LANTRONIX



EDS3000 Device Server Command Reference EDS3008/16/32PR EDS3008/16PS

Part Number PMD-00014
Revision D November 2026

Intellectual Property

© 2021-2026 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

Patented: http://patents.lantronix.com; additional patents pending.

Windows is a registered trademark of Microsoft Corporation. *Wi-Fi* is registered trademark of Wi-Fi Alliance Corporation. All other trademarks and trade names are the property of their respective holders.

Warranty

For details on the Lantronix warranty policy, please go to our web site at www.lantronix.com/support/warranty.

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support Online: www.lantronix.com/support

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided “AS IS.” **Lantronix undertakes no obligation to update the information in this publication.** Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. **The information and specifications contained in this document are subject to change without notice.**

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), and the Python Software Foundation (PSF) License Agreement for Python 2.7.6 (Python License). Lantronix grants you no right to receive source code to the Open Source software. The BSD license is available at http://opensource.org/licenses. The GNU General Public License is available at http://www.gnu.org/licenses/. The Python License is available at https://www.python.org/download/releases/2.7/license/.Your use of each Open Source component or software is subject to the terms of the applicable license.

wpa_supplicant: http://w1.fi/cgit/hostap/plain/wpa_supplicant/README

Openssl : http://openssl.org/source/license.html

Busybox: http://busybox.net/license.html

Dropbear: https://raw.githubusercontent.com/mkj/dropbear/master/LICENSE

VSFTPD: https://security.appspot.com/vsftpd.html#about

Bootstrap: https://github.com/twbs/bootstrap/blob/master/LICENSE

Python: https://www.python.org/download/releases/2.7/license/

Linux kernel version 3.6.5. https://www.kernel.org/pub/linux/kernel/COPYING

OPEN SOURCE SOFTWARE IS DISTRIBUTED WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSE AGREEMENT FOR ADDITIONAL INFORMATION.

Revision History

Date	Rev.	Comments
August 2020	A	Initial document.
February 2021	B	Updated document to firmware revision 2.0.0.0R7.
May 2023	C	Updated to firmware version 2.2.0.0R2: ◆ Added Audit Log enable and disable option to ConsoleFlow client ◆ Added IP Address Filter support. ◆ Added 1000Mbps option to Wired Network (eth0) Link Configuration. ◆ Updated SNMP configuration settings
November 2026	D	Updated to firmware version 3.2.0.0 ◆ Renamed consoleflow to percepxion ◆ Added auth type <uri> basic ◆ Added clrscrn (under root level commands)

About This Guide 7

Chapter Summaries 7
Conventions 7
Additional Documentation 8

Overview 9

XML Architecture and Control 9
Command Line Interface 9
Web API 9

Command Line Interface 10

Configuration Using Telnet 10
Configuration Using the Serial Lines 10
Navigating the CLI Hierarchy 11
Using Keyboard Shortcuts and CLI 11
Understanding the CLI Level Hierarchy 12

Configuration Using XML 15

XML Configuration Record Document Type Definition 15
Quick Tour of XML Syntax 16
Record, Group, Item, and Value Tags 17
Importing and Exporting an XML Configuration File 18
Best Practices 19
XML Configuration Groups 20
XML Status Record Groups and Items 30

Configuration Using Web API 41

Overview 41
Device Actions API 41
File System Web API 46

Commands and Levels 49

List of Figures

Figure 3-1 CLI Level Hierarchy 13
Figure 3-2 Login Level Commands 14
Figure 3-3 Enable Level Commands 14
Figure 4-4 DTD for XCRs 15
Figure 4-5 XML Example 16
Figure 4-6 XML Example 17
Figure 4-7 XML Example of Multiple Named Values 17
Figure 4-8 XML Example of Multiple Items 18
Figure 4-9 XML Example with Multiple Groups 18

List of Tables

Table 3-1 Keyboard Shortcuts _____ 12
Table 4-2 XCR Groups _____ 20
Table 4-3 XSR Group and Items _____ 30

1: About This Guide

This document describes how to configure the Lantronix® EDS3000 device server using the Command Line Interface (CLI) and/or Extensible Markup Language (XML). CLI provides an interactive mode for accessing the configuration and management interface. It is most suited for system and network administrators comfortable with using similar interfaces on enterprise IT and networking products. It is also helpful as a quick tool for access via the product's serial ports or console/management ports. XML provides an extensible mode for software developers interfacing with the EDS and system integrators performing batch provisioning/updates.

Chapter Summaries

This table lists and summarizes the content of each chapter.

Chapter	Summary
2: Overview	Gives an overview of CLI and XML.
3: Command Line Interface	Lists commands and describes how to use CLI to configure the EDS3000PR device server.
4: Configuration Using XML	Lists XML Configuration Record (XCR) groups and items and describes how to use XCRs to configure the EDS3000 device server.
5: Configuration Using Web API	Lists Web API actions that can be used to export and import configuration, export status, take a status action, and manipulate the file system.
6: Commands and Levels	Provides an index of the CLI command hierarchy with hyperlinks to the corresponding command details.

