end-day

The day to end summer time and start standard time.

end-month

The month to end summer time and start standard time.

end-time

The time to end summer time and start standard time; uses the format hh:mm for a 24-hour clock (00:00-23:59).

end-week

The week to end summer time and start standard time.

Show Date

Description Shows the date, according to the IOLAN system clock.
User Level Normal, Admin
Syntax `show date`

Show Summertime

Description Shows the summertime settings.
User Level Admin
Syntax `show summertime`

Administration Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's administration parameters.

Bootup Commands

Reboot

Description Reboots the IOLAN. You will be prompted to save configuration to FLASH, if there have been unsaved configuration changes.
User Level Admin
Syntax **`reboot`**

Reset

Description Resets the user profile or serial line to the default factory configuration.
User Level Admin
Syntax **`reset user .|<`***`username`***`>|*`**

`reset line <`*`number`***`>|*`**

Reset Serial Statistics

Description Resets the serial port statistics.
User Level Admin
Syntax **`reset serial-statistics [<line number>|*]`**

Reset Factory

Description Resets the IOLAN to the factory configuration.
User Level Admin
Syntax **`reset factory`**

Save

Description Saves the configuration to FLASH.
User Level Admin
Syntax **`save`**

Set Bootup

Description Specifies remote the TFTP host and pathname for files to be loaded after a IOLAN reboot or indicates that SFTP should be used.

User Level Admin

Syntax

```
set bootup firmware host <hostname> [firmware file
 <path_filename>] [firmware sftp on|off]

set bootup configuration host <hostname> [configuration file
 <path_filename>] [configuration sftp on|off]
```

Options

firmware file

The path and file name, relative to the default path of your TFTP server software, of the update software for the IOLAN that will be loaded when the IOLAN is rebooted.

configuration file

The path and file name, relative to the default path of your TFTP server software, of the configuration software for the IOLAN that will be loaded when the IOLAN is rebooted.

host

The host name or IP address of the server that contains the configuration or firmware file. If you use a host name, it must exist in the IOLAN's host table or be resolved by DNS.

firmware sftp or configuration sftp

If this parameter is set to on, the IOLAN will use SFTP to transfer the firmware or configuration file. The sftp specific parameters are set using the "set sftp...." command. If the host is configured using this command, it will be used instead of the one configured by the "set sftp host" command.

Show ARP

Description Shows the current contents of the ARP cache.

User Level Admin

Syntax

```
show arp
```

Show text-config

Description Shows the current configuration of the IOLAN in text format on the console.

User Level Admin

Syntax

```
show text-config
```

Set cli

Description Allows normal users to execute certain admin commands.

User Level Admin

Syntax

```
set cli [elevate-privileges on|off]
```

Show Bootup

Description Shows the Firmware and Configuration files specified for IOLAN bootup.

User Level Admin

Syntax

```
show bootup
```

TFTP File Transfer Commands

Netload

Description Transfers a file from a remote host to the IOLAN using the TFTP protocol.

User Level Admin

Syntax

```
netload text-config|factory-default-config|firmware|
 configuration|customlang|term1|term2|term3|customapp-file|
 wan-driver <hostname|IP_address> <*> <filename>
```

Options

text-config

Specify this option if you are uploading a text-based configuration file to the IOLAN from a TFTP server.

factory-default-config

Specifies the configuration file that you are going to load from a TFTP server to the IOLAN that will act as the factory default configuration. See the *User Guide* for directions on how to revert back to the original factory default configuration, if required.

firmware

Specifies that you are going to download a new firmware file to the IOLAN.

configuration

Specifies that you are going to download a new configuration file to the IOLAN.

customlang

Specifies that you are going to download a custom language file to the IOLAN.

term1|term2|term3

You can create and download up to three custom terminal definitions to the IOLAN.

customapp-file

You can download multiple SDK program executables and ancillary files using this command by running the command multiple times to download multiple files. Use the **`shell`** CLI command as described in the *SDK Programmer's Guide* to manage the files that you download.

wan-driver

Download wireless WAN custom drivers to the IOLAN that have been downloaded from the Perle website.

<hostname|IP_address>

The IP address or host name where the file you are downloading to the IOLAN resides. If you are using a host name, it must be resolved in either the IOLAN's **Host Table** or a DNS server.

<*>

Select * to use the preconfigured HTTP tunnel.

<filename>

The complete path and file name of the file you are downloading to the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

Netsave

Description Transfers a file from the IOLAN to a remote host using the TFTP protocol.
User Level Admin
Syntax **netsave configuration|crash|serialt-buf|text-config <*hostname/IP_address*> <*filename*>**

Options **configuration**

Specifies that you are going to upload a configuration file from the IOLAN to the specified host or IP address.

crash

Specifies that you are going to upload a crash file from the IOLAN to the specified host or IP address.

serialt-buf

Specifies that you are going to upload the contents of the serial trace buffer.

text-config

Saves the current configuration to a text file on a TFTP server.

<hostname/IP_address>

The IP address or host name for where the file you are uploading from the IOLAN is going. If you are using a host name, it must be resolved in either the IOLAN's **Host Table** or a DNS server.

<filename>

The complete path and file name for the file you are uploading from the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

SFTP File Transfer Commands

Snetload

Description Transfers a file from a remote host to the IOLAN using the SFTP protocol.
User Level Admin
Syntax **snetload text-config|factory-default-config|firmware| configuration|customlang|term1|term2|term3|customapp-file| wan-driver <*hostname|IP_address*> <*> <*filename*>**

Options **text-config**

Specify this option if you are uploading a text-based configuration file to the IOLAN from a SFTP server.

factory-default-config

Specifies the configuration file that you are going to load from a SFTP server to the IOLAN that will act as the factory default configuration. See the *User Guide* for directions on how to revert back to the original factory default configuration, if required.

firmware

Specifies that you are going to download a new firmware file to the IOLAN.

configuration

Specifies that you are going to download a new configuration file to the IOLAN.

customlang

Specifies that you are going to download a custom language file to the IOLAN.

term1|term2|term3

You can create and download up to three custom terminal definitions to the IOLAN.

customapp-file

You can download multiple SDK program executables and ancillary files using this command by running the command multiple times to download multiple files. Use the **`shell`** CLI command as described in the *SDK Programmer's Guide* to manage the files that you download.

wan-driver

Download wireless WAN custom drivers to the IOLAN that have been downloaded from the Perle website.

<hostname|IP_address|user@host or >

The IP address or host name where the file you are downloading to the IOLAN resides. If using SFTP, you must specify a user. Specify the host in the following format.

user@host where;

user - the user name to use.

host - can be a fully qualified name, a name from the host table or the IPV4 or IPV6 address.

