



December 2016

Secure Device Servers - LES5011 to 5164
Secure Terminal Servers - LES6044 to 7244
Secure Console Servers - LES8084 to 8324

Secure Terminal Server Secure Console Server Secure Device Server Command Line Interface Reference Guide

Version 4.8

5500209-48

CUSTOMER Order **toll-free** in the U.S 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
SUPPORT FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
INFORMATION Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** * E-mail **info@blackbox.com**

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - a. El cable de poder o el contacto ha sido dañado; u
 - b. Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - c. El aparato ha sido expuesto a la lluvia; o
 - d. El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - e. El aparato ha sido tirado o su cubierta ha sido dañada.

FCC Requirements for Telephone-Line Equipment

1. The Federal Communications Commission (FCC) has established rules which permit this device to be directly connected to the telephone network with standardized jacks. This equipment should not be used on party lines or coin lines.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until the repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. If you have problems with your telephone equipment after installing this device, disconnect this device from the line to see if it is causing the problem. If it is, contact your supplier or an authorized agent.
4. The telephone company may make changes in its technical operations and procedures. If any such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes.
5. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number that this unit is connected to.
 - b. The ringer equivalence number.
 - c. The USOC jack required: RJ-11C.
 - d. The FCC registration number.

Items (B) and (D) can be found on the unit's FCC label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five. If too many devices are attached, they may not ring properly.

6. In the event of an equipment malfunction, all repairs should be performed by your supplier or an authorized agent. It is the responsibility of users requiring service to report the need for service to the supplier or to an authorized agent.

Certification Notice for Equipment Used in Canada

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications-network protective, operation, and safety requirements. Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility—in this case, Black Box. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The LOAD NUMBER (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading.

The termination on a loop may consist of any combination of devices, subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

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

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le Industrie Canada.

Table of Contents

Preface	15
About This Book	15
Intended Audience	15
Typeface Conventions	15
Chapter 1 Introduction	16
CLI Conventions	16
Command Syntax	16
Command Shortcuts	17
Command Options	17
Chapter 2 Server Commands	18
Server Commands	18
Set Console	18
Set Port-Buffering	18
Set Server	20
Set SSL Server	25
Set Service	26
Show Console	27
Show Server	27
Show Port-Buffering	27
Show Modbus	27
Hardware Commands	27
Set Ethernet	27
Show Hardware	27

SSH Server Commands	28
Set SSH-Server	28
Show SSH-Server	29
SSL/TLS Commands	29
Set SSL Server	29
Set SSL Server Cipher-suite	30
Show SSL	31
Modbus Commands	32
Set Modbus Gateway	32
Show Modbus	33
Authentication Commands	33
Set Authentication	33
Set Authentication Local	34
Set Authentication Kerberos	34
Set Authentication LDAP/Active Directory	35
Set Authentication NIS	36
Add RADIUS	36
Delete RADIUS	37
Set Authentication RADIUS	37
Set Authentication TACACS+	38
Set Authentication SecurID	39
Show Authentication	40
COMredirect Baud Commands	40
Set COMredirect Remap-Baud	40
Show COMredirect	41
Email Commands	41
Set Email-Alert Server	41
Show Email-Alert Server	42
Clustering Commands	42
Add Clustering Slave-IP	42
Delete Clustering Slave-IP	43
Set Clustering Slave-IP	43

Show Clustering Slave-IP	44
Dynamic DNS Commands	44
Set Dynamic-DNS	44
Set Dynamic-DNS SSL	45
Set Dynamic-DNS SSL Cipher-Suite	46
Show Dynamic-DNS	47
PCI Commands	47
Set PCI Card	47
Show PCI	47
IPv6 Commands	47
Set IPv6	47
Show IPv6	48
Add Custom-IPv6	48
Set Custom-IPv6	49
Delete Custom-IPv6	50
IPv6 Router Advertisements	50
Set IPv6-Router-Advertisement	50
Show IPv6-Router-Advertisement	51
Chapter 3 User Commands	52
Admin	52
Help	52
Line	52
Kill Line	52
Kill Session	52
Logout	53
Menu	53
Ping	53
Resume	53
Rlogin	53
Screen	54
Set Termttype	54
Set User	54

Set User Session	55
Show Line Users.....	56
SSH	56
Syslog Console.....	57
Show Sessions	57
Show Termtype.....	58
Start	58
Telnet.....	58
Version	59
Configuring Users.....	59
Add User.....	59
Delete User.....	59
Set Default User.....	60
Set User	63
Set User Session	67
Show Default User.....	67
Show User	68
Chapter 4 Line Commands.....	69
1-Port vs. 2-Port+ Line Commands	69
Line Commands	69
Set Line.....	69
Set Line Interface.....	75
Set Line Service.....	78
Set Modem	80
Set Termtype.....	81
Show Line.....	81
Line Service Commands	81
Set Rlogin-Client.....	81
Set Telnet-Client	82
Set SSH-Client	83
Set PPP.....	84
Set PPP Dynamic-DNS	89

Set SLIP	89
Set UDP	91
Set Vmodem.....	92
Set Vmodem-Phone.....	94
Set SSL Line.....	94
Set SSL Line Cipher-suite.....	96
Set Modbus-Slave Line	97
Set Modbus-Master Line	97
Set Multihost	98
Set Line Initiate-Connection	98
Show Interface	99
Show PPP	99
Show Rlogin-Client.....	99
Show SLIP	99
Show SSH-Client	99
Show Telnet-Client	99
Show Modbus	99
Show UDP	99
Show Vmodem.....	100
Show Vmodem-Phone.....	100
Modem Commands	100
Add Modem	100
Delete Modem	100
Set Modem	100
Show Modems	100
Email Commands	101
Set Email-Alert Line.....	101
Show Email-Alert Line.....	102
Packet Forwarding Commands	102
Set Packet-Forwarding Line	102
Show Packet-Forwarding Line	105
Chapter 5 Network Commands	106

SNMP Commands	106
Add Community.....	106
Add Trap.....	107
Delete Community	107
Delete Trap	107
Set SNMP.....	107
Set SNMP V3-Security.....	108
Set SNMP engine-id-string	109
Set SNMP inform-timeout	109
Set SNMP inform-retries	109
Show SNMP.....	109
TFTP Commands	109
Set Server TFTP	109
SFTP Commands	110
Set Server SFTP.....	110
Show SFTP	111
Hosts Commands	111
Add Host.....	111
Delete Host.....	111
Set Host.....	112
Show Hosts	112
DNS/WINS Commands	112
Add DNS.....	112
Add WINS	112
Delete DNS	113
Delete WINS	113
Show DNS	113
Show Server.....	113
Show WINS.....	113
Gateway Commands.....	114
Add Gateway.....	114
Delete Gateway	115

Set Gateway	115
Show Gateways	115
Logging Commands	116
Set Syslog	116
Show Syslog	116
RIP Commands	117
Add RIP.....	117
Delete RIP	117
Set RIP	118
Show RIP	118
Show RIP Peers	119
IPsec Commands	119
Add IPsec	119
Set IPsec.....	119
Show IPsec.....	122
IPsec	122
IPv6 Tunnels.....	122
Add IPv6tunnel	122
Set IPv6tunnel.....	123
Show IPv6tunnel.....	123
Delete IPv6tunnel.....	123
L2TP/IPsec.....	124
Set L2TP	124
Show LT2P	126
VPN Exceptions	126
Add VPN Exception	126
Set VPN Exception	126
Delete VPN Exception	127
Show VPN Exception	127
HTTP Tunnel Commands	127
Add http-tunnel.....	127
Set http_tunnel	128

Delete HTTP Tunnel.....	129
Show HTTP Tunnel.....	129
Chapter 6 Time Commands	130
Server Commands	130
Set Time.....	130
Set Timezone	130
Show Time.....	130
Show Timezone	130
SNTP Commands	131
Add SNTP	131
Delete SNTP	131
Set SNTP	131
Show SNTP	132
Show SNTP-Info.....	132
Time/Date Setting Commands	132
Set Date	132
Set Summertime	132
Set Summertime Fixed.....	133
Set Summertime Recurring	133
Show Date	134
Show Summertime	134
Chapter 7 Administration Commands	135
Bootup Commands	135
Reboot	135
Reset.....	135
Reset Serial Port Statistics.....	135
Reset Factory.....	135
Save	135
Set Bootup	136
Show ARP	136
Set cli.....	136
Show Bootup	136

TFTP File Transfer Commands	137
Netload	137
Netsave	138
SFTP File Transfer Commands	138
Snetload	138
Snetsave	139
Custom Factory Default	140
Netload	140
Snetload	141
Set	141
Keys and Certificates Commands	142
Netload	142
Netsave	143
Snetload	144
Snetsave	145
MOTD Commands	145
Set MOTD	145
Show MOTD	146
Delete Files	146
ipsec_key	146
ntp_key	146
ssh_host	146
ssh_user	147
ssl_ca	147
ssl_certificate	147
ssl_key	147
Chapter 8 Statistics Commands	148
Configuration Statistics	148
Show Netstat	148
Show Netstat Statistics	148
Show Modbus Statistics	149

Show Routes.....	149
Run-Time Statistics	149
Delete Arp.....	149
Show Arp.....	149
Show Serial	149
Uptime	149

Preface

About This Book

This guide provides the information you need to configure the Secure Terminal Server using the Command Line Interface.