Conventions

The table below lists and describes the conventions used in this book.

Convention	Description
Bold text	Default parameters
Italic text	Required values for parameters.
Square Brackets [ ]	Optional parameters.
Angle Brackets < >	Possible values for parameters.
Pipe |	Choice of parameters.
Warning	***Warning:*** ***Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.***
Note	***Note:*** *Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.*
Caution	***Caution:*** ***Means you might do something that could result in faulty equipment operation or loss of data.***
Screen Font	CLI terminal sessions and examples of CLI input are depicted in `courier new font`.

Additional Documentation

Visit the Lantronix website at www.Lantronix.com/support/documentation for all latest Lantronix documentation which includes the latest versions of the EDS3000PR\EDS3000PS device server-related documentation listed below.

Document	Description
EDS3000 Device Server User Guide	Describes how to configure and use the EDS3000 Device Server.
Lantronix Provisioning Manager Online Help	Instructions for using the Lantronix Provisioning Manager application that discovers, configures, upgrades, and manages Lantronix devices.

2: Overview

The EDS3000 device server supports several convenient configuration methods: Web Manager, CLI, and XML. For more information about Web Manager, see the *EDS3000 Device Server User Guide* available at www.Lantronix.com/support/documentation.

XML Architecture and Control

XML is a fundamental building block for Machine-to-Machine (M2M) and Internet of Things (IoT) networks. The EDS3000 device server supports XML configuration records that make configuring the EDS3000 unit easy for users and administrators. XML configuration records are easy to edit with a standard text editor or an XML editor.

For a brief overview of XML, refer to *4: Configuration Using XML*. It provides guidelines for basic XML syntax, the specific XML tags used, and XML configuration records.

Command Line Interface

Making the edge-to-enterprise vision a reality, the EDS3000 device server uses industry-standard tools for configuration, communication, and control. For example, the EDS3000 device server uses a command line interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

For details of the CLI, refer to *6: Commands and Levels*. It provides an index of the CLI Command Hierarchy with links to the corresponding command details. The CLI provides commands for configuring, monitoring, and controlling the EDS3000 device server.

Web API

The Web APIs are restful APIs that allow access to a subset of device server functions through a standard HTTP request. They can be used to export and import configuration, export status, take a status action, and manipulate the file system.

For Web API details and a list of actions, refer to *5: Configuration Using Web API*.

3: Command Line Interface

This chapter describes accessing the EDS3000 device server by using Telnet, SSH, or serial ports to configure the EDS3000, navigating the CLI, typing keyboard shortcuts, and moving between the levels.

It contains the following sections:

- *Configuration Using Telnet*
- *Configuration Using the Serial Lines*
- *Navigating the CLI Hierarchy*
- *Using Keyboard Shortcuts and CLI*
- *Understanding the CLI Level Hierarchy*

Refer to *Chapter 6: Commands and Levels* for a complete list of levels, commands, and descriptions.

Configuration Using Telnet

To access and configure the EDS3000 device server by using a Telnet session over the network, you must first establish a Telnet connection.

To access the EDS3000 by using Telnet, perform the following steps.

1. Using a terminal application such as Tera Term, connect to the EDS3000 device server's IP address.
2. The EDS3000 device server is online when the command prompt (>) displays. You are at the root level of the CLI.

Note: *Depending on the level of security, a password may be required.*

Configuration Using the Serial Lines

Serial Command Mode

The serial port can be configured to operate in command mode permanently or to be triggered under specified conditions. See the line <line> Level command description for more information.

Serial Recovery

Serial Recovery mode will temporarily override line settings for the serial line to allow configuration changes to be made. Line settings will be restored once the user exits the Serial Recovery mode CLI.

To configure the EDS3000PR or EDS3000PS device server locally using a serial port:

1. Connect a terminal or a PC running a terminal emulation program to one of the EDS's serial ports.

2. Configure the terminal to the following settings:
   - 9600 baud
   - 8-bit
   - No parity
   - 1 stop bit
   - No flow control.
3. Power off the EDS3000.
4. Press and hold down the exclamation point (`!`) key.
5. Power on the EDS3000. After about 10 seconds, the exclamation point will display on the terminal or PC screen.
6. Type `xyz` within 5 seconds to display the CLI prompt.

Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each level has a group of commands for a specific purpose. For example, to configure a setting for the FTP server, one would navigate to the FTP level, which is under the configuration level.