If you have not configured the password using the "set sftp password" command, you will be prompted to enter it.

<*>

Select * to use the preconfigured HTTP tunnel.

<filename>

The complete path and file name of the file you are downloading to the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

Snetsave

Description Transfers a file from the IOLAN to a remote host using the SFTP protocol.

User Level Admin

Syntax **`snetsave configuration|crash|serialt-buf|text-config <`***`hostname|IP_address`***`> <`***`filename`***`>`**

Options **configuration**

Specifies that you are going to upload a configuration file from the IOLAN to the specified host or IP address.

crash

Specifies that you are going to upload a crash file from the IOLAN to the specified host or IP address.

serialt-buf

Specifies that you are going to upload the contents of the serial trace buffer.

text-config

Saves the current configuration to a text file on a SFTP server.

<hostname/IP_address|*>

The IP address or host name where the file you are downloading to the IOLAN resides. If using SFTP, you must specify a user. Specify the host in the following format.

user@host where;

user - the user name to use.

host - can be a fully qualified name, a name from the host table or the IPV4 or IPV6 address. IPV6 address needs to be enclosed within square brackets.

* preconfigured tunnel

If you have not configured the password using the set sftp password command, you will be prompted to enter it.

<filename>

The complete path and file name for the file you are uploading from the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

Custom Factory Default

Netload

Description Transfers a file from a remote host to the IOLAN using the TFTP protocol.

User Level Admin

Syntax **`netload factory-default-config <`***`hostname|IP_address`***`> <*> <`***`filename`***`>`**

Options **factory-default-config**

Specifies the configuration file that you are going to load from a SFTP/TFTP server to the IOLAN that will act as the factory default configuration. See the *User Guide* for directions on how to revert back to the original factory default configuration, if required.

<hostname|IP address>

Enter the host or IP address that contains the certificate/key you are downloading to the IOLAN. If you are using a host name, If you are using a host name, it must be resolved in either the IOLAN's **Host Table** or a DNS server.

<*>

Select * to use the preconfigured tunnel.

<filename>

The complete path and file name of the file you are downloading to the IOLAN (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).

Snetload

Description Transfers a file from a remote host to the IOLAN using the SFTP protocol.

User Level Admin

Syntax **`snetload factory-default-config <`***`hostname|IP_address`***`> <*> <`***`filename`***`>`**

Options **factory-default-config**

Specifies the configuration file that you are going to load from a SFTP/TFTP server to the IOLAN that will act as the factory default configuration. See the *User Guide* for directions on how to revert back to the original factory default configuration, if required.

<hostname/IP_address|*>

The IP address or host name where the file you are downloading to the IOLAN resides. If using SFTP, you must specify a user. Specify the host in the following format.

user@host where;

user - the user name to use.

host - can be a fully qualified name, a name from the host table or the IPV4 or IPV6 address. IPV6 address needs to be enclosed within square brackets.

If you have not configured the password using the set sftp password command, you will be prompted to enter it.

<*>

Select * to use the preconfigured tunnel.

<filename>

The complete path and file name of the file you are downloading to the IOLAN (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).

Set

Description Sets the current configuration on IOLAN to act as the factory default configuration. See the *User Guide* for directions on how to revert back to the original factory default configuration, if required.

User Level Admin

Syntax `set config-to-factory-default`

Keys and Certificates Commands

Netload

Description Loads certificates and keys into the IOLAN using TFTP.

User Level Admin

Syntax

netload ssl certificate|private-key <*hostname/IP_address***>**
<*filename***>**

netload ssh-client host <*config_host***> public-key ssh-1 rsa**
<*hostname/IP_address***> <***filename***>**

netload ssh-client host <*config_host***> public-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

netload ssh-client user <*config_user***> private-key ssh-1 rsa**
<*hostname/IP_address***> <***filename***>**

netload ssh-client user <*config_user***> private-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

netload ssh-server user <*config_user***> public-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

netload ipsec <*config_tunnel_name***> public-key rsa**
<*hostname|IP_address***> <***filename***>**

netload sntp-keys <*hostname|IP_address***> <***filename***>**

Options

ssl certificate|private-key

If you are using the secure version of the WebManager (HTTPS), or LDAP authentication with TLS, then you need to download the SSL/TLS private key and CA list to make a secure connection.

ssh-client host

The public key for the host that is being authenticated by the IOLANs SSH server.

public-key ssh-1

Specify ssh-1 when you are using SSH version 1.

public-key ssh-2

Specify ssh-2 when you are using SSH version 2.

rsa|dsa

When downloading keys to the IOLAN, specify the authentication method used by the key.

ssh-client user

The user that the SSH key is for.

ssh-server user

The user that the SSH key is for.

ipsec <*tunnel_name***>**

When you configure an IPsec tunnel with an **Authentication Method** of **RSA Signature**, you need to download the RSA key from the remote VPN gateway to the IOLAN for that specific tunnel.

<*hostname*/*IP_address*>

Enter the host or IP address that contains the certificate/key you are downloading to the IOLAN. If you are using a host name, If you are using a host name, it must be resolved in either the IOLAN's **Host Table** or a DNS server.

<*filename*>

Enter the complete path and file name of the certificate/key you are downloading to the IOLAN.

sntp-keys

Enter the complete path and file name of the sntp file that you are downloading to the IOLAN.

Netsave

Description Uploads certificates and keys from the IOLAN to a remote host using TFTP.

User Level Admin

Syntax **netsave ssh-server public-key ssh-2 rsa|dsa <*hostname/IP_address*> <*filename*>**

netsave ipsec public-key rsa <*hostname/IP_address*> <*filename*>

Options **rsa|dsa**

When uploading SSH keys from the IOLAN, specify the SSH authentication method used by the SSH key.

ipsec public-key rsa

When you configure an IPsec tunnel with an **Authentication Method** of **RSA Signature**, you need to upload the RSA key from the IOLAN to the remote VPN gateway host for that specific tunnel.

<*hostname*/*IP_address*>

The IP address or host name for where the SSH key you are uploading from the IOLAN is going. If you are using a host name, it must be resolved in either the IOLAN's **Host Table** or a DNS server.

<*filename*>

The complete path and file name for the file you are uploading from the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

Snetload

Description Loads certificates and keys into the IOLAN using SFTP.