Intended Audience

This guide is for administrators who will be configuring the Secure Terminal Server.

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 protocol the Secure Terminal Server 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: <code>add host</code>	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.
<code>subscribe <i>project</i> <i>subject</i></code> <code>run yourcode.exec</code>	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 <i>project</i> , you enter your own value, such as <code>stock_trader</code> , and for yourcode , enter the name of your program.
<i>BLACK BOX® User Guide</i>	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.

1 Introduction

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

CLI Conventions

This section explains how to interpret the CLI syntax.

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 Secure Terminal Server), 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$
```

2 Server Commands

This chapter defines all the CLI commands associated with configuring server parameters for the Secure Terminal Server.

Server Commands

Set Console

- Description** Sets the flow control and baud rate on Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server models that have a dedicated console port, specifies the baud rate of the line connected to the console port.

Set Port-Buffering

- Description** Configures port buffering.
- User Level** Admin
- Syntax** `set port-buffering [duplicate-nfs-to-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 Secure Terminal Server'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 Secure Terminal Servers using the same NFS host, it is recommended that each Secure Terminal Server 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.

nfs-host

The NFS host that the Secure Terminal Server will use for its **Remote Port Buffering** feature. The Secure Terminal Server 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 tunnel name on the tunnel peer Terminal Server

time-stamp

Enable/disable time stamping of the port buffer data.

view-port-buffer-string

The string (up to 8 characters) used by 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 <1-6> <IPv4_address>]
set server [ip-filter-range on|off]
set server [ip-filter-start-address <1-6> <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 1 port models)
set server [disable-ip-forwarding <on|off>]
```

Options **auto-obtain-dns**

When DHCP/BOOTP is enabled, you can enable this option to have the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server 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 Secure Terminal Server's unique IPv4 network IP address. If you are using the Secure Terminal Server in an IPv6 network, use the **set ipv6** command.

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 Terminal Server has more than one interface, each of the interfaces can be set separately, however only one MTU size can be set for both IPV4 and IPV6 frames.

Valid options: 68-1500 bytes

Default mtu size: 1500 bytes

name

You must supply a name for the Secure Terminal Server.

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 Terminal Server will send a TCP keepalive. This only applies to line service types that support the keepalive feature.

Default: 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 Secure Terminal Server 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 Secure Terminal Server will only accept data from hosts configured in the Secure Terminal Server's **Host Table** with an IP address (hosts configured with a Fully Qualified Domain Name, FQDN, will not be able to access the Secure Terminal Server when this option is enabled).

The default value is **Off**.

ip-filter-end-address

Set the end IPv4 address of this filter.

ip-filter-range

A security feature that when enabled, the Terminal Server will only accept data from or send data to hosts configured within this IPv4 address range. You can define 6 IPv4 traffic ranges.

The default value is **Off**.

ip-filter-start-address

Set the start IPv4 address of this 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server will wait to make the secondary interface (Ethernet 2) active after it has been detected as up.

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 and TS1 models, all other models the maximum size is 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.

Data Logging is only valid for COMredirect and TCP sockets profiles.

Values: 1-2000 KB (DS1/TS1)

Values: 1-4000 KB (all other models)

Default: 4 KB (DS1/TS1)

Default: 256 KB (all other models)

pre-4.3g-data-logging

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

Default: Disabled.

udp-always-arp

This controls whether the Secure Terminal Server 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 Secure Terminal Server. 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** (<026>s in decimal).

retry

The number of times the Secure Terminal Server will retry to transmit a TFTP 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 Secure Terminal Server will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the Secure Terminal Server 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 unencrypted 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 Secure Terminal Server, they need to be generated using the same SSL passphrase for both to work.

disable-ip-forwarding

(SCS 8, 16, 32 models with Ethernet Interfaces)

When enabled, no IP traffic will be forwarded between Ethernet interfaces.

Default: Disabled.

Set SSL Server

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

User Level Admin

Syntax `set ssl server [version any|tlsv1|sslv3|tlsv1.1|tlsv1.2] [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 Terminal Server will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try all other connection methods.
- **TLSv1**—The connection will use only TLSv1
- **SSLv3**—The connection will use only SSLv3
- **TLSv1.1**—The connection will use only TLSv1.1
- **TLSv1.2**—The connection will use only TLSv1.2

The default is **Any**.

type

Specify whether the Secure Terminal Server 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 Secure Terminal Server.

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	<pre>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]</pre>
Options	<p>routed</p> <p>Route daemon process in the Secure Terminal Server on port 520/521.</p> <p>telnetd</p> <p>Telnet daemon process in the Secure Terminal Server on port 23.</p> <p>sshd</p> <p>SSH daemon process in the Secure Terminal Server on port 22.</p> <p>httpd</p> <p>HTTP daemon process in the Secure Terminal Server on port 80.</p> <p>snmpd</p> <p>SNMP daemon process in the Secure Terminal Server on port 161.</p> <p>spcd</p> <p>SPC (TruePort) daemon process in the Secure Terminal Server that supports TruePort Full Mode on UDP port 668. You can still communicate with the Secure Terminal Server in Lite Mode when this service is disabled.</p> <p>sntp</p> <p>Simple Network Time Protocol client process in the Secure Terminal Server.</p> <p>httpsd</p> <p>Secure HTTP daemon process in the Secure Terminal Server on port 443.</p> <p>syslog</p> <p>Syslog client process in the Secure Terminal Server.</p> <p>dmgrd</p> <p>DeviceManager daemon process in the Secure Terminal Server. If you disable this service, you will not be able to connect to the Secure Terminal Server with the DeviceManager application. DeviceManager listens on port 33812 and sends on port 33813.</p> <p>modbusd</p> <p>Modbus daemon process in the Secure Terminal Server on port 502.</p>

ipsec

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

Show Console

Description For Secure Terminal Server models that have a dedicated console port, this command displays the configured parameters of the console port.

User Level Admin

Syntax `show console`

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`

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 *Users Guide* for information about the keys and certificates that need to be uploaded or downloaded with the Secure Terminal Servers SSH server.

Description Configures the Secure Terminal Servers 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-cbc on|off] [arcfour on|off] [aes-ctr on|off]
aes-gcm on|off] [chacha20-poly1305 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 Terminal Server'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|tls1|ssl3|tls1.1|tls1.2] [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 Terminal Server will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try all other connection methods.
- **TLSv1**—The connection will use only TLSv1
- **SSLv3**—The connection will use only SSLv3
- **TLSv1.1**—The connection will use only TLSv1.1
- **TLSv1.2**—The connection will use only TLSv1.2

The default is **Any**.

type

Specify whether the Secure Terminal Server 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 Secure Terminal Server.

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

Description	Sets the default SSL/TLS cipher suite parameters.
User Level	Admin
Syntax	<pre>set ssl server cipher-suite option1 option2 option3 option4 option5 encryption any aes 3des des arcfour arc2wo aes-gcm 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 ecdh-ecdsa hmac any sha1 md5 sha256 sha384</pre>
Options	<pre>option1 option2 option3 option4 option5</pre> <p>Sets the priority of the cipher suite, with option1 being highest priority and option5 lowest priority.</p>

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
- AES-GCM
- 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.
- **ECDH-ECDSA**—This is an ECDH key exchange using an ECDSA key and certificate.