- To move to a different level—Enter the name of the level from within its parent level. For example, to enter the line level, type `line <number>` at the enable prompt. This displays: `<enable> line <number>#`.
- To exit and return to one level higher—Type `exit` and press the **Enter** key. Typing `exit` at the login level or the enable level will close the CLI session.
- To view the current configuration at any level—Type `show`.
- To view the list of commands available at the current level—Type the question mark "`?`". Items within `< >` (e.g. `<string>`) are required parameters.
- To view the available commands and explanations—Type the asterisk (`*`).
- To view the list of commands available for a partial command—Type the partial command followed by the question mark "`?`". For example: `<line 1>#show?` displays a list of all show commands at the line level.
- To view available commands and their explanations for a partial command—Type the partial command followed by the asterisk (`*`). For example: `<line 1>#show*` displays a list of all show commands and descriptions at the line level.
- To view the last 20 commands entered at the CLI—Type `show history`.

Using Keyboard Shortcuts and CLI

One useful shortcut built into the EDS3000 is that the complete text of a command does not have to be entered to issue a command. Typing just enough characters to uniquely identify a command, then hitting enter, can be used as a short cut for a command. For example, at the enable level, "`sh`" can be used for the "`show`" command.

Tab Completion is also available using the **Tab** and **Enter** keys on the keyboard. Typing the first few characters of a command, then hitting the **Tab** key displays the first command that begins with those characters. Hitting the **Tab** key again displays the next command that begins with the original characters typed. You can press **Enter** to execute the command or you can backspace to edit any parameters.

The following key combinations are allowed when configuring the EDS using the CLI:

Table 3-1 Keyboard Shortcuts

Key Combination	Description
Ctrl + a	Places cursor at the beginning of a line
Ctrl + b	Backspaces one character
Ctrl + d	Deletes one character
Ctrl + e	Places cursor at the end of the line
Ctrl + f	Moves cursor forward one character
Ctrl + k	Deletes from the current position to the end of the line
Ctrl + l	Redraws the command line
Ctrl + n	Displays the next line in the history
Ctrl + p	Displays the previous line in the history
Ctrl + u	Deletes entire line and places cursor at start of prompt
Ctrl + w	Deletes one word back
Ctrl + z	Exits the current CLI level
Esc + b	Moves cursor back one word
Esc + f	Moves cursor forward one word

Understanding the CLI Level Hierarchy

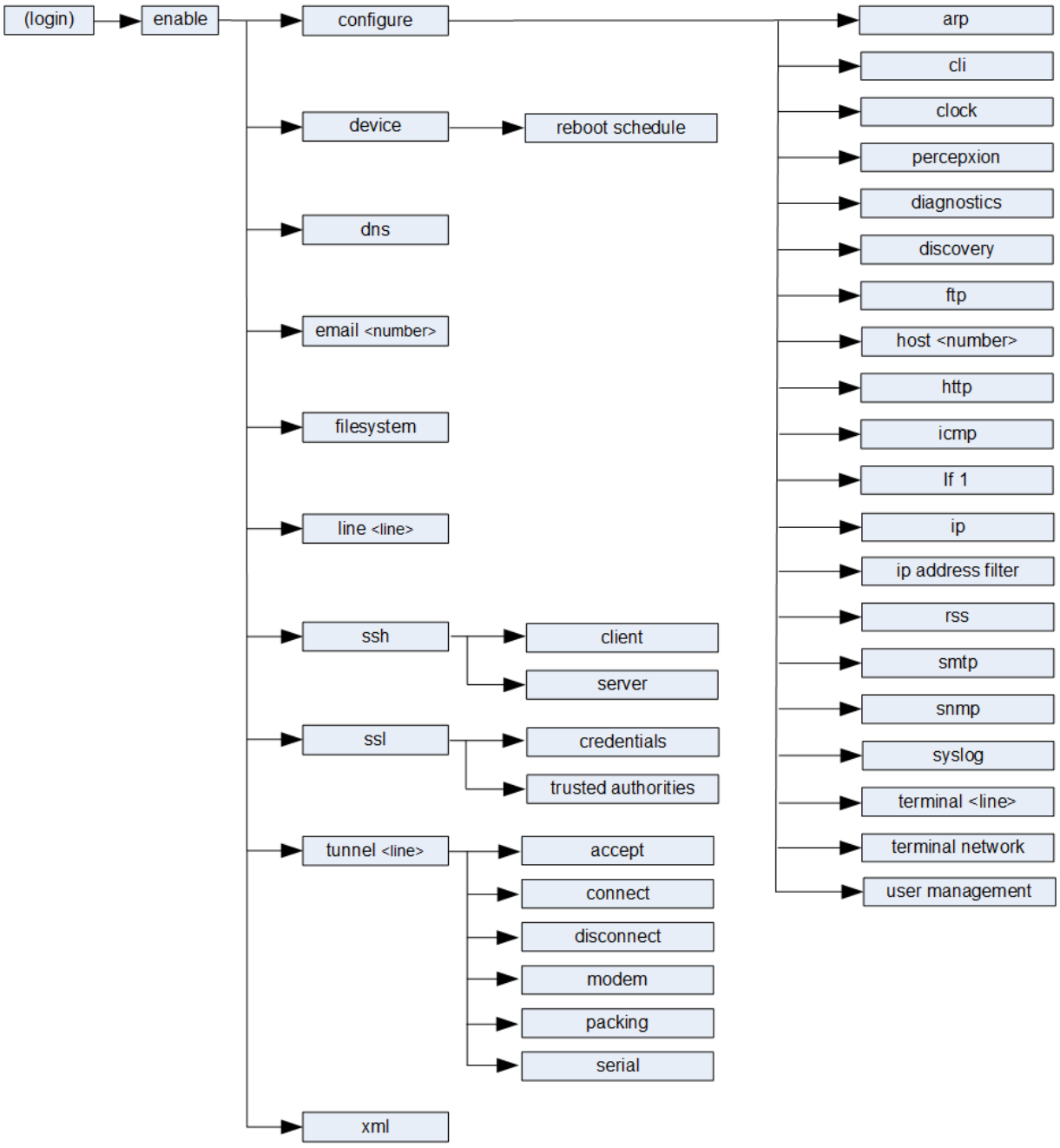
The CLI hierarchy is a series of levels. Arranging commands in a hierarchy of levels provides a way to organize and group similar commands, provide different levels of security, and reduce the complexity and number commands and options presented to a user at one time.