User Level Admin

Syntax

snetload ssl certificate|private-key <*hostname/IP_address|**>**
<*filename***>**

snetload ssh-client host <*config_host***> public-key ssh-1 rsa**
<*hostname/IP_address***> <***filename***>**

snetload ssh-client host <*config_host***> public-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

snetload ssh-client user <*config_user***> private-key ssh-1 rsa**
<*hostname/IP_address***> <***filename***>**

snetload ssh-client user <*config_user***> private-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

snetload ssh-server user <*config_user***> public-key ssh-2 rsa|dsa**
<*hostname/IP_address***> <***filename***>**

snetload ipsec <*config_tunnel_name***> public-key rsa**
<*hostname/IP_address***> <***filename***>**

snetload sntp-keys <*hostname/IP_address***> <***filename***>**

Options

ssl certificate|private-key

If you are using the secure version of the WebManager (HTTPS), or LDAP authentication with TLS, then you need to download the SSL/TLS private key and CA list to make a secure connection.

ssh-client host

The public key for the host that is being authenticated by the IOLANs SSH server.

public-key ssh-1

Specify ssh-1 when you are using SSH version 1.

public-key ssh-2

Specify ssh-2 when you are using SSH version 2.

rsa|dsa

When downloading keys to the IOLAN, specify the authentication method used by the key.

ssh-client user

The user that the SSH key is for.

ssh-server user

The user that the SSH key is for.

ipsec <*tunnel_name***>**

When you configure an IPsec tunnel with an **Authentication Method** of **RSA Signature**, you need to download the RSA key from the remote VPN gateway to the IOLAN for that specific tunnel.

<*hostname*/*IP_address*>

The IP address or host name where the file you are downloading to the IOLAN resides. If using SFTP, you must specify a user. Specify the host in the following format.

user@host where;

user - the user name to use.

host - can be a fully qualified name, a name from the host table or the IPV4 or IPV6 address. IPV6 addresses needs to be enclosed within square brackets.

If you have not configured the password using the set sftp password command, you will be prompted to enter it.

<*filename*>

Enter the complete path and file name of the certificate/key you are downloading to the IOLAN.

sntp-keys

Enter the complete path and file name of the sntp file that you are downloading to the IOLAN.

Snetsave

Description Uploads certificates and keys from the IOLAN to a remote host using SFTP.

User Level Admin

Syntax

```
snetsave ssh-server public-key ssh-2 rsa|dsa
 <hostname/IP_address> <filename>

netsave ipsec public-key rsa <hostname/IP_address> <filename>
```

Options

rsa|dsa

When uploading SSH keys from the IOLAN, specify the SSH authentication method used by the SSH key.

ipsec public-key rsa

When you configure an IPsec tunnel with an **Authentication Method** of **RSA Signature**, you need to upload the RSA key from the IOLAN to the remote VPN gateway host for that specific tunnel.

<*hostname*/*IP_address*>

The IP address or host name where the file you are downloading to the IOLAN resides. If using SFTP, you must specify a user. Specify the host in the following format.

user@host where;

user - the user name to use.

host - can be a fully qualified name, a name from the host table or the IPV4 or IPV6 address. IPV6 address needs to be enclosed within square brackets.

If you have not configured the password using the "set sftp password" command, you will be prompted to enter it.

<*filename*>

The complete path and file name for the file you are uploading from the IOLAN (this path should be relative to the default path of your TFTP server, which may or may not allow drive letters).

MOTD Commands

Set MOTD

Description Specifies the server/file that contains the message of the day (MOTD) that is displayed when users log into the IOLAN. You can also retrieve the MOTD from a local file (it must already be downloaded to the IOLAN using the **`netload customapp-file`** command); to do this, do not specify the host parameter.

User Level Normal, Admin

Syntax

```
set motd [display on|off] [host <hostname><*>] [file
 <path_filename>][sftp on|off]
set motd file <local_file>
```

Options

display

When enabled, displays the Message of the Day to users who are logging into WebManager or EasyPort Web. The default is off.

host

The host that the IOLAN will be getting the Message of the Day file from.

<*>

Select * to use the preconfigured HTTP tunnel.

<path_filename>

The path and file name, relative to the default path of your TFTP server software, of the file that contains a string that is displayed when a user connects to the IOLAN.

sftp

If this parameter is set to on, the IOLAN will use SFTP to retrieve the motd. The sftp specific parameters are set using the "set sftp...." command. If the host is configured using this command, it will be used instead of the one configured by the "set sftp host" command.

<local_file>

This is the name of a file already downloaded to the IOLAN. The contents of this file will be used for the MOTD.

Show MOTD

Description Show the Message of the Day (MOTD) settings.

User Level Admin

Syntax

```
show motd
```

Statistics Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's statistics parameters.

Configuration Statistics

Show Netstat

Description Shows currently used TCP/UDP sockets/ports.
User Level Admin
Syntax `show netstat [all] [listening] [tcp] [udp] [tcpv6] [updv6]`
Options **all**

Displays all ports, including server (listening) ports; by default, listening ports are not displayed.

listening

Displays server (listening) ports; by default, listening ports are not displayed.

tcp

Displays TCP port statistics.

udp

Displays UDP port statistics.

tcpv6

Displays TCPv6 port statistics.

udpv6

Displays UDPv6 port statistics.

Show Netstat Statistics

Description Shows protocol (IP/ICMP/TCP/UDP) counters.
User Level Admin
Syntax `show netstat statistics [ip] [ipv6] [icmp] [icmpv6] [tcp] [udp] [udp6]`

Show Modbus Statistics

Description Shows the Modbus statistics.
User Level Admin
Syntax **`show modbus statistics master-tcp line *|<`***`number`***`>`**

`show modbus statistics master-udp line *|<`*`number`***`>`**

`show modbus statistics slave-tcp line *|<`*`number`***`>`**

`show modbus statistics slave-udp line *|<`*`number`***`>`**

Show Routes

Description Shows current information about IPv4 or IPv6 network routes.
User Level Admin
Syntax **`show routes [ipv6]`**

Run-Time Statistics

Delete Arp

Description Delete entries from the IOLAN's ARP cache. Takes effect immediately; not related to configuration.
User Level Admin
Syntax **`delete arp`**

Show Arp

Description Shows the current contents of the ARP cache.
User Level Admin
Syntax **`show arp`**

Show Serial

Description Shows statistics on the serial port.
User Level Admin
Syntax **`show serial [<`***`line_number`***`>]`**

Uptime

Description Displays the elapsed time (in days, hours, minutes, and seconds) since the last reboot/power cycle.
User Level Admin
Syntax **`uptime`**

IOLAN+ User Commands

You can configure the IOLAN using the IOLAN+ menu. See the *IOLAN+ User's Guide* for the command line interface and menu parameters. See ***IOLAN+ Interface*** in the *IOLAN User's Guide* for a list of changes to the IOLAN+ menu.