The default is **Any**.

hmac

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

- Any
- MD5
- SHA1
- SHA256
- SHA384

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 Secure Terminal Server when it is operating as a Modbus Gateway.
User Level	Admin
Syntax	<pre> set modbus gateway [addr-mode embedded re-mapped] set modbus gateway [broadcast on off] set modbus gateway [char-timeout <number>] set modbus gateway [next-req-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 on off] </pre>
Options	<p>addr-mode</p> <p>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.</p> <p>broadcast</p> <p>When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. The default is Off.</p> <p>char-timeout</p> <p>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.</p> <p>next-req-delay</p> <p>A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. The default is 50 ms.</p> <p>exceptions</p> <p>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.</p> <p>idle-timer</p> <p>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.</p> <p>mess-timeout</p> <p>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.</p> <p>port</p> <p>The network port number that the Slave Gateway will listen on for both TCP and UDP messages. The default is 502.</p>

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>| statistics [master-tcp |
master-udp | slave-udp | slave-tcp]
```

Authentication Commands

Set Authentication

Description Sets the authentication method for the Secure Terminal Server.

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 Secure Terminal Server attempts.

secondary

If the **Primary Authentication Method** fails, the next authentication method that the Secure Terminal Server 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 Secure Terminal Server (**Local**) others in **RADIUS**.

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

Specify the authentication method that the Secure Terminal Server 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 Secure Terminal Server cannot communicate with the Primary Authentication server.

auth-admin-user-local

When enabled, the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server.

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 Secure Terminal Server'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 tunnel name on the tunnel peer Terminal Server

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 Terminal Server will authenticate itself to the LDAP Server. The name to be used by the Terminal Server 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 host. If you use a host name, that host must either have been defined in the Secure Terminal Server'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 host listens to for authentication requests. The default port is 389.

tunnel_name

Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Terminal Server

encrypt-password

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

tls

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

tls-port

Specify the port number that LDAP 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 Terminal Server will use the Microsoft Active Directory attribute sAMAccountName for the user name.
- **uid** - When enabled, the Terminal Server 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 tunnel name on the tunnel peer Terminal Server

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 Secure Terminal Server 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 tunnel name on the tunnel peer Terminal Server

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 Secure Terminal Server 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 Secure Terminal Server will send the Secure Terminal Server's Ethernet 1 IPv4 address to the RADIUS server. This is the default.

nas-ip-address specify <ipv4_address>

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

nas-ipv6-address auto

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

nas-ipv6-address specify <ipv6_address>

When specified, the Secure Terminal Server will send the specified IPv6 address to the RADIUS server.

retry

The number of times the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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>] [authorisation <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.

Default: None

secondary

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

Default: None

tunnel_name

Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Terminal Server

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 “admincli” and the service name for Web Manager or Device Manager to be “adminweb”.

authorisation

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

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.

acct-secondary

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

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	<pre>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</pre>
Options	<p>primary host</p> <p>The first SecurID server that is tried for user authentication.</p>

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 tunnel name on the tunnel peer Terminal Server

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 Secure Terminal Server.

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.

COMredirect Baud Commands

Set COMredirect 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 Secure Terminal Server.
User Level	Admin
Syntax	set comredirect 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 Secure Terminal Server and the connected serial device. You can also specify a custom baud rate; valid values are 50 - 1843200.

Show COMredirect

Description Shows the Secure Terminal Server COMredirect remapping table.
User Level Normal, Admin
Syntax `show comredirect`

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 Secure Terminal Server.

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 Secure Terminal Server 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 your 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 validation 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 Secure Terminal Server 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 Secure Terminal Server 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 slave Secure Terminal Server.

Delete Clustering Slave-IP

Description	Deletes a Slave Secure Terminal Server from the clustering group. Type <code>delete clustering slave-ip ?</code> to get a list of Slave Secure Terminal Server IP addresses.
User Level	Admin
Syntax	<code>delete clustering slave-ip <IPv4_address></code>
Option	<code><IPv4_address></code> 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	<code>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>]</code>
Options	<code><IPv4_address></code> 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 slave Secure Terminal Server.

Show Clustering Slave-IP

Description	Show a Slave Secure Terminal Servers clustering group settings. Type <code>show clustering slave-ip ?</code> to get a list of Slave Secure Terminal Server IP addresses.
User Level	Admin
Syntax	<code>show clustering slave-ip <IPv4_address> [get-port-names] [get-port-names-and-save]</code>
Options	<p><code><IPv4_address></code></p> <p>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.</p> <p>get-port-names</p> <p>Retrieves the port/line names from the specified Slave Secure Terminal Server.</p> <p>get-port-names-and-save</p> <p>Retrieves the port/line names from the specified Slave Secure Terminal Server and saves them in the Slave Secure Terminal Server clustering configuration.</p>

Dynamic DNS Commands

Set Dynamic-DNS

Description	Configures the dynamic DNS parameters.
User Level	Admin
Syntax	<code>set dynamic-dns [on off]</code> <code>[connection-method http http-port-8245 https]</code> <code>[hostname <hostname>] [username <username>]</code> <code>[password <password>] [system-type dynamic static custom]</code> <code>[wildcard enable disable nochange]</code>
Options	<p>connection-method</p> <p>Specify how the Secure Terminal Server is going to connect to the DynDNS.org server, via HTTP, HTTP through Port 8245, or HTTPS.</p> <p>hostname</p> <p>Specify the registered hostname with DynDNS.org that will be updated with the Secure Terminal Server's IP address should it change. Put in the full name; for example, <code>mydeviceserver.dyndns.org</code>.</p> <p>username</p> <p>Specify the user name used to access the DynDNS.org server.</p> <p>password</p> <p>Specify the password used to access the DynDNS.org server.</p> <p>system-type</p> <p>Specify how your account was set up with DynDNS.org, using a Dynamic, Static, or Custom IP address schema.</p>

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 Secure Terminal Server 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 Secure Terminal Server.

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

Description Sets the SSL/TLS cipher suite parameters for the connection between the Secure Terminal Server 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|aes-gcm|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|ecdh-ecdsa
hmac any|sha1|md5|SHA256|SHA384`

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**
- **AES-GCM**
- **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.
- **ECDH-ECDSA**—This is an ECDH key exchange using an ECDSA key and certificate.

The default is **Any**.

hmac

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

- Any
- MD5
- SHA1
- SHA256
- SHA384

The default is **Any**.

Show Dynamic-DNS

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

PCI Commands

Set PCI Card

Description Sets the type of card in the PCI slot.
User Level Admin
Syntax `set pci card none|modem`
Option `card`
 Choose default modem card or leave select NONE if no card is inserted in the PCI slot.

Show PCI

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

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 Secure Terminal Server will accept from the DHCPv6 server, IPv6 address(es) and/or network prefix(es).
ipv6-address
 When enabled, the Secure Terminal Server will accept IPv6 address(es) from the DHCPv6 server. This is `off` by default.

network-prefix

When enabled, the Secure Terminal Server will accept the network prefix from the DHCPv6 server. This is **off** by default.

eth1|eth2

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

enable-ipv6-addressing

When enabled, you can configure the Secure Terminal Server 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 Secure Terminal Server will send out a Router Solicitation message. If a Router Advertisement message is received, the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

method auto

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

network-prefix

Specify the IPv6 network prefix. The Secure Terminal Server will derive the complete IPv6 address from the entered network prefix and the Secure Terminal Server'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 Secure Terminal Server's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

method auto

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

network-prefix

Specify the IPv6 network prefix. The Secure Terminal Server will derive the complete IPv6 address from the entered network prefix and the Secure Terminal Server'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 Secure Terminal Server 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: <ul style="list-style-type: none"> • 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 Secure Terminal Server'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 Secure Terminal Server's Ethernet interface 1 or Ethernet interface 2 (SCS models only) interface.

3 User Commands

This chapter defines all the CLI commands available to users who are logged into the Secure Terminal Server.

Commands for Users Logged Into the Secure Terminal Server

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 Secure Terminal Servers 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 Secure Terminal Server. The internal modem is addressed as last serial port +1. On single port models, use the command `kill line`.

User Level Normal, 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 Secure Terminal Server.
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 settings for the current user.
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 Secure Terminal Server 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 Secure Terminal Server. 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, CLI, or WebManager. The Secure Terminal Server supports one custom language that must be downloaded to the Secure Terminal Server; 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 Secure Terminal Server.
- **Send**—RIP packets can only be sent by the Secure Terminal Server.
- **Listen**—RIP packets can only be received by the Secure Terminal Server.
- **Send and Listen**—RIP packets are sent and received by the Secure Terminal Server.

password

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

Set User Session

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

Description Sets the session settings for the current user.

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 Secure Terminal Server.

telnet-options

See *Set Telnet-Client* in the *Users Guide*.

rlogin-options

See *Set Rlogin-Client* in the *Users Guide*.

ssh-options

See *Set SSH-Client* in the *Users Guide*.

tunnel_name

Provide a name for this tunnel. This name must match the name on the tunnel peer Secure Terminal Server.

strict-host-key-checking

When enabled, a host public key (for each host you wish to ssh to) must be downloaded to the Terminal Server.

Default: Enabled

Show Line Users

Description Shows the users who are on the line.

User Level Admin

Syntax `show line users`

SSH

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-cbc arcfour aes-ctr
aes-gcm chacha20-poly1305> 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 Secure Terminal Server will use for the SSH version 2 connection:

- **3des**
- **blowfish**
- **aes-cbc**
- **arcfour**
- **cast**
- **aes-ctr**
- **aes-gcm**
- **chacha20-poly1305**

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 Termtypes

Description Shows the terminal type for the current session.
User Level Admin
Syntax **show termtypes**

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>*]
[*termtypes* *<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.
termtypes
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 Secure Terminal Server to call the user back (the **Callback** parameter is unrelated to the **Line Dial** parameter).

Note: the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. The Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server 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, CLI, or WebManager. The Secure Terminal Server supports one custom language that must be downloaded to the Secure Terminal Server; otherwise, **Customlang** defaults to English.

level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the Secure Terminal Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Secure Terminal Server.
- **Normal**—The Normal level user has limited access to the Secure Terminal Server. 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 Secure Terminal Server. 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 Secure Terminal Server 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 Secure Terminal Server to the device.
- **Read Out**—Users are given access to read only inbound data, data that is going from the device to the Secure Terminal Server.

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 Secure Terminal Server 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 spaces).

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 Secure Terminal Server.
- **Send**—RIP packets can only be sent by the Secure Terminal Server.
- **Listen**—RIP packets can only be received by the Secure Terminal Server.
- **Send and Listen**—RIP packets are sent and received by the Secure Terminal Server.

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 Secure Terminal Server 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, this is the target host name or IP address. 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 Secure Terminal Servers 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	<code>set user . [hotkey-prefix <00-7f>] [language english customlang] [password] [routing none send listen send-and-listen]</code>
Admin User Only	<code>set user . <username> * [callback on off]</code> <code>[framed-compression on off] [framed-ip <IPv4_address>]</code> <code>[framed-interface-id <IPv6_interface_id>]</code> <code>[framed-mtu <64-1500>] [hotkey-prefix <00-7f>]</code> <code>[idle-timer <0-4294967>]</code> <code>[host-ip None <IP_address> <config_host> <tunnel_name>]</code> <code>[language english customlang]</code> <code>[level admin normal restricted menu] [password]</code> <code>[line-access readin readout readwrite [on off] <line(s)> [0]]</code> <code>[netmask <IPv4_address>] [phone-number <phone_number>]</code> <code>[routing none send listen send-and-listen]</code> <code>[service dsprompt telnet tcp-clear rlogin ppp slip ssh]</code> <code>[sess-timer <0-4294967>] [port tcp-clear telnet ssh <TCP_port>]</code> <code>[access-clustered-ports on off]</code>
Options	callback <p>When On, enter a phone number for the Secure Terminal Server to call the user back (the Callback parameter is unrelated to the Line Dial parameter).</p> <p>Note: the Secure Terminal Server 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.</p> <p>The Secure Terminal Server supports another type of callback, Roaming Callback, which is configurable when the Line Service is set to PPP.</p>

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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. The Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server 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 Secure Terminal Server.

language

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

level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the Secure Terminal Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Secure Terminal Server.
- **Normal**—The Normal level user has limited access to the Secure Terminal Server. 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 Secure Terminal Server. Does not have any access to CLI commands.

line-access

Specifies the user access rights to each Secure Terminal Server 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 Secure Terminal Server to the device.
- **Read Out**—Users are given access to read only inbound data, data that is going from the device to the Secure Terminal Server.

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).

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 Secure Terminal Server. This case-sensitive field accepts a maximum of 16 characters.

phone-number

The phone number the Secure Terminal Server 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 spaces).

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 Secure Terminal Server.
- **Send**—RIP packets can only be sent by the Secure Terminal Server.
- **Listen**—RIP packets can only be received by the Secure Terminal Server.
- **Send and Listen**—RIP packets are sent and received by the Secure Terminal Server.

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 Secure Terminal Server 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, this is the target host name or IP address. 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 Secure Terminal Servers 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](#) on page 55 for the options descriptions.

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-cbc arcfour aes-ctr
aes-gcm chacha20-poly1305>
```