When you start a command line session, you begin at the login level. This level can be password protected and provides access to high level status, a few diagnostic commands, and the enable level. Further EDS information and configuration are accessed via the enable level.

The enable level can also be password protected and is the gateway to full configuration and management of the EDS. There are commands for gathering and effecting all elements of EDS status and configuration, as well as commands that take you to additional levels. For instance, network specific status and configuration commands are found under the “configuration” level.

An overview of the levels in the EDS3000 is presented in *Figure 3-1 CLI Level Hierarchy*.

Figure 3-1 CLI Level Hierarchy



Commands at the login level (see *Figure 3-2 Login Level Commands* below) do not affect current configuration settings and are not displayed initially. If you type?, you will see the login subcommands. These commands provide diagnostic and status information only.

Figure 3-2 Login Level Commands

```
admin@EDS3032PR-0080a38aa011>?
clrscrn                                 exit
iperf <params>                          ping <host>
ping <host> <count>                     ping <host> <count> <timeout>
show                                    show history
show lines                              show multicast routes
show routes                             show rules
tcpdump <parameters>                    trace route <host>
trace route <host> <protocol>           enable

admin@EDS3032PR-0080a38aa011>
```

Note: *To configure the EDS3000 device server, you must be in the enable level and any of its sub-levels. Figure 3-3 Enable Level Commands below shows the enable level commands.*

Figure 3-3 Enable Level Commands

```
admin@EDS3032PR-0080a38aa011(enable)#
admin@EDS3032PR-0080a38aa011(enable)#?
auto show interfaces                    auto show processes
clrscrn                                 configure
connect                                 connect line <line>
device                                  disable
dns                                     email <number>
exit                                    filesystem
iperf <params>                          kill ssh <session>
kill telnet <session>                   line <line>
ping <host>                             ping <host> <count>
ping <host> <count> <timeout>           reload
reload factory defaults                 show
show history                            show interfaces
show ip sockets                         show lines
show multicast routes                   show processes
show routes                             show rules
show sessions                           ssh
ssh <optClientUsername> <host>          ssh <optClientUsername> <host> <port>
ssl                                     tcpdump <parameters>
telnet <host>                           telnet <host> <port>
trace route <host>                      trace route <host> <protocol>
tunnel <line>                           write
xml

admin@EDS3032PR-0080a38aa011(enable)#
admin@EDS3032PR-0080a38aa011(enable)#
```

Refer to the *Chapter 6: Commands and Levels* at the end of this document for a complete list of levels, commands, and descriptions.

4: Configuration Using XML

The EDS3000 device server provides an XML interface that you can use to configure EDS3000 device servers. Every configuration setting that can be issued from the EDS's Web Manager interface and CLI can be specified using XML.

The EDS3000 device server can import and export configuration settings as an XML document known as an XML Configuration Record (XCR). An XCR can be imported or exported via the CLI, a Web browser, or FTP. An XCR can contain many configuration settings or just a few. For example, it might change all of the configurable parameters for an EDS3000 device server, or it may only change the baud rate for a single serial line. Using XCRs is a straightforward and flexible way to manage the configuration of multiple EDS3000 device servers.

XML Configuration Record Document Type Definition

An XML document type definition (DTD) is a description of the structure and content of an XML document. It verifies that a document is valid. XCRs are exported using the DTD as shown in *Figure 4-4 DTD for XCRs*.