IOLAN+

Description Displays the IOLAN+ configuration menu.
User Level Admin
Syntax `iolan+`

I/O Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's I/O parameters.

Global I/O Commands

Set IO UDP

Description Sets the UDP settings for I/O unicast messages.

User Level Admin

Syntax

```
set io udp [mode on|off]
 [broadcast-interval <broadcast_interval>]

set io udp entry 1|2|3|4 disabled

set io udp entry 1|2|3|4 <udp_port> <start_ip> [<end_ip>]
```

Options

mode

Enables/disables UDP broadcast of I/O channel status (data).

broadcast-interval

Enter the interval, in seconds, for UDP broadcasts of I/O channel status (data). Valid values are 1-9999. Default value is 30 seconds.

entry

You can specify up to four sets of UDP IP address that will receive the I/O unicast.

udp_port

The UDP port that the IOLAN will use to relay messages to servers/hosts.

start_ip

The first host IP address in the range of IP addresses (for IPV4 or IPV6) that the IOLAN will listen for messages from and/or send messages to.

end_ip

The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the IOLAN will listen for messages from and/or send messages to.

Set IO Failsafe

Description Sets the failsafe (watchdog) settings for I/O.
User Level Admin
Syntax `set io failsafe [mode on|off] [timeout <seconds>]`
Options **mode**

Enables/disables the **Failsafe Timer**. This is the global setting that must be enabled to set the **Failsafe Action** on the channel for digital outputs and relays. When this timer expires because of no I/O activity within the specified time interval, the **Failsafe Action** set for the channel determines the action on the output.

timeout

The number of seconds that must elapse with no I/O activity before the channel **Failsafe Action** is triggered. Valid values are 1-9999. The default is 30 seconds.

Set IO Modbus

Description Enabling the Modbus option makes the IOLAN act as a Modbus Slave, allowing Modbus Masters to communicate with the IOLAN to control and/or retrieve I/O data.
User Level Admin
Syntax `set io modbus [mode on|off] [uid <1-255>]`
Options **mode**

Enables/disables Modbus as the communication protocol for all the I/O channels.

uid

This is the UID you are assigning to the IOLAN, which is acting as a Modbus slave.

Set IO Temperature-Scale

Description Sets the temperature scale that will be used for all I/O temperature readings.
User Level Admin
Syntax `set io temperature-scale celsius|fahrenheit`
Option **temperature-scale**

Select the temperature scale that will be used to display temperature data, either Fahrenheit or Celsius. The default is Celsius.

Set Line

Set Line Service

Description Sets the **Line Service** settings for signal I/O. When the line service is set to signal-io, you also have the option of enabling the I/O extension for the serial signal pins. See ***Set IOChannel IOExtension*** for more information.
User Level Admin
Syntax `set line <number> service signal-io`
Option **signal-io**

Sets the line to use signal I/O. You still need to define the serial pins for digital input (CTS, DSR, or DCD) or digital output (RTS or DTR). See ***Set IOChannel Digital Input (Serial Pins)*** or ***Set IOChannel Digital Output (Serial Pins)*** for configuration options.

Set IOChannel

Set IOChannel Mode

Description Sets general I/O channel settings for the specified channel, these settings are available to all channels and I/O serial pins.

User Level Admin

Syntax **`set iochannel <`***`i/o_channel`***`> [mode enabled|disabled] [description <`***`string`***`>]`**

Options ***i/o_channel***

Specify the channel number, for example, d2 or a4. Temperature models use Analog input, so the channel numbers are a1-a4.

mode

Enables the channel, allowing the settings to become active.

description

Provide a description of the channel, making it easier to identify. The channel description can be up to 20 characters.

Set IOChannel Digital I/O

Description Sets up the Digital I/O channel to act as either an output or input channel.

User Level Admin

Syntax **`set iochannel <`***`digital_channel`***`> resource-type input|output`**

Options ***digital_channel***

Specify the Digital channel number, for example, d2.

source-type

Specify whether the channel will drive the line (output) or will be reading the status of the line (input). The default is **Input**. The internal jumpers must match the software configuration, so if you change this setting to **Output**, you will have to also change the internal hardware jumpers.

Set IOChannel Digital Input

Description Sets the Digital input settings for the channel.

User Level Admin

Syntax

```
set iochannel <digital_channel>
 [alarm [trigger disabled|inactive-input|active-input]
   [clear auto|manual] [email on|off] [syslog on|off]
   [snmp on|off]]
 [description <string>] [invert-signal on|off]
 [latch disabled|inactive-to-active|active-to-inactive]
```

Options ***digital_channel***

Specify the Digital channel number, for example, d2.

alarm

Configures alarm settings when the Digital input trigger is activated.

trigger

When the trigger condition is met, triggers the specified alarm action. Triggers can be:

- **Disabled**—No alarm settings. This is the default.
- **Inactive**—When the expected Digital input is active, going inactive will trigger an alarm.
- **Active**—When the expected Digital input is inactive, going active will trigger an alarm.

clear

Specify **Manual** to manually clear an alarm. Specify **Auto** to automatically clear the alarm when the trigger condition changes; for example, if the **Trigger** is **Inactive** and the alarm is triggered, once the input becomes active again, the alarm will be cleared when **Auto** is set. The default is **Auto**.

email

Sends an email alert to an email account(s) set up in the Server settings (the Line Email Alert settings are not used with this feature) when an alarm is triggered or cleared. The email alert data includes the severity level and the value that caused the alarm to trigger or clear. The **Email Alert** is associated with **Level Critical**.

syslog

Sends a message to syslog when an alarm is triggered or cleared. The syslog entry includes the severity level and the value that caused the alarm to trigger or clear. The syslog message is associated with **Level Critical**.

snmp

Sends an SNMP trap when an alarm is triggered or cleared. The trap consists of the severity level and whether the alarm was triggered or cleared.

description

Provide a description of the channel, making it easier to identify. The channel description can be up to 20 characters.

invert-signal

Inverts the actual condition of the I/O signal in the status; therefore, an inactive status will be displayed as active.

latch

Latches (remembers) the activity transition (active-to-inactive or inactive-to-active). The latched status is maintained until it is read. Once it is read, it will revert to the current status. The default is disabled.

Set IOChannel Digital Input (Serial Pins)

Description Sets the Digital input settings for serial pins CTS, DSR, and DCD. This option is only available when the **Line Service** is set to **Signal I/O**.