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.

4 Line Commands

This chapter defines all the CLI commands associated with configuring the line parameters for the Secure Terminal Server.

1-Port vs. 2-Port+ Line Commands

If you are using a 1-port Secure Terminal Server, 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+ Secure Terminal Server, 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-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 Secure Terminal Server is being used as a router (depending on which end of the link your Secure Terminal Server 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 Secure Terminal Server 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 1 or **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 Secure Terminal Server 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 Secure Terminal Server ignores the break key completely and it is not passed through to the host. This is the default setting.
- **local**—The Secure Terminal Server 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 Secure Terminal Server 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: 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**.

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 Terminal Server causes all buffered data to be lost.

The minimum data buffer size for all models is 1K. 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 H* in the *BLACK BOX® User Guide* for more information.

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

Values: 1-4000 (all other models)

Default: Disabled

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**.

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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server'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 Secure Terminal Server 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 Secure Terminal Server will wait to establish a connection to a remote modem. The default value is **45** seconds.

dial-retries

The number of times the Secure Terminal Server 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+ Secure Terminal Server 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 Secure Terminal Server by the specified Internet Address (or host name that can be resolved by a DNS). You must reboot the Secure Terminal Server 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: 1000 ms

A value of 0 will cause the "request to send a break signal" to be ignored.

discard-characters-with-error

When enabled, the Terminal Server will discard characters received with a parity or framing error.

Default: Disabled.

rts-toggle

Configure the Toggle RTS Feature if your application needs for RTS to be raised during character transmission.

Initial delay: configure the time (in ms) between the time the RTS signal is raised and the start of character transmission. This delay only applies if this port is not running hardware flow control. If hardware flow control is used, the transmission will occur as soon as CTS is raised by the modem.

Final delay: configure the time (in ms) between the time of character transmission and when RTS is dropped.

Initial delay range: 0-1000 ms

Final delay range: 0-1000 ms

Default: Off

Set Line Interface

The SCS and STS Secure Terminal Server models only support the EIA-232 interface and therefore does not require the **interface** parameter, instead you can just set the parameters for the EIA-232 interface.

Description Configures line interface (hardware) parameters.

User Level Admin

Syntax	<pre> 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>] </pre>
Options	<p>eia-232 eia-422 eia-485-half-duplex eia-485-full-duplex</p> <p>Specifies the type of serial line that is being used with the Secure Terminal Server. 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.</p> <p>monitor-dcd</p> <p>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 Secure Terminal Server 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.</p> <p>monitor-dsr</p> <p>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 Secure Terminal Server 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.</p> <p>flow</p> <p>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.</p> <p>tx-driver-control</p> <p>Used with a EIA-485 serial interface, if your application supports RTS (Request To Send), select this option. Otherwise, select Auto. Default is Auto.</p> <p>duplex</p> <p>Specify whether the line is Full Duplex (communication both ways at the same time) or Half Duplex (communication in one direction at a time).</p>

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, and COMredirect.

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>]

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

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

Options **bidir**

This service allows the Secure Terminal Server 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 Secure Terminal Server host table.

<server_port>

The Secure Terminal Server port number.

<host_port>

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

direct

Direct connections bypass the Secure Terminal Server, enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Secure Terminal Server 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 redisplay 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 Secure Terminal Server displays a login on that line. For example, **DSLogin** is used when a System Administrator configures the Secure Terminal Server, providing authentication of a user before starting a **User Service** of **SLIP**, or users starts a session(s) from the Secure Terminal Server to hosts.

printer

Using the Secure Terminal Server 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 Secure Terminal Server 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.

comredirect

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

client-initiated

When this option is turned on, the Secure Terminal Server will wait for a connection from the COMredirect host (see the COMredirect documentation for information on how to set up this feature on the COMredirect host). When this option is turned off, the Secure Terminal Server will initiate the connection to the COMredirect 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 COMredirect 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 COMredirect 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 *Users Guide* for a more detailed explanation).

tunnel_name

Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Secure Terminal Server

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 Termttype

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 termttype [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: <ul style="list-style-type: none"> • 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 Rlogin-Client

Description	Configures the Rlogin parameters for the specified line. When the Secure Terminal Server initiates an rlogin connection to a host, it is acting as a rlogin client.
User Level	Normal, Admin
Syntax	set rlogin-client line . <number> * termttype <terminal_name>
Option	termttype 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 Secure Terminal Server 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 Secure Terminal Server initiates a SSH connection to a host, it is acting as a SSH client.
User Level	Normal, Admin
Syntax	<pre>set ssh-client line . <number> * [termttype <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-cbc arcfour aes-ctr aes-gcm chacha20-poly1305arcfour></pre>
Options	<p>termttype Type of terminal attached to this line; for example, ANSI or WYSE60.</p> <p>protocol Specify the SSH protocol you want to use for the connection, SSH-1, SSH-2, or either, SSH2/1.</p> <p>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.</p> <p>verbose Displays debug messages on the terminal.</p> <p>auto-login Creates an automatic SSH login, using the Name and Password values.</p> <p>name The user's name when Auto Login is enabled.</p> <p>password The user's password when Auto Login is enabled.</p> <p>ssh-1-cipher Select the encryption method (cipher) that you want to use for your SSH version 1 connection:</p> <ul style="list-style-type: none"> • 3DES • Blowfish

ssh-2-cipher-list

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

- **3des**
- **blowfish**
- **aes-cbc**
- **arcfour**
- **cast**
- **aes-ctr**
- **aes-gcm**
- **chacha20-poly1305**

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 Secure Terminal Server.

Set PPP

Description Configures the Lines PPP settings.