Figure 4-4 DTD for XCRs

```
<!DOCTYPE configrecord [
<!ELEMENT configrecord (configgroup+)>
<!ELEMENT configgroup (configitem+,configgroup*)>
<!ELEMENT configitem (value+)>
<!ELEMENT value (#PCDATA)>
<!ATTLIST configrecord version CDATA #IMPLIED>
<!ATTLIST configgroup name CDATA #IMPLIED>
<!ATTLIST configgroup instance CDATA #IMPLIED>
<!ATTLIST configitem name CDATA #IMPLIED>
<!ATTLIST configitem instance CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
]>
```

The EDS3000 DTD rules state the following:

- The XML document element is a `<configrecord>` element. This is the root element.
- A `<configrecord>` must have one or more `<configgroup>` elements and can have a version attribute.
- A `<configgroup>` must have one or more `<configitem>` elements and can have name and instance attributes.
- A `<configitem>` element must have one or more `<value>` elements and can have a name attribute.
- A `<value>` element can have only data and can have a name attribute.
- The name attribute identifies a group, item, or value. It is always a quoted string.
- The instance attribute identifies the specific option, like the serial port number. The "instance" attribute is always a quoted string.

Notes:

- *The name for each* `<configgroup>` *(specified with the name attribute) is the group name listed in the Web Manager XCR groups or with the "xcr list" CLI command. See the EDS3000 Device Server User Guide (available at www.Lantronix.com/support/documentation) for more information about the XCR groups.*
- *An empty or missing* `<value>` *element in each present* `<configgroup>` *clears the setting to its default.*

Quick Tour of XML Syntax

Declaration

The first line, `<?xml version="1.0" standalone="yes"?>`, is called the XML declaration. It is required and indicates the XML version in use (normally version 1.0). The remainder of the file consists of nested XML elements, some of which have attributes and content.

Element Start and End Tags

An element typically consists of two tags: start tag and an end tag that surrounds text and other elements (element content). The start tag consists of a name surrounded by angle brackets, for example `<configrecord>`. The end tag consists of the same name surrounded by angle brackets, but with a forward slash preceding the name, for example `</configrecord>`. The element content can also contain other "child" elements.

Element Attributes

The XML element attributes that are name-value pairs included in the start tag after the element name. The values must always be quoted, using single or double quotes. Each attribute name should appear only once in an element.

Figure 4-5 XML Example shows an XML example which consists of a declaration (first line), nested elements with attributes and content.

Figure 4-5 XML Example

```
<configrecord version="0.1.0.0T0">
   <configgroup name = "diagnostics">
      <configitem name = "log">
         <value name="output">Disable</value>
      </configitem>
   </configgroup>
</configrecord>
```

The EDS3000 device server uses the attributes in the following subsections to label the group configuration settings.

Record, Group, Item, and Value Tags

A <configgroup> is a logical grouping of configuration parameters and must contain one or more <configitem> elements. It must have a name attribute and may have an instance attribute.

A <configitem> is a specific grouping of configuration parameters relevant to its parent group. An item takes the name attribute and must contain one or more value elements. For example, the line group might have parameters such as baud rate, data bits, and parity.

A value may specify the value of a configuration parameter. It may contain the name attribute. In this example, a value of 9600 might be specified for baud rate; 7 may be specified for data bits, and even may be specified for parity.

A name attribute identifies the group, item, or value. It is always quoted (as are all XML attributes). For example, a group that contains serial port parameters has the name "line".

An instance attribute identifies which of several instances is being addressed. It is always quoted. For example, the serial port name (in the line configgroup) has the instance "1" to indicate serial port 1 or "2" to specify serial port 2..

The following figures show examples of XML configuration records and the use of the <configrecord>, <configgroup>, <configitem>, and <value> XML elements.

Figure 4-6 XML Example

```
<configrecord version=”0.1.0.0T0”>
   <configgroup name = “diagnostics”>
      <configitem name = “log”>
         <value name=”output”>Disable</value>
      </configitem>
   </configgroup>
</configrecord>
```

Figure 4-7 XML Example of Multiple Named Values

```
<configrecord version="0.1.0.0T0">
   <configgroup name=“xml import control">
      <configitem name=“restore factory configuration">
         <value>disable</value>
      </configitem>
      <configitem name=“delete http authentication uris">
         <value>disable</value>
      </configitem>
      <configitem name=“http authentication uri delete">
         <value name=“name"/>
      </configitem>
      <configitem name=“reboot">
            <value>disable</value>
      </configitem>
   </configgroup>
```

Figure 4-8 XML Example of Multiple Items

```
<configrecord version="0.1.0.0T0">
   <configgroup name="device">
      <configitem name="short name">
         <value>EDS3032PR</value>
      </configitem>
      <configitem name="long name">
         <value>Lantronix EDS3032PR</value>
      </configitem>
      <configitem name="serial number">
         <value>0080A3D92B9B</value>
      </configitem>
      </configitem><configitem name="firmware version">
         <value>1.0.0.0R8</value>
      </configitem>
   </configgroup>
```