User Level Admin

Syntax

```
set iochannel cts|dsr|dcd
 [alarm [trigger disabled|inactive-input|active-input]
   [clear auto|manual] [email on|off] [syslog on|off]
   [snmp on|off]]
 [description <string>] [invert-signal on|off]
 [latch disabled|inactive-to-active|active-to-inactive]
```

Options ***digital_channel***

Specify the Digital channel number, for example, d2.

alarm

Configures alarm settings when the Digital input trigger is activated.

trigger

When the trigger condition is met, triggers the specified alarm action. Triggers can be:

- **Disabled**—No alarm settings. This is the default.
- **Inactive**—When the expected Digital input is active, going inactive will trigger an alarm.
- **Active**—When the expected Digital input is inactive, going active will trigger an alarm.

clear

Specify **Manual** to manually clear an alarm. Specify **Auto** to automatically clear the alarm when the trigger condition changes; for example, if the **Trigger** is **Inactive** and the alarm is triggered, once the input becomes active again, the alarm will be cleared when **Auto** is set. The default is **Auto**.

email

Sends an email alert to an email account(s) set up in the Server settings (the Line Email Alert settings are not used with this feature) when an alarm is triggered or cleared. The email alert data includes the severity level and the value that caused the alarm to trigger or clear. The **Email Alert** is associated with **Level Critical**.

syslog

Sends a message to syslog when an alarm is triggered or cleared. The syslog entry includes the severity level and the value that caused the alarm to trigger or clear. The syslog message is associated with **Level Critical**.

snmp

Sends an SNMP trap when an alarm is triggered or cleared. The trap consists of the severity level and whether the alarm was triggered or cleared.

description

Provide a description of the channel, making it easier to identify. The channel description can be up to 20 characters.

invert-signal

Inverts the actual condition of the I/O signal in the status; therefore, an inactive status will be displayed as active.

latch

Latches (remembers) the activity transition (active-to-inactive or inactive-to-active). The latched status is maintained until it is read. Once it is read, it will revert to the current status. The default is disabled.

Set IOChannel Digital Output

Description Sets the Digital output channel settings.

User Level Admin

Syntax

```
set iochannel <digital_channel>
 [type sink|source|sink-and-source] [active-signal-width <width>]
 [inactive-signal-width <width>]
 [failsafe-action none|activate-output|deactivate-output]

set iochannel <digital_channel>
 output [pulse continuous|counted <pulse_count>]
 [active-to-inactive-delay <delay>]
 [inactive-to-active-delay <delay>]
```

Options ***digital_channel***

Specify the Digital channel number, for example, d2.

type

Specify the type of digital output:

- **Sink**—Specifies that the channel will be grounded when active.
- **Source**—Specifies that the channel will provide voltage when active.
- **Sink and Source**—Specifies that channel will be grounded when it is inactive and will provide voltage when it is active.

The default is **Sink**.

active-signal-width

How long the channel will be active during the pulse mode. Valid values are 1-9999 x 100 ms. The default is 100 ms.

inactive-signal-width

How long the channel will remain inactive during pulse mode. Valid values are 1-9999 x 100 ms. The default is 100 ms.

failsafe-action

When there has been no I/O activity within the specified time (set in the Global Settings) and the **Failsafe Timer** is triggered, you can set the **Failsafe Action** to:

- **None**—The state of the Digital/Relay output remains the same, no change.
- **Activate Output**—Activates the channel.
- **Deactivate Output**—Deactivates the channel.

output

Specify how the channel output will be handled:

- **Manual**—You must manually manipulate the channel output.
- **Pulse**—Activates and deactivates the channel output activity in intervals after it is manually activated.
- **Inactive-to-Active Delay**—The channel output will remain inactive for the specified time interval after it is manually started.
- **Active-to-Inactive Delay**—The channel output will go inactive after the specified time interval after it is manually started.

The default is **Manual**.

pulse

When the **Output** is **Pulse**, you can have it pulse in a **Continuous** manner or specify a pulse **Count** (each count consists of an active/inactive sequence). The default is **Continuous**.

active-to-inactive-delay

When the I/O is commanded to an inactive state, this is the length of the delay before the command is executed. Valid values are 1-9999 x 100 ms. The default is 100 ms.

inactive-to-active-delay

When the I/O is commanded to an active state, this is the length of the delay before the command is executed. Valid values are 1-9999 x 100 ms. The default is 100 ms.

Set IOChannel Digital Output (Serial Pins)

Description Sets the Digital output for serial pins RTS and DTR. This option is only available when the **Line Service** is set to **Signal I/O**.

User Level Admin

Syntax

```
set iochannel rts|dtr [description <string>]
 [failsafe-action none|activate-outut|deactivate-output]
 [mode enabled|disabled]
```

Options

description

Provide a description of the channel, making it easier to identify. The channel description can be up to 20 characters.

failsafe-action

When there has been no I/O activity within the specified time (set in the Global Settings) and the **Failsafe Timer** is triggered, you can set the **Failsafe Action** to:

- **None**—The state of the Digital/Relay output remains the same, no change.
- **Activate Output**—Activates the channel.
- **Deactivate Output**—Deactivates the channel.

mode

Enables the channel, allowing the settings to become active.

Set IOChannel Relay

Description Sets the Relay output channel settings.

User Level Admin

Syntax

```
set iochannel <relay_number> output
 [pulse continuous|counted <pulse_count>]
 [active-to-inactive-delay <delay>]
 [inactive-to-active-delay <delay>]

set iochannel <relay_number>
 [active-signal-width <width>] [inactive-signal-width <width>]
 [failsafe-action none|activate|deactivate]
```

Options ***relay_number***

Specify the Relay channel number, for example, r2.

output

Specify how the channel output will be handled:

- **Manual**—You must manually manipulate the channel output.
- **Pulse**—Activates and deactivates the channel output activity in intervals after it is manually activated.
- **Inactive-to-Active Delay**—The channel output will remain inactive for the specified time interval after it is manually started.
- **Active-to-Inactive Delay**—The channel output will go inactive after the specified time interval after it is manually started.

The default is **Manual**.

pulse

When the **Output** is **Pulse**, you can have it pulse in a **Continuous** manner or specify a pulse **Count** (each count consists of an active/inactive sequence). The default is **Continuous**.

active-to-inactive-delay

When the I/O is commanded to an inactive state, this is the length of the delay before the command is executed. Valid values are 1-9999 x 100 ms. The default is 100 ms.

inactive-to-active-delay

When the I/O is commanded to an active state, this is the length of the delay before the command is executed. Valid values are 1-9999 x 100 ms. The default is 100 ms.

active-signal-width

How long the channel will be active during the pulse mode. Valid values are 1-9999 x 100 ms. The default is 100 ms.

inactive-signal-width

How long the channel will remain inactive during pulse mode. Valid values are 1-9999 x 100 ms. The default is 100 ms.

failsafe-action

When there has been no I/O activity within the specified time (set in the Global Settings) and the **Failsafe Timer** is triggered, you can set the **Failsafe Action** to:

- **None**—The state of the Digital/Relay output remains the same, no change.
- **Activate Output**—Activates the channel.
- **Deactivate Output**—Deactivates the channel.