User Level Admin

Syntax

```
set ppp 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] [echo-retry <0-255>]
[echo-timeout <0-255>]
```

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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server'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 Secure Terminal Server. If you set the **PPP** parameter **IP Address Negotiation** to **On**, the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server'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**.

mrui

The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the Secure Terminal Server'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 Secure Terminal Server, 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server. If you set the PPP parameter IP Address Negotiation to **On**, the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server to use the remote IP address value configured here.

roaming-callback

A user can enter a telephone number that the Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. 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 Secure Terminal Server, from a remote location, or authenticate a remote client/device, from the Secure Terminal Server.

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 Terminal Server 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 Secure Terminal Server and the remote client/device have the same setting. For example, if the Secure Terminal Server 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 Secure Terminal Server, 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 Secure Terminal Server will use the value in the RADIUS file in preference to the value configured here.

echo-timeout

The maximum time, in seconds, between sending an echo request packet if no response is received from the remote host.

Range: 0-255

Default: 90

echo-retry

The maximum number of times an echo request packet will be re-sent before the link is terminated.

Range: 0-255

Default: 30

Set PPP Dynamic-DNS

- Description** This option is only available when IP address negotiation (**ipaddr-neg**) is **on**. When enabled, the Secure Terminal Server 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 SLIP settings for the line.
- 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 Secure Terminal Server 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 Secure Terminal Server'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 Secure Terminal Server. Enter a value between 256 and 1500. The default value is **256**. If your user is authenticated by the Secure Terminal Server, 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server. If your user is authenticated by the Secure Terminal Server, 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 Secure Terminal Server 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 Secure Terminal Server, 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 Secure Terminal Server 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> [<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>
[<start_IP_address>] [<end_IP_address>]
```

Options

```
set udp line .|<number>|* entry 1|2|3|4 none
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 Secure Terminal Server 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 Secure Terminal Server 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, Secure Terminal Server 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 Secure Terminal Server will forward the data to the IP address range and UDP port configured for this entry. If **auto-learn** is enabled, the Secure Terminal Server must receive a UDP message before it can send one, since the UDP port number is learned from the received message.

auto-learn

The Secure Terminal Server 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 tunnel name on the tunnel peer Secure Terminal Server

any-port

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

specific

The port that the Secure Terminal Server will use to relay messages to servers/hosts or the port from which the Secure Terminal Server will receive messages to be forwarded to the serial port.. This option works with any setting except **None**. The Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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	<pre>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]</pre>
Options	<p>echo</p> <p>When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Disabled by default.</p> <p>failure-string</p> <p>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.</p> <p>host</p> <p>The target host name.</p> <p>init-string</p> <p>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.</p> <p>See <i>VModem Initialisation Commands</i> in the <i>Users Guide</i> for a more detailed explanation of the support initialisation commands.</p> <p>mode</p> <p>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.</p> <p>port</p> <p>The port number the target host is listening on for messages.</p> <p>response-delay</p> <p>The amount of time, in milliseconds, before an AT response is sent to the requesting device. The default is 250 ms.</p>

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 Secure Terminal Server 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** INTERFACE 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 search 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 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 models support up to 48 entries.
User Level	Admin
Syntax	<pre>set vmodem-phone entry <number> phone-number <string> <ip_address <number> host <string>] [port <TCP_port>]</pre> <pre>set vmodem-phone entry <number> delete</pre>
Options	<p>entry Specify the entry number in the vmodem phone number table.</p> <p>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.</p> <p><ip_address> Specify the IP address of the remote host that is receiving the vmodem connection.</p> <p><host> Select the hostname (from the host table) of the remote host that is receiving the vmodem connection.</p> <p><port> Specify the TCP port that the remote host is listening on for the vmodem connection</p> <p>delete Deletes the specified entry from the phone number table.</p> <p>tunnel_name Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Secure Terminal Server</p>

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 and COMredirect.
User Level	Admin
Syntax	<pre>set ssl line . <number> * [enable on off] [use-server on off] [version any tslv1 sslv3 tslv1.1 tslv1.2] [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>]</pre>
Options	<p>enable Activates the SSL/TLS settings for the line.</p> <p>use-server Uses the SSL/TLS server configuration for the line.</p>

version

Specify whether you want to use:

- **Any**—The Terminal Server will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try all other connection methods.
- **TLSv1**—The connection will use only TLSv1
- **SSLv3**—The connection will use only SSLv3
- **TLSv1.1**—The connection will use only TLSv1.1
- **TLSv1.2**—The connection will use only TLSv1.2

The default is **Any**.

type

Specify whether the Secure Terminal Server 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 Secure Terminal Server.

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

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-gcm|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
- AES-GCM
- 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.
- **ECDH-ECDSA**—This is an ECDH key exchange using an ECDSA key and certificate.

The default is **Any**.

hmac

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

- Any
- MD5
- SHA1
- SHA256
- SHA384

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 Secure Terminal Server 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 octet 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 Secure Terminal Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Secure Terminal Server will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.

Set Multihost

Description	Configures multiple hosts or a primary/backup host schema for Silent Raw, Reverse Raw, or Client-Initiated COMredirect 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	<pre>set multihost line <number> entry <number> host <host> <tunnel_name> <TCP_port> set multihost line <number> entry <number> delete</pre>
Options	<p>entry</p> <p>You can specify up to 49 hosts in the multihost table.</p> <p>host <host></p> <p>Specify the preconfigured host that will be in the multihost list.</p> <p>tunnel_name</p> <p>Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Secure Terminal Server</p> <p><TCP_port></p> <p>Specify the TCP port that the Secure Terminal Server will use to communicate to the Host.</p> <p>delete</p> <p>Deletes the specified entry from the multihost table.</p>

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 Interface

Description Shows the network interface information.

User Level Admin

Syntax `show interface [brief|ppp|slip|ethernet]`

Show PPP

Description Shows the PPP line settings.

User Level Admin

Syntax `show ppp line <number>`

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 string for a modem defined in the modem table.

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 Secure Terminal Server 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	<pre>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]</pre>
Options	<p>from</p> <p>This field will be specified in the from field of the email message sent by the Secure Terminal Server.</p> <p>level</p> <p>Choose the event level that triggers an email notification:</p> <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Info • Debug <p>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.</p> <p>mode</p> <p>Determines whether or not email notification is turned on. Default is Off.</p> <p>to</p> <p>An email address or list of email addresses that will receive the email notification.</p> <p>reply-to</p> <p>The email address to whom all replies to the email notification should go.</p> <p>smtp-host</p> <p>The SMTP host (email server) that will process the email notification request. This can be either a host name defined in the Secure Terminal Server host table or the SMTP host IP address.</p> <p>subject</p> <p>A text string, which can contain spaces, that will display in the Subject field of the email notification.</p> <p>use-server</p> <p>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.</p>

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 Secure Terminal Server. 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 Secure Terminal Server 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 Secure Terminal Server 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 Secure Terminal Server 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 <i><number></i>

5

Network Commands

This chapter defines all the CLI commands associated with configuring the network parameters for the Secure Terminal Server.

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 Secure Terminal Server.

The IPv4 or IPv6 address of the SNMP manager that will send requests to the Secure Terminal Server. If the address is `0.0.0.0`, any SNMP manager with the **Community Name** can access the Secure Terminal Server. 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 Secure Terminal Server.

`none|readonly|readwrite`

Permits the Secure Terminal Server 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 Secure Terminal Server supports SNMP traps for restart and SNMP community authentication error.

User Level Admin

Syntax **add trap** *<trap_name>* *<config_host>*|*<IP_address>* *<version>* *<type>* *<tunnel_name>*

Options *<trap_name>*

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 Secure Terminal Server. Up to four trap hosts can be defined.

version

Select the version of the trap you want the Terminal Server 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 Secure Terminal Server.

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	<p>contact</p> <p>The name and contract information of the person who manages this SMNP node.</p> <p>location</p> <p>The physical location of the SNMP node.</p> <p>readonly user</p> <p>Specify the name of the readonly user.</p> <p>readwrite user</p> <p>Specify the name of the read/write user.</p> <p>trap user</p> <p>Specify the name of the trap user.</p>

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	<p>type</p> <p>Select the user type you wish to configure. The options are readonly, readwrite and trap.</p> <p>security-level</p> <p>Select the security level for the user type being defined. The valid options are:</p> <p>none - no security or authentication will be used.</p> <p>auth/nopriv - authentication but no privacy will be used.</p> <p>auth/priv - both authentication and privacy with be used.</p> <p>auth-algorithm</p> <p>Specify the authentication algorithm that will be used for this user. The options are MD5 or SHA1. The default is MD5.</p> <p>auth-password</p> <p>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 your password to ensure accuracy</p> <p>privacy-algorithm</p> <p>Specify the privacy (encryption) algorithm to be used for this user. Valid options are des or aes.</p> <p>privacy-password</p> <p>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 your password to ensure accuracy</p>

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 Terminal Server on your network. The default engine id uses the MAC address of the Ethernet interface to ensure the engine id is unique to this agent. To set the engine id back to the default, enter a null string <"">.