Figure 4-9 XML Example with Multiple Groups

```
<configrecord version="0.1.0.0T0">
   <configgroup name="diagnostics">
      <configitem name="log">
         <value name="output">Disable</value>
      </configitem>
   </configgroup>
   <configgroup name="discovery">
      <configitem name="state">
         <value>enable</value>
      </configitem>
   </configgroup>
   <configgroup name="ethernet" instance="eth0">
      <configitem name="speed">
         <value>Auto</value>
      </configitem>
      <configitem name="duplex">
         <value>Auto</value>
      </configitem>
   </configgroup>
   <configgroup name="ftp server">
      <configitem name="state">
         <value>enable</value>
      </configitem>
   </configgroup>
```

Importing and Exporting an XML Configuration File

An XCR can be imported or exported using the following methods:

- **CLI**
  XCRs can be imported (captured) or exported (dumped) directly to a Telnet, SSH, or serial line

CLI session. Capturing an XCR can be started by pasting a valid XCR directly into the CLI prompt. The EDS3000 device server immediately processes the configuration record, changing any settings specified. This can be done on any level, including the root. Special tags in the XML allow for providing root and enable level passwords so that this can also be done at the password prompt.

- **Web Browser**
  Web Manager can be used to import and export an XCR from an external source such as your local hard drive.
- **FTP**
  The EDS3000 device server FTP server can export and import XCRs when an FTP get or put command on the filename (`EDS3000PR.xcr` for export, `EDS3000PR_import.xcr` for import; both are under the **pwxcr** directory) is requested. On export (FTP get of `EDS000PR.xcr`), the FTP server obtains the current XCR from the EDS3000 device server and sends it as a file. On import (FTP put of `EDS3000PR_import.xcr`), the FTP server processes the file by sending it directly to the XML engine. In both cases the EDS3000 file system is not accessed. The files `EDS3000PR.xcr` and `EDS3000PR_import.xcr` are not read from or written to the file system. See the FTP section in the *EDS3000 Device Server User Guide* (available at www.Lantronix.com/support/documentation.)

Best Practices

You can import or export an entire XCR, or just a portion of it, by specifying the group name and/or group instances. In the examples below, import and export operations are performed from the Web. See *Importing and Exporting an XML Configuration File* above to import and export using Web Manager, the CLI or FTP.

Caution: ***Using Microsoft Word to edit and save an XCR will change the format of the file and make it incompatible with the EDS3000PR device server. This is true even if the file is saved as Plain Text (.txt) or an XML Document (.xml). Notepad, a third party text editor, or a specialized XML editor should be used instead.***

Exporting

Using the Web Manager interface, select from “Lines to Export” and “Groups to Export” filters and select from either “Export to Browser” or “Download (from link)” option. Save the output to your local file system.

Importing

Modify the exported file by removing “configgroup” records and filling in any required secret data such as passwords, and private keys. Using the Web Manager, import the updated clone by uploading it from your local file system.

XML Configuration Groups

Table 4-2 lists the supported EDS3000 XML configuration record (XCR) groups, items, and possible value names and options in alphabetical order.

Note: *Any instance of* `&#60` *in the table may be read as "less than" and any instance of* `&#62` *may be read as "greater than".*

Table 4-2 XCR Groups

Group Name	Group Item	Value Name	Value Options	Additional Info
arp	arp delete	ip address		
	arp entry	ip address		
		mac address		
cli	enable level password			
	quit connect line		<control&#62	
	inactivity timeout		15 minutes	
	line authentication		disable	
clock time and zone	time zone	zone	GMT	
		offset		
	time set	hours		
		minutes		
		seconds		
		day of month		
		month		
		year		
clock	synchronization method	manual, SNTP		
	ntp	server (0.pool.ntp.org)		
percepxion	state		enable	
	device id			
	device key		configured and ignored	
	device name			
	device description			
	status update interval		1 minutes	
	content check interval		24 hours	
	local port		<Random&#62	

Group Name	Group Item	Value Name	Value Options	Additional Info
percepxion line Attribute of an instance is a number.)	state		disable	
	project tag			
	command delimeter		+++	
	status update interval		1 minutes	
	content check interval		24 hours	
	local port		<control&#62	
device	short name			
	long name			
	serial number			
	firmware version		2.2.0.0R2	
	configuration version			
diagnostics	log	output		
		max length		
discovery	state		enable	
email (Attribute of an instance is a number.)	to			
	cc			
	reply to			
	subject			
	message file			
	priority			
ethernet (“Instance” attribute is “eth0”)	speed			
	duplex			
firmware		version	2.2.0.0R2	
ftp server	state		enable	
	port		21	
	data port		20	
	passive mode start port		<Random>	
	passive mode ports		<Random>	
host (Attribute of an instance is a number.)	name			
	protocol		Telnet	
	ssh user name			
	remote address			
	remote port		0	