Set IOChannel Analog (True Analog)

Description Sets the Analog input channel settings.

User Level Admin

Syntax

```
set iochannel <analog_channel> type current|voltage
 range <range_specifier>

set iochannel <analog_channel> alarm
 [level 1|2|3|4|5 [mode on|off] [trigger-type disabled|low|high]
  [trigger-level <decimal_value>] [clear-mode auto|manual]
  [clear-level <decimal_value>] [email on|off] [snmp on|off]
  [syslog on|off]]
```

Options ***analog_channel***

Specify the Analog channel number, for example, a2 or a4 (this also applies to Temperature models).

type

Select the type of input being measured, either **Current** or **Voltage**. The default is **Current**.

range

Select the range for the measurement type. For current, the range is:

- 0-20 (0-20mA) This is the default.
- 4-20 (04-20mA)

For voltage, the range is:

- 1 (+/-1V)
- 5 (+/-5V)
- 10 (+/-10V) This is the default.
- 150 (+/-150mV)
- 500 (+/-500mV)

alarm

Configures alarm settings when the Analog input trigger is activated.

level

You can specify up to five alarm trigger/clear severity levels. If the **Trigger Type** is **Low**, an alarm is triggered when the input drops below the specified **Trigger** value; other severity level trigger values must decrease in value with each subsequent level. If the **Trigger Type** is **High**, an alarm is triggered when the input is higher than the specified **Trigger** value; other severity level trigger values must increase in value with each subsequent level. To clear an alarm, the input must drop below the specified value when **Trigger Type** is **High** or go above the specified value when **Trigger Type** is **Low**.

mode

Enables/disables an alarm level. The default is off.

trigger-type

If the **Trigger Type** is **Low**, an alarm is triggered when the input drops below the specified **Trigger** value; other severity level trigger values must decrease in value with each subsequent level. If the **Trigger Type** is **High**, an alarm is triggered when the input is higher than the specified **Trigger** value; other severity level trigger values must increase in value with each subsequent level.

trigger-level

Specify the value that will trigger an alarm, the measurement is based on the **Type** and **Range** that you specify. This value must not fall within the scope of the value used to clear an alarm.

clear-mode

Specifies whether an activated alarm must be **Manually** cleared, or can be cleared when the input drops below the specified value (when **Trigger Type** is **High**) or goes above the specified value (when **Trigger Type** is **Low**).

clear-level

Specify that value that will clear an alarm, the measurement is based on the **Type** and **Range** that you specify. This value must not fall within the scope of the value used to trigger an alarm.

email

Sends an email alert to an email account(s) set up in the Server settings (the **Line Email Alert** settings are not used with this feature) when an alarm is triggered or cleared. The email alert data includes the severity level and the value that caused the alarm to trigger or clear. The Email Alert is associated with **Level Critical**.

snmp

Sends an SNMP trap when an alarm is triggered or cleared. The trap consists of the severity level and whether the alarm was triggered or cleared.

syslog

Sends a message to syslog when an alarm is triggered or cleared. The syslog entry includes the severity level and the value that caused the alarm to trigger or clear. The syslog message is associated with **Level Critical**.

Set IOChannel Analog (Temperature)

Description Sets the Analog input channel settings for Temperature models.

User Level Admin

Syntax

```
set iochannel <analog_channel> type rtd|thermocouple
 range <range_specifier>

set iochannel <analog_channel> alarm
 [level 1|2|3|4|5 [mode on|off] [trigger-type disabled|low|high]
  [trigger-level <decimal_value>] [clear-mode auto|manual]
  [clear-level <decimal_value>] [email on|off] [snmp on|off]
  [syslog on|off]]
```

Options ***analog_channel***

Specify the Analog channel number, for example, a2 or a4 (this also applies to Temperature models).

type

Specify the type of sensor you are using to measure temperature, either RTD or thermocouple. The default is RTD.

range

Specify the temperature range that you want to measure. For RTD, the range is:

- 1 (Pt100 a=385 -50 to 150C) This is the default.
- 2 (Pt100 a=385 0 to 100C)
- 3 (Pt100 a=385 0 to 200C)
- 4 (Pt100 a=385 0 to 400C)
- 5 (Pt100 a=385 -200 to 200C)
- 6 (Pt100 a=392 -50 to 150C)
- 7 (Pt100 a=392 0 to 100C)
- 8 (Pt100 a=392 0 to 200C)
- 9 (Pt100 a=392 0 to 400C)
- 10 (Pt100 a=392 -200 to 200C)
- 11 (Pt1000 a=385 -40 to 160C)
- 12 (NiFe604 a=518 -80 to 100C)
- 13 (NiFe604 a=518 0 to 100C)

For thermocouple, the range is:

- b (B 500 to 1800C)
- e (E 0 to 1000C)
- j (J 0 to 760C) This is the default.
- k (K 0 to 1370C)
- r (R 500 to 1750C)
- s (S 500 to 1750C)
- t (T -100 to 400C).

alarm

Configures alarm settings when the Analog input trigger is activated.

level

You can specify up to five alarm trigger/clear severity levels. If the **Trigger Type** is **Low**, an alarm is triggered when the input drops below the specified **Trigger** value; other severity level trigger values must decrease in value with each subsequent level. If the **Trigger Type** is **High**, an alarm is triggered when the input is higher than the specified **Trigger** value; other severity level trigger values must increase in value with each subsequent level. To clear an alarm, the input must drop below the specified value when **Trigger Type** is **High** or go above the specified value when **Trigger Type** is **Low**.

mode

Enables/disables an alarm level. The default is off.

trigger-type

If the **Trigger Type** is **Low**, an alarm is triggered when the input drops below the specified **Trigger** value; other severity level trigger values must decrease in value with each subsequent level. If the **Trigger Type** is **High**, an alarm is triggered when the input is higher than the specified **Trigger** value; other severity level trigger values must increase in value with each subsequent level.

trigger-level

Specify the value that will trigger an alarm, the measurement is based on the **Type** and **Range** that you specify. This value must not fall within the scope of the value used to clear an alarm.

clear-mode

Specifies whether an activated alarm must be **Manually** cleared, or can be cleared when the input drops below the specified value (when **Trigger Type** is **High**) or goes above the specified value (when **Trigger Type** is **Low**).

clear-level

Specify that value that will clear an alarm, the measurement is based on the **Type** and **Range** that you specify. This value must not fall within the scope of the value used to trigger an alarm.

email

Sends an email alert to an email account(s) set up in the Server settings (the **Line Email Alert** settings are not used with this feature) when an alarm is triggered or cleared. The email alert data includes the severity level and the value that caused the alarm to trigger or clear. The Email Alert is associated with **Level Critical**.

snmp

Sends an SNMP trap when an alarm is triggered or cleared. The trap consists of the severity level and whether the alarm was triggered or cleared.

syslog

Sends a message to syslog when an alarm is triggered or cleared. The syslog entry includes the severity level and the value that caused the alarm to trigger or clear. The syslog message is associated with **Level Critical**.