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 Terminal Server 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-retries <number>
User Level Admin
Syntax `set snmp inform-retries <number>`
Options `number`

This is the number of times the Terminal Server 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 Secure Terminal Server TFTP client settings.
User Level Admin
Syntax `set server tftp [retry <integer>] [timeout <integer>]`

Options retry

The number of times the Secure Terminal Server will retry to transmit a TFTP 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 Secure Terminal Server will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the Secure Terminal Server 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 Secure Terminal Server 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|aes-ctr|aes-gcm|chacha20-poly1305]`

Options host

This is the name of the SFTP host. The name must come from the Terminal Server's 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 and keyboard-interactive. At least one method must be enabled.

The default is to have all methods enabled.

auto-login

You can have the Terminal Server automatically login to the SFTP server. When set, the Terminal Server will use the name and password fields to login to the SFTP server.

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 of data is desirable on slow connections, however on faster networks, compression will degrade overall data transmission rates.

protocol

Select the protocol you are going to use with the SFTP server. You can enable ssh1, ssh2 or both. At least one protocol must be enabled.

ssh1

Enable to negotiate the ssh1 protocol.

ssh-1-cipher

Select the encryption cipher to be used if the ssh1 protocol is used . Valid options are 3des or blowfish.

ssh2

Enable to negotiate the ssh2 protocol.

ssh-2cipher-list

Show SFTP

Description Shows the SFTP settings.

User Level Admin

Syntax `show sftp`

Hosts Commands

Add Host

Description Adds a host to the Secure Terminal Server 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 Secure Terminal Server, 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 Secure Terminal Server 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 Secure Terminal Server host table.
User Level	Admin
Syntax	set host <i><config_host></i> <i><IP_address></i> set host <i><config_host></i> fqdn <i><text></i>
Options	<i><config_host></i> The name of the host. <i><IP_address></i> The host IPv4 or IPv6 address. fqdn When you have DNS defined in the Secure Terminal Server, 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 Secure Terminal Server 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 <i><IP_address></i>
Option	<i><IP_address></i> 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 <i><IP_address></i>
Option	<i><IP_address></i> 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 50 hosts on desktop models and 49 hosts on rack mount models to act as gateways in your network. Each gateway host must be defined in the Secure Terminal Server'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	<pre>set syslog [level emergency alert critical error warning notice info debug] [primary-host <config_host>] [secondary-host <config_host>] <tunnel-name></pre>
Options	<p>level</p> <p>Choose the event level that triggers a syslog entry:</p> <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Info • Debug <p>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.</p> <p>primary-host</p> <p>The first preconfigured host that the Secure Terminal Server will attempt to send system log messages to; messages will be displayed on the host's monitor.</p> <p>secondary-host</p> <p>If the Secure Terminal Server cannot communicate with the primary host, then the Secure Terminal Server will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor.</p> <p>tunnel_name</p> <p>Provide a name for this tunnel. This name must match the name on the tunnel peer Secure Terminal Server.</p>

Show Syslog

Description	Shows the syslog settings.
User Level	Admin
Syntax	<code>show syslog</code>

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 <i><integer_md5_id></i> <i><start_date></i> <i><start_time></i> <i><end_date></i> <i><end_time></i>
Options	<p><i><integer_md5_id></i></p> <p>The MD5 identification key.</p> <p><i><start_date></i></p> <p>The start date that the MD5 key becomes valid. The date format is dependent on your system's settings.</p> <p><i><start_time></i></p> <p>The time that the MD5 key becomes valid. The time format is dependent on your system's settings.</p> <p><i><end_date></i></p> <p>The last day that the MD5 key is valid. The date format is dependent on your system's settings.</p> <p><i><end_time></i></p> <p>The time that the MD5 key becomes invalid. The time format is dependent on your system's settings.</p>

Delete RIP

Description	Deletes a RIP MD5 key.
User Level	Admin
Syntax	delete rip md5 <i><integer_md5_id></i>
Option	<p><i><integer_md5_id></i></p> <p>You can see a list of MD5 IDs available for deletion by typing delete rip md5 ?.</p>

Set RIP

Description	Configures the RIP MD5 key. After pressing Enter, you will be prompted for the MD5 key value.
User Level	Admin
Syntax	<pre>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]</pre>
Options	<p>authentication</p> <p>Specify the type of RIP authentication:</p> <ul style="list-style-type: none"> • None—No authentication for RIP. • Password—Simple RIP password authentication. • MD5—Use MD5 RIP authentication. <p>ethernet-mode</p> <p>Enable/disable RIP (Routing Information Protocol) mode for the Ethernet interface with one of the following options:</p> <ul style="list-style-type: none"> • 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. <p>password</p> <p>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.</p> <p><configured_md5_id></p> <p>The MD5 identification key.</p> <p>end <date> <time></p> <p>The last day that the MD5 key is valid. Specify as dd/mm/yyyy.</p> <p>The time that the MD5 key becomes invalid. Specify as hh:mm:[ss].</p> <p>start <date> <time></p> <p>The start date that the MD5 key becomes valid. Specify as dd/mm/yyyy.</p> <p>The time that the MD5 key becomes valid. Specify as hh:mm:[ss].</p> <p>key</p> <p>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.</p>

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 Secure Terminal Server expects all connections to be established through a VPN tunnel. To allow 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 Secure Terminal Server and upload the IPsec RSA public key from the Secure Terminal Server 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 Secure Terminal Server.

The default is shared secret.

boot-action

Determines the state of the VPN network when the Secure Terminal Server 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 Secure Terminal Server-side of the VPN tunnel. The default is left.

local-external-ip-address

When **NAT Traversal (NAT_T)** is enabled, this is Secure Terminal Server's external IPv4 or IPv6 address or FQDN. When the Secure Terminal Server 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 Secure Terminal Server will provide a VPN connection to.

local-ip-address

The IPv4 or IPv6 address or FQDN of the Secure Terminal Server. You can specify **%defaultroute** when the IP address of the Secure Terminal Server 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 Secure Terminal Server. Leave this parameter blank if you want to use the **Default Gateway** configured in the Secure Terminal Server.

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 Secure Terminal Server 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 Secure Terminal Server (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 successful 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 asterisk (*) 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 Secure Terminal Server 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	<code>set ipv6tunnel <config_tunnel_name> [mode manual teredo 6to4] [gateway <interface>] [remote-host <config_host>]</code>
Options	<p>mode</p> <p>The method or protocol that is used to create the IPv6 tunnel.</p> <ul style="list-style-type: none"> • Manual—When enabled, the Secure Terminal Server will manually create the IPv6 tunnel to the specified Remote Host through the specified Interface. • 6to4—When enabled, the Secure Terminal Server 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 Secure Terminal Server. • 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. <p>Default: Manual</p> <p>gateway</p> <p>The interface that the Secure Terminal Server 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.</p> <p>Default: ethernet_1</p> <p>remote-host</p> <p>The IPv4 host that can access the IPv6 network when the Mode is Manual. The Teredo server when the Mode is Teredo.</p> <p>Default: None</p>

Show IPv6tunnel

Description	Shows the specified IPv6 tunnel settings.
User Level	Admin
Syntax	<code>show ipv6tunnel <config_tunnel_name></code>

Delete IPv6tunnel

Description	Controls the state of all IPsec tunnels.
User Level	Admin
Syntax	<code>delete ipv6tunnel <config_tunnel_name></code>
Options	<code><config_tunnel_name></code>

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 Secure Terminal Server expects all connections to be established through a VPN tunnel. To allow 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 Secure Terminal Server, 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 Secure Terminal Server.

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 successful 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 Secure Terminal Server will listen on for L2TP/IPsec connections. If the default value (0.0.0.0) is kept, the Secure Terminal Server 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 Secure Terminal Server 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 assigned 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 Secure Terminal Server 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>`

Options `add vpn-exception host-ip <ipv4/ipv6_address>`
`network-ip <ipv4_net_ip> <network_subnet>|<ipv6_net_ip> <prefix_bits>`

The network address that will communicate with the Secure Terminal Server 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 Secure Terminal Server 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>`

Options `set vpn-exception <config_vpn_except> host-ip <ipv4/ipv6_address>`
`network-ip <ipv4_net_ip> <network_subnet>|<ipv6_net_ip> <prefix_bits>`

The network address that will communicate with the Secure Terminal Server 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 Secure Terminal Server 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 Terminal Server 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 Terminal Server has a listener on the same local TCP port. If not entered, the IP address of the Terminal Server 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

Specify 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 Terminal Server 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 Terminal Server to authenticate with the proxy server.

tunnel-name

Select an existing tunnel. This tunnel must match the tunnel name on the tunnel peer Terminal Server DS.

https

The Terminal Server will use secure access (HTTPS) mode to connect to the listening Terminal Server.