Group Name	Group Item	Value Name	Value Options	Additional Info
http authentication uri	user delete	name		
	realm	config		
	type	digest		
	user (Attribute of an instance is “admin”.)	password		
http server	state		enable	
	port		80	
	https state		enable	
	secure port		443	
	secure protocols		TLS1.0, TLS1.1, TLS1.2, TLS1.3	
	secure credentials			
	max timeout		10 seconds	
	max bytes		40960	
	logging state		enable	
	max log entries		50	
	log format			
	authentication timeout		30 minutes	
icmp	state		enable	
interface (“Instance” attribute is “eth0”)	dhcp		enable	
	ip address		<None>	
	default gateway		<None>	
	hostname			
	domain			
	dhcp client id			
	primary dns		<None>	
	secondary dns		<None>	
	mtu		1500 bytes	
ip	ip time to live		64 hops	
	multicast time to live		1 hops	

Group Name	Group Item	Value Name	Value Options	Additional Info
line (Attribute of an instance is a number or “console”.)	name			
	state		enable	
	protocol			
	baud rate		9600 bits per second	
	parity			
	data bits		8	
	stop bits		1	
	flow control			
	xon char		<None>	
	xoff char		<None>	
	gap timer		<None>	
	threshold		56 bytes	
reboot schedule	state		disable	
	schedule			
	hours			
	minutes			
	interval			
	unit			
rss	feed		disable	
	persist		disable	
	max entries		100 value	
serial command mode (Attribute of an instance is a number or “console”.)	mode		always	
	echo serial string		enable	
	serial string			
	signon message			
	wait time		5000	
smtp	from address			
	server address			
	server port			
	username			
	password			
	overriding domain			
	local port		<None>	

Group Name	Group Item	Value Name	Value Options	Additional Info
snmp	snmpd	state		
		port		
		version		
		read community		
		write community		
		username		
		security		
		authentication protocol		
		authentication password		
		privacy protocol		
		privacy password		
		read-only username		
		read-only security	Authentication but No Privacy, Authentication and Privacy, No Authentication and No Privacy	
		read-only authentication protocol	MD5, SHA	
		read-only authentication password		
		read-only privacy protocol	DES, AES	
		read-only privacy password		
		system contact		
		system name		
		system description		
	system location			

Group Name	Group Item	Value Name	Value Options	Additional Info
snmp (continued)	traps	community		
		primary destination port		
		primary destination		
		secondary destination		
		secondary destination port		
		version		
		username		
		security		
		authentication protocol		
		authentication password		
		privacy protocol		
		privacy password		
ssh client	delete known hosts		enable, disable	
	known host delete	name		
	known host	public rsa key		
		public dsa key		
	delete client users		disable	
	client user delete	name		
	client user	password		
		remote command		
		public rsa key		
		private rsa key		
		public dsa key		
		private dsa key		
ssh server	host rsa keys	public key		
		private key		
	host dsa keys	public key		
		private key		
	delete authorized users		disable	
	authorized user delete	name		
	authorized user	password		
		public rsa key		
		public dsa key		

Group Name	Group Item	Value Name	Value Options	Additional Info
ssh	state		enable	
	port		22	
	max sessions		3	
ssl	credentials	rsa certificate		
		rsa certificate type		
		rsa pfx password		
		rsa private key		
		rsa private key type		
		rsa private key pfx password		
		dsa certificate		
		dsa certificate type		
		dsa pfx password		
		dsa private key		
		dsa private key type		
		dsa private key pfx password		
		ecdsa certificate		
		ecdsa certificate type		
		ecdsa pfx password		
		ecdsa private key		
		ecdsa private key type		
		ecdsa private key pfx password		
		credential type		
	trusted authority	certificate		
		certificate type		
		pfx password		
	intermediate authority	certificate		
		certificate type		
		pfx password		
	delete all credentials		disable	
	delete credential	name		
	delete all cas		disable	

Group Name	Group Item	Value Name	Value Options	Additional Info
syslog	state		disable	
	host			
	remote port			
	local port		<None>	
	severity log level			
telnet	state		enable	
	port			
	max sessions		3	
	authentication		enable	
terminal (“Instance” attribute is a number or “network”)	terminal type			
	login connect menu		disable	
	exit connect menu		disable	
	send break		<None>	
	break duration			
	echo		enable	
tunnel accept (Attribute of an instance is a number.)	accept mode			
	local port			
	protocol			
	secure credentials		TLS1.1, TLS1.2, TLS1.3	
	credentials			
	tcp keep alive			
	tcp keep alive interval			
	tcp keep alive probes			
	aes encrypt key			
	aes decrypt key			
	initial send			
	start character		<None>	
	flush start character		enable, disable	
	flush serial		enable, disable	
	block serial		enable, disable	
	block network		enable, disable	
	password	password		
		prompt		
	email connect		<None>	
	email disconnect		<None>	