Set IOChannel IOExtension

Description Configures the I/O extension options that allow you to connect the Digital Input channel or input serial signal pin (when the line is configured for signal-io) to Digital Output/Relay channels or output serial signal pins (when the line is configured for signal-io) on the same IOLAN, remote IOLAN(s), and/or TCP/IP applications running on local hosts.

User Level Admin

Syntax

```
set iochannel <channel> ioextension enabled on|off
 [keepalive on|off]

set iochannel <channel> ioextension connection-method
 client-initiated [tcp-port <tcp_port>] [multihost on|off]

set iochannel <channel> ioextension connection-method
 server-initiated <host_name> <tunnel_name> [tcp-port <tcp_port>]
 [multihost all|backup <config_backup_host> tunnel_name>
 <host_port>|none]

set iochannel <channel> ioextension connection-method
 local-connection [<input_channel>]
```

Options ***<channel>***

Specify the Digital/Relay channel or serial signal pin that you are configuring the I/O extension for. The channel can be d1, d2, d3, d4, r1, r2, depending on the model. The serial signal pins are dsr, dcd, or cts for input and dtr or rts for output.

enabled

When enabled, the digital input channel or DSR/DCD/CTS input serial signal pins can be connected to:

- A Digital output or relay (if the I/O model supports relay) channel on the same IOLAN
- Output Serial Signal Pins (DTR/RTS)
- A Digital output channel on another IOLAN(s) or output serial signal pins (DTR/RTS) on another IOLAN(s)
- A TCP/IP application(s) running on a host on the network

When enabled, the digital output/relay channel or DTR/RTS output serial signal pins can be associated with a digital input channel or input serial signal pins.

Default: Disabled

keepalive

Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.

This parameter needs to be used in conjunction with server parameter, monitor-connection-every. The interval determines how long the IOLAN will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.

connection-method

The connection-method is one of the following:

- **Client-Initiated**—When specified, the channel/serial signal pin will wait for connections to be initiated by another I/O channel or a TCP/IP application.
- **Server-Initiated**—When specified, the channel/serial signal pin initiates communication to another I/O channel or a TCP/IP application.
- **Local-Connection**—When specified, the input or output, depending on how the channel or serial signal pin is configured, will be associated with another local IOLAN I/O channel or serial signal pin.

  When the channel is configured as digital input or when configuring an input serial signal pin, the **Output Channels** parameter displays all the local digital output signals or relays that it is associated with.

  When the channel is configured as digital output, you must select a local digital input channel or input serial signal pin on the IOLAN.

  Note that the **Failsafe Action** is not compatible with the local-connection option.

Default: Client-Initiated

client-initiated tcp-port

The TCP port that the channel/serial signal pin will use to listen for incoming connections.

Default: 2000 for channel 1, then increments by one for each channel

client-initiated multihost

When this option is enabled, multiple I/O channels and/or TCP/IP applications can connect to this channel/serial signal pin. The default is off.

server-initiated tcp-port

The TCP Port that the channel/serial signal pin will use to communicate to another IOLAN or a TCP/IP application.

Default: 2000 for channel 1, then increments by one for each channel

server-initiated multihost all|backup <*config_backup_host*> <*tcp_port*>|none

Used for connections going from the Digital input channel or input serial signal pins, allows the input channel/serial signal pin to communicate to either all the hosts in the multihost list or a primary/backup host schema (see *Configuring Multiple Hosts* in the *IOLAN User's Guide* for a more detailed explanation).

local-connection <*input_channel*>

Specify the Digital input channel or input serial signal pin that will control the Digital/Relay output channel or output serial signal pin.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer IOLAN DS.

Set IOChannel Multihost

Description Configures up to 49 hosts/IOLANs that the Digital input channel or input serial signal pins (DSR, DCD, or CTS-when the line is configured for signal-io) will connect to. To see a list of configured hosts/IOLANs, enter the **`show iochannel <`***`channel`***`>`** command.

User Level Admin

Syntax

`set iochannel <`*`channel`***`> multihost entry <`***`number`***`> delete`**

`set iochannel <`*`channel`***`> multihost entry <`***`number`***`> host <`***`host_name`***`> <`***`tcp_port`***`>`**

Options **<*channel*>**

Specify the Digital input channel or input serial signal pin that will be connecting to all the hosts/IOLANs in the multihost list.

entry

Specify the multihost table entry number. Valid values are 1-100.

delete

Deletes the entry number in the multihost table.

host

Specify the preconfigured host that will be in the multihost list.

Default: None

<tcp_port>

Specify the TCP port that the I/O channel or serial signal pin will use to communicate to the **Host**.

Default: 0

Set IOChannel IOExtension SSL

Not all SSL/TLS encryption options are available on all firmware versions.

Description Configures the secure SSL/TLS connection between the Digital/Relay I/O channel or serial signal pin and the host/IOLAN. For an explanation of the parameters, see ***Set SSL Line*** .

User Level Admin

Syntax

```
set iochannel <channel> ioextension ssl [enabled on|off]
 [use-server on|off] [version any|tslv1|sslv3]
 [type client|server] [verify-peer on|off]
 [validation-criteria country <code>|state-province <text>|
    locality <text>|organisation <text>|organisation-unit <text>|
    common-name <text>|email <email_addr>]

set iochannel <channel> ioextension ssl cipher-suite
 option1|option2|option3|option4|option5
 encryption any|aes|3des|des|arcfour|arctwo|none
 min-key-size 40|56|64|128|168|256
 max-key-size 40|56|64|128|168|256
 key-exchange any|rsa|edh-rsa|edh-dss|adh
 hmac any|sha1|md5
```

Show IOChannel Status

Description Shows the I/O channel status for all channels and the serial signal pins (when the line is configured for signal-io).