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 Terminal Server DS.

listen

Listen for connection requests generated from the connecting Terminal Server 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`

6 Time Commands

This chapter defines all the CLI commands associated with configuring the time parameters for the Secure Terminal Server.

Server Commands

Set Time

Description Sets the Secure Terminal Server system clock.
User Level Admin
Syntax `set time <hh:mm[:ss]>`
Option `<hh:mm[:ss]>`
Sets the Secure Terminal Server's system time, using the 24-hour clock time format (00:00-23:59).

Set Timezone

Description Sets the Secure Terminal Server'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 Secure Terminal Server'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	<code>add sntp [server-1 <config_host>] [server-2 <config_host>]</code>
Options	<p>server-1</p> <p>The name of the primary NTP/SNTP server from the Secure Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Secure Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.</p> <p>server-2</p> <p>The name of the secondary NTP/SNTP server from the Secure Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Secure Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.</p>

Delete SNTP

Description	Deletes an SNTP server.
User Level	Admin
Syntax	<code>delete sntp server-1 server-2</code>
Options	<p>server-1</p> <p>The name of the primary NTP/SNTP server from the Secure Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Secure Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.</p> <p>server-2</p> <p>The name of the secondary NTP/SNTP server from the Secure Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Secure Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.</p>

Set SNTP

Description	Configures an SNTP server.
User Level	Admin
Syntax	<code>set sntp mode none unicast anycast multicast</code> <code>[server-1 <config_host>] [server-2 <config_host>]</code> <code>[version 1 2 3 4] [server-authentication on off]</code> <code>[keyid-1 <1-65534>] [keyid-2 <1-65534>]</code>
Options	<p>mode</p> <p>The SNTP mode. Valid modes are:</p> <ul style="list-style-type: none"> • 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 Secure Terminal Server host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the Secure Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.

server-2

The name of the secondary NTP/SNTP server from the Secure Terminal Server host table. Valid with **Unicast** and **Multicast** modes, although in **Multicast** mode, the Secure Terminal Server 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 Terminal Server.

Valid keyids: 1-65534

(**Note:** The structure for the ntp/sntp (symmetric key) file can be found in your *BLACK BOX® User Guide - Appendix J*)

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 Secure Terminal Server'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 Secure Terminal Server system clock.

User Level Normal, Admin

Syntax `show date`

Show Summertime

Description Shows the summertime settings.

User Level Admin

Syntax `show summertime`

7 Administration Commands

This chapter defines all the CLI commands associated with configuring the administrative parameters for the Secure Terminal Server.

Bootup Commands

Reboot

Description Reboots the Secure Terminal Server. 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 Port Statistics

Description Resets the serial port statistics.
User Level Admin
Syntax `reset serial-statistics [<line number>|*]`

Reset Factory

Description Resets the Secure Terminal Server 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 the remote TFTP host and pathname for files to be loaded after a Secure Terminal Server reboot.
User Level	Admin
Syntax	set bootup firmware host <hostname> [file <path_filename>] set bootup configuration host <hostname> [file <path_filename>]
Options	<p>firmware file</p> <p>The path and file name, relative to the default path of your TFTP server software, of the update software for the Secure Terminal Server that will be loaded when the Secure Terminal Server is rebooted.</p> <p>configuration file</p> <p>The path and file name, relative to the default path of your TFTP server software, of the configuration software for the Secure Terminal Server that will be loaded when the Secure Terminal Server is rebooted.</p> <p>host</p> <p>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 Secure Terminal Server's host table or be resolved by DNS.</p> <p>firmware sftp or configuration sftp</p> <p>If this parameter is set to on, the Terminal Server will use SFTP to transfer the firmware or configuration file. The sftp specific parameters are set using the set sftp command.</p> <p>If the host is configured using this command, it will be used instead of the one configured by the set sftp host command.</p>

Show ARP

Description	Shows the current contents of the ARP cache.
User Level	Admin
Syntax	show arp

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 Secure Terminal Server bootup.
User Level	Admin
Syntax	show bootup

TFTP File Transfer Commands

Netload

Description	Transfers a file from a remote host to the Secure Terminal Server 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	<p>text-config</p> <p>Specify this option if you are uploading a text-based configuration file to the Secure Terminal Server from a TFTP server.</p> <p>factory-default-config</p> <p>Specifies the configuration file that you are going to load from a SFTP/TFTP server to the Secure Terminal Server that will act as the factory default configuration. See the <i>User Guide</i> for directions on how to revert back to the original factory default configuration, if required.</p> <p>firmware</p> <p>Specifies that you are going to download a new firmware file to the Secure Terminal Server.</p> <p>configuration</p> <p>Specifies that you are going to download a new configuration file to the Secure Terminal Server.</p> <p>customlang</p> <p>Specifies that you are going to download a custom language file to the Secure Terminal Server.</p> <p>term1 term2 term3</p> <p>You can create and download up to three custom terminal definitions to the Secure Terminal Server.</p> <p>other-file</p> <p>Specify this option when you are downloading a custom Message of the Day (MOTD) file, a custom PAP secrets file (must be named pap-secrets), a custom CHAP secrets file (must be named chap-secrets), or a custom default configuration file.</p> <p><hostname/IP_address></p> <p>The IP address or host name where the file you are downloading to the Secure Terminal Server resides. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server. If using SFTP, you must specify a user.</p> <p>Specify the host in the following format:</p> <p>user@host where:</p> <p>user - the user name to use</p> <p>host - can be a fully qualified name, a name from the Secure Terminal Server's Host Table or the IPV4 or IPV6 address.</p> <p>If you have not configured a password using the set sftp password command, you will be prompted to enter it.</p> <p><*></p> <p>Select * to use a preconfigured HTTP tunnel.</p>

<filename>

The complete path and file name of the file you are downloading to the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).

Netsave

Description	Transfers a file from the Secure Terminal Server to a remote host using the TFTP protocol.
User Level	Admin
Syntax	netsave configuration crash serialt-buf text-config <i><hostname/IP_address> <*> <filename></i>
Options	<p>configuration</p> <p>Specifies that you are going to upload a configuration file from the Secure Terminal Server to the specified host or IP address.</p> <p>crash</p> <p>Specifies that you are going to upload a crash file from the Secure Terminal Server to the specified host or IP address.</p> <p>serialt-buf</p> <p>Specifies that you are going to upload the contents of the serial trace buffer.</p> <p>text-config</p> <p>Saves the current configuration to a text file on a SFTP/TFTP server.</p> <p><i><hostname/IP_address></i></p> <p>The IP address or host name for where the file you are uploading from the Secure Terminal Server is going. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server.</p> <p><i><*></i></p> <p>Select * to use a preconfigured HTTP tunnel.</p> <p><i><filename></i></p> <p>The complete path and file name for the file you are uploading from the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).</p>

SFTP File Transfer Commands

Snetload

Description	Transfers a file from a remote host to the Secure Terminal Server using the SFTP protocol.
User Level	Admin
Syntax	snetload text-config factory-default-config firmware configuration customlang term1 term2 term3 customapp-file wan-driver <i><hostname/IP_address> <*> <filename></i>
Options	<p>text-config</p> <p>Specify this option if you are uploading a text-based configuration file to the Secure Terminal Server from a SFTP server.</p>

factory-default-config

Specifies the configuration file that you are going to load from a SFTP/TFTP server to the Secure Terminal Server 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 Secure Terminal Server.

configuration

Specifies that you are going to download a new configuration file to the Secure Terminal Server.

customlang

Specifies that you are going to download a custom language file to the Secure Terminal Server.

term1|term2|term3

You can create and download up to three custom terminal definitions to the Secure Terminal Server.

other-file

Specify this option when you are downloading a custom Message of the Day (MOTD) file, a custom PAP secrets file (must be named **pap-secrets**), a custom CHAP secrets file (must be named **chap-secrets**), or a custom default configuration file.

<hostname/IP_address>

The IP address or host name where the file you are downloading to the Secure Terminal Server resides. If you are using a host name, it must be resolved in either the Secure Terminal Server's **Host Table** or a DNS server. 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 Secure Terminal Server's **Host Table** or the IPV4 or IPV6 address.

If you have not configured a password using the set sftp password command, you will be prompted to enter it.

<*>

Select * to use a preconfigured HTTP tunnel.

<filename>

The complete path and file name of the file you are downloading to the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).

Snetsave

Description Transfers a file from the Secure Terminal Server to a remote host using the SFTP protocol.

User Level Admin

Syntax **snetsave** **configuration|crash|serialt-buf|text-config**
<hostname/IP_address> **<*>** **<filename>**

Options	<p>configuration</p> <p>Specifies that you are going to upload a configuration file from the Secure Terminal Server to the specified host or IP address.</p> <p>crash</p> <p>Specifies that you are going to upload a crash file from the Secure Terminal Server to the specified host or IP address.</p> <p>serialt-buf</p> <p>Specifies that you are going to upload the contents of the serial trace buffer.</p> <p>text-config</p> <p>Saves the current configuration to a text file on a SFTP/TFTP server.</p> <p><hostname/IP_address></p> <p>The IP address or host name for where the file you are uploading from the Secure Terminal Server is going. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server.</p> <p><*></p> <p>Select * to use a preconfigured HTTP tunnel.</p> <p><filename></p> <p>The complete path and file name for the file you are uploading from the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).</p>
----------------	---

Custom Factory Default

Netload

Description	Transfers a file from a remote host to the Secure Terminal Server using the TFTP protocol.
User Level	Admin
Syntax	netload factory-default-config <hostname IP_address> <*> <filename>
Options	<p>factory-default-config</p> <p>Specifies the configuration file that you are going to load from a SFTP/TFTP server to the Secure Terminal Server that will act as the factory default configuration. See the <i>User Guide</i> for directions on how to revert back to the original factory default configuration, if required.</p> <p><hostname/IP_address></p> <p>The IP address or host name where the file you are downloading to the Secure Terminal Server resides. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server. If using SFTP, you must specify a user.</p> <p>Specify the host in the following format:</p> <p>user@host where:</p> <p>user - the user name to use</p> <p>host - can be a fully qualified name, a name from the Secure Terminal Server's Host Table or the IPV4 or IPV6 address.</p> <p>If you have not configured a password using the set sftp password command, you will be prompted to enter it.</p>

<*>

Select * to use a preconfigured HTTP tunnel.

<filename>

The complete path and file name of the file you are downloading to the Secure Terminal Server (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 Secure Terminal Server using the SFTP protocol.
User Level	Admin
Syntax	snetload factory-default-config <hostname/IP_address> <*> <filename>
Options	<p>factory-default-config</p> <p>Specifies the configuration file that you are going to load from a SFTP/TFTP server to the Secure Terminal Server that will act as the factory default configuration. See the <i>User Guide</i> for directions on how to revert back to the original factory default configuration, if required.</p> <p><hostname/IP_address></p> <p>The IP address or host name where the file you are downloading to the Secure Terminal Server resides. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server. If using SFTP, you must specify a user.</p> <p>Specify the host in the following format:</p> <p>user@host where:</p> <p>user - the user name to use</p> <p>host - can be a fully qualified name, a name from the Secure Terminal Server's Host Table or the IPV4 or IPV6 address.</p> <p>If you have not configured a password using the set sftp password command, you will be prompted to enter it.</p> <p><*></p> <p>Select * to use a preconfigured HTTP tunnel.</p> <p><filename></p> <p>The complete path and file name of the file you are downloading to the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).</p>

Set

Description	Sets the current configuration on Secure Terminal Server to act as the factory default configuration. See the <i>User Guide</i> 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 Secure Terminal Server.

User Level Admin

Syntax

```
netload ssl certificate|private-key <hostname/IP_address>
<filename>

netload ldap certificate <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 snmp-keys <hostname/IP_address> <filename>
```

Options certificate|private-key

If you are using the secure version of the WebManager (HTTPS), then you need to download the SSL/TLS private key and CA list to make a secure connection.

ldap certificate

If you are using LDAP authentication with TLS, you need to download the certificate of the CA who signed the LDAP certificate to the Secure Terminal Server for authentication to work properly.

ssh-client host

The public key for the host that is being authenticated by the Secure Terminal Servers 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 Secure Terminal Server, 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 Secure Terminal Server for that specific tunnel.

<hostname/IP_address>

Enter the host or IP address that contains the certificate/key you are downloading to the Secure Terminal Server. If you are using a host name, If you are using a host name, it must be resolved in either the Secure Terminal Server's **Host Table** or a DNS server.

<filename>

Enter the complete path and file name of the certificate/key you are downloading to the Secure Terminal Server.

sntp-keys

Enter the complete path and file name of the sntp file that you are downloading to the Terminal Server.

Netsave

Description	Uploads certificates and keys from the Secure Terminal Server to a remote host using TFTP.
User Level	Admin
Syntax	netsave ssh-server public-key ssh-2 rsa dsa <i><hostname/IP_address></i> <i><filename></i>
	netsave ipsec public-key rsa <i><hostname/IP_address></i> <i><filename></i>
Options	rsa dsa
	When uploading SSH keys from the Secure Terminal Server, 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 Secure Terminal Server to the remote VPN gateway host for that specific tunnel.
	<i><hostname/IP_address></i>
	The IP address or host name for where the SSH key you are uploading from the Secure Terminal Server is going. If you are using a host name, it must be resolved in either the Secure Terminal Server's Host Table or a DNS server.
	<i><filename></i>
	The complete path and file name for the file you are uploading from the Secure Terminal Server (this path should be relative to the default path of your SFTP/TFTP server, which may or may not allow drive letters).

Snetload

Description Loads certificates and keys into the Secure Terminal Server.

User Level Admin

Syntax

```

snetload ssl certificate|private-key <hostname/IP_address>
<filename>

snetload ldap certificate <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), then you need to download the SSL/TLS private key and CA list to make a secure connection.

ldap certificate

If you are using LDAP authentication with TLS, you need to download the certificate of the CA who signed the LDAP certificate to the Secure Terminal Server for authentication to work properly.

ssh-client host

The public key for the host that is being authenticated by the Secure Terminal Servers 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 Secure Terminal Server, 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 Secure Terminal Server for that specific tunnel.

<hostname>|<IP_address>

Enter the host or IP address that contains the certificate/key you are downloading to the Secure Terminal Server. If you are using a host name, If you are using a host name, it must be resolved in either the Secure Terminal Server's **Host Table** or a DNS server.

<filename>

Enter the complete path and file name of the certificate/key you are downloading to the Secure Terminal Server.

sntp-keys

Enter the complete path and file name of the sntp file that you are downloading to the Terminal Server.

Snetsave

Description Uploads certificates and keys from the Secure Terminal Server to a remote host using SFTP.

User Level Admin

Syntax **snetsave ssh-server public-key ssh-2 rsa|dsa**
 <hostname/IP_address> <filename>

snetsave ipsec public-key rsa <hostname/IP_address> <filename>

Options **rsa|dsa**

When uploading SSH keys from the Secure Terminal Server, 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 Secure Terminal Server 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 Secure Terminal Server is going. If you are using a host name, it must be resolved in either the Secure Terminal Server's **Host Table** or a DNS server.

<filename>

The complete path and file name for the file you are uploading from the Secure Terminal Server (this path should be relative to the default path of your SFTP/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 Secure Terminal Server. You can also retrieve the MOTD from a local file. To do this, do not specify the host parameter.

User Level Normal, Admin

Syntax	<pre>set motd [display on off] [host <hostname> <*>] [file <path_filename>] [sftp on off] set motd file <local_file></pre>
Options	<p>display</p> <p>When enabled, displays the Message of the Day to users who are logging into WebManager or EasyPort Web. The default is off.</p> <p>host</p> <p>The host that the Secure Terminal Server will be getting the Message of the Day file from.</p> <p><*></p> <p>Select * to use a preconfigured HTTP tunnel.</p> <p><path_name></p> <p>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 Secure Terminal Server.</p> <p><sftp></p> <p>If this parameter is set to on, the Terminal Server will use SFTP to retrieve the motd. The sftp specify 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.</p> <p><local_file></p> <p>This is the name of a file on the Secure Terminal Server. The contents of this file will be used for the MOTD.</p>

Show MOTD

Description	Show the Message of the Day (MOTD) settings.
User Level	Admin
Syntax	<code>show motd</code>

Delete Files

ipsec_key

Description	Deletes ipsec tunnel name or * for all.
User Level	Admin
Syntax	<code>delete file [ipsec_key <tunnel-name> <*>]</code>

ntp_key

Description	Delete ntp key.
User Level	Admin
Syntax	<code>delete file ntp_key</code>

ssh_host

Description	Deletes ssh host certificate for host, _default or * for all.
User Level	Admin
Syntax	<code>delete file ssh_host [host <hostname> <_default> <*>]</code>

ssh_user

Description Delete ssh users or * for all.
User Level Admin
Syntax `delete file ssh_users <username> | *`

ssl_ca

Description Delete ssl_ca
User Level Admin
Syntax `delete file ssl_ca`

ssl_certificate

Description Deletes ssl_certificate.
User Level Admin
Syntax `delete file ssl_certificate`

ssl_key

Description Delete ssl_key.
User Level Admin
Syntax `delete file ssl_key`

8

Statistics Commands

This chapter defines all the CLI commands associated with configuring the statistics parameters for the Secure Terminal Server.

Configuration Statistics

Show Netstat

Description Shows currently used TCP/UDP sockets/ports.
User Level Admin
Syntax `show netstat [all] [listening] [tcp] [udp] [tcpv6] [udpv6]`
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 Secure Terminal Server'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`



© Copyright 2016. Black Box Corporation. All rights reserved.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746