User Level Admin

Syntax

```
show iochannel status
```

Kill IOChannel

Description Kills the I/O channel.

User Level Admin

Syntax

```
kill iochannel <i/o_channel>

kill iochannel line <number> rts|cts|dtr|dsr|dcd
```

Options

i/o_channel

Specify the channel number, for example, d2 or a4. Temperature models use Analog input, so the channel numbers are a1-a4.

rts|cts|dtr|dsr|dcd

Specify the Digital output pins (RTS or DTR) or Digital input pins (CTS, DSR, or DCD).

Show IO

Description Shows global I/O information (for example, UDP, TruePort, Modbus). Temperature I/O is Analog.

User Level Admin

Syntax **show iochannel <*i/o_channel*>**

show iochannel rts|cts|dtr|dsr|dcd

Options ***i/o_channel***

Specify the channel number, for example, d2 or a4. Temperature models use Analog input, so the channel numbers are a1-a4.

rts|cts|dtr|dsr|dcd

Specify the Digital output pins (RTS or DTR) or Digital input pins (CTS, DSR, or DCD).

Show IOChannel

Description Shows I/O channel information. Temperature I/O is Analog.

User Level Admin

Syntax **show iochannel <*i/o_channel*>**

show iochannel line <*number*> rts|cts|dtr|dsr|dcd

Options ***i/o_channel***

Specify the channel number, for example, d2 or a4. Temperature models use Analog input, so the channel numbers are a1-a4.

rts|cts|dtr|dsr|dcd

Specify the Digital output pins (RTS or DTR) or Digital input pins (CTS, DSR, or DCD).

I/O Channel Control Commands

The I/O commands in this section are used to manually manage the I/O channels.

Digital Output

Description Manages the Digital output channel status. Not all models have four Digital channels, most have just two.

User Level Admin

Syntax **iochannel d1|d2|d3|d4|cts|dsr|dcd clear alarm|input-latch**

Options **alarm**

Clears the alarm. Note that if the condition that tripped the alarm still exists, the alarm will not look like it's cleared, but will reflect the appropriate alarm level severity. Alarm Level 0 means that the alarm has not been triggered.

latch-input

Clears the latch value.

Digital Input

Description Manages the Digital input channel status.
User Level Admin
Syntax `iochannel d1|d2|d3|d4|rts|dtr output activate|deactivate`
Option **output**

Manually deactivates the I/O channel.

Relay

Description Manages the Relay output channel status.
User Level Admin
Syntax `iochannel r1|r2 output activate|deactivate`
Option **output**

Manually deactivates the I/O channel.

Analog Input

Description Manages the Analog input channel status.
User Level Admin
Syntax `iochannel a1|a2|a3|a4 clear alarm|min|max`
Options **alarm**

Clears the alarm. Note that if the condition that tripped the alarm still exists, the alarm will not look like it's cleared, but will reflect the appropriate alarm level severity. Alarm Level 0 means that the alarm has not been triggered.

min

Clears the minimum value.

max

Clears the maximum value.

Calibrating Analog Input (Analog/Temperature)

Calibrate Analog

Description Calibrates the Analog input channel. When this command is issued, a script will automatically start, requesting that the minimum and maximum calibration values be applied to the requested Analog/Temperature channel. See ***Calibrating Analog Input*** in the *IOLAN User's Guide* for more information.
User Level Admin
Syntax `iochannel a1|a2|a3|a4 calibrate`

Reset Calibration

Description Resets the calibration to factory defaults.
User Level Admin
Syntax `reset io calibration`

Power Commands

This chapter defines all the CLI commands associated with configuring the IOLAN's power parameters.

Power Commands

Description Actively controls the RPS plug power.

User Level Admin, Normal

Syntax

```
power cycle line <number> [plug <number|range|*>]

power on line <number> [plug <number|range|*>]

power off line <number> [plug <number|range|*>]

power reset line <number>

power status line <number>
```

Options

cycle

Turns the specified plug(s) off and then on.

on

Turns the specified plug(s) on.

off

Turns the specified plug(s) off.

reset

Resets all the RPS plugs to the default state as defined in the Power Management line settings.

status

Displays the status (on/off) of the plug(s).

Glossary

This chapter provides definitions for IOLAN terms.

BOOTP (BOOTstrap Protocol)	An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.
Callback	A security feature where the IOLAN calls back the User at a predetermined number defined in the Users account.
CHAP (Challenge Handshake Authentication Protocol)	Standard authentication protocol for PPP connections. It provides a higher level of security than PAP and should be used whenever possible. *see PAP*
Community (SNMP)	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that provides static and dynamic address allocation and management.
Direct Connection	Connections that bypass the IOLAN enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the IOLAN is not required.
Ethernet	A high-speed (10Mbps,100Mbps) cable technology that connects devices to a LAN, using one or more sets of communication protocols.
Fixed Callback	A method where there is a specific number defined to callback a user.
Local Authentication	Uses the user ID and password stored within the IOLAN User database.
LPD	Line Printer Daemon. A printer protocol that uses TCP/IP to establish connections between printers and workstations on a network. The technology was developed originally for BSD UNIX and has since become the de facto cross-platform printing protocol.
Modem Initialization String	A series of commands sent to the modem by a communications program at start up. These commands tell a modem how to set itself up in order to communicate easily with another modem.
MOTD	Message of the day. This is defined by a file whose contents display when users log into the IOLAN.
Multicast	The broadcasting of messages to a specified group of workstations on a LAN, WAN, or internet.
NAK (Negative Acknowledgment)	A communication control character sent by the receiving destination indicating that the last message was not received correctly.

PAP (Password Authentication Protocol)	Standard authentication protocol for PPP connections. *see CHAP*
RADIUS (Remote Authentication Dial In Users Services)	An open standard network security server that communicates with the PAP protocol.
Reverse Connection	Connections that originate from a host that go directly to a serial device through the IOLAN.
RIP (Routing Information Protocol)	A protocol that allows gateways and hosts to exchange information about various routes to different networks.
Roaming Callback	A method where the client supplies the number for callback when they dial in.
RPC	Remote Procedure Call. A type of protocol that allows a program on one computer to execute a program on a server computer.
Silent Connection	Silent connections are the same as direct connections except that they are permanently established. The host login prompt is displayed on the screen. Logging out redisplays this prompt. Silent connections, unlike direct connections, however, make permanent use of pseudo tty resources and therefore consume host resources even when not in use.
SNMP (Simple Network Management Protocol)	A protocol for managing network devices.
Subnet/Prefix Bits	Identifies the devices IP address, which portion constitutes the network address and which portion constitutes the host address.