Group Name	Group Item	Value Name	Value Options	Additional Info
tunnel connect (Attribute of an instance is a number.)	connect mode		enable, disable	
	start character		<control>B	
	flush start character		enable, disable	
	local port		<Random>	
	host (Attribute of an instance is a number.)	address		
		port		
		protocol		
		ssh username		
		secure protocols	TLS1.1, TLS1.2, TLS1.3	
		credentials		
		validate certificate		
		tcp user timeout		
		tcp keep alive		
		tcp keep alive interval		
		tcp keep alive probes		
		aes encrypt key		
		aes decrypt key		
		initial send		
	host mode			
	reconnect time			
	flush serial			
	block serial			
	block network			
	email connect			
	email disconnect			
tunnel disconnect (Attribute of an instance is a number.)	stop character		<None>	
	flush stop character		enable	
	modem control		disable	
	timeout			
	flush serial		disable	

Group Name	Group Item	Value Name	Value Options	Additional Info
tunnel modem (Attribute of an instance is a number.)	echo pluses		disable	
	echo commands		enable	
	verbose response		enable	
	response type			
	error unknown commands		disabled	
	incoming connection			
	connect string			
	display remote ip		enable, disable	
tunnel packing (Attribute of an instance is a number.)	packing mode		disable	
	timeout			
	threshold			
	send character		<Control>	
	trailing character		<None>	
tunnel serial (Attribute of an instance is a number.)	dtr		<None>	
user management	admin username			
	admin password			
	users (Attribute of an instance is a number)	username		
		password		
		role		
	roles (Attribute of an instance is a number)	name		
		write		
		execute		
xml import control	restore factory configuration		disable	
	delete http authentication uris		disable	
	http authentication uri delete	name		
	missing values		set to default, unchanged	
	reboot		disable	

XML Status Record Groups and Items

Table 4-3 lists the supported XML status record (XSR) groups and items. These groups and items show the status of the EDS in XML form and can only be exported. The XSR schema differs slightly from the XCR groups and items in that the XSR allows groups within groups.

Table 4-3 XSR Group and Items

Group Name	Item Name	Value Name	Valid Values
arp	arp entry	ip address	
		mac address	
		type	
		interface	
clock	time		
	date		
	timezone	zone	
		offset	
device	product info	product type	
		secure boot	enabled, disabled
		serial number	
		firmware version	
		firmware version on inactive bank	
		current bank	
		last firmware update	
		configuration version	
		build date year	
		build date month	
		build date day	
		build date hour	
		build date minute	
		build date second	
		uptime	
		permanent config	
email log (Attribute of an instance is a number.)	entry	time	
		log	
email (Attribute of an instance is a number.)	success	sent	
		sent with retries	
	failed		
	queued		

Group Name	Item Name	Value Name	Valid Values
hardware	cpu	type	
		speed	
	memory	flash size	
		ram size	
	connections	number serial	
		number usb	
		number ethernet	
		number wireless	
		number cellular	
http log	totals	entries	
		bytes	
	entry (Attribute of an instance is a number.)		
http	state		enable, disable
	logging	entries	
		bytes	

Group Name	Item Name	Value Name	Valid Values
icmp	snmp	InMsgs	
		InErrors	
		InDestUnreachs	
		InTimeExcds	
		InParmProbs	
		InSrcQuenchs	
		InRedirects	
		InEchos	
		InEchoReps	
		InTimestamps	
		InTimestampReps	
		InAddrMasks	
		InAddrMaskReps	
		OutMsgs	
		OutErrors	
		OutDestUnreachs	
		OutTimeExcds	
		OutParmProbs	
		OutSrcQuenchs	
		OutRedirects	
		OutEchos	
		OutEchoReps	
		OutTimestamps	
		OutTimestampReps	
		OutAddrMasks	
		OutAddrMaskReps	

Group Name	Item Name	Value Name	Valid Values
interface (Attribute of an instance is “eth0”.)	generic	status	
	mac address		
	ip address		
	network mask		
	default gateway		
	ipv4 domain		
	ipv4 address type		
	receive	bytes	
		packets	
		errs	
		drop	
		fifo	
		frame	
		compressed	
		multicast	
	transmit	bytes	
		packets	
		errs	
		drop	
		fifo	
		colls	
		carrier	
		compressed	
ip sockets	ip socket	protocol	
		rx queue	
		tx queue	
		local address	
		local port	
		remote address	
		remote port	
		state	

Group Name	Item Name	Value Name	Valid Values
ip	snmp	Forwarding	
		DefaultTTL	
		InReceives	
		InHdrErrors	
		InAddrErrors	
		ForwDatagrams	
		InUnknownProtos	
		InDiscards	
		InDelivers	
		OutRequests	
		OutDiscards	
		OutNoRoutes	
		ReasmTimeout	
		ReasmReqds	
		ReasmOKs	
		ReasmFails	
		FragOKs	
		FragFails	
		FragCreate	
	netstat	InNoRoutes	
		InTruncatedPkts	
		InMcastPkts	
		OutMcastPkts	
		InBcastPkts	
		OutBcastPkts	
		InOctets	
		OutOctets	
		InMcastOctets	
		OutMcastOctets	
		InBcastOctets	
		OutBcastOctets	

Group Name	Item Name	Value Name	Valid Values
line (Attribute of an instance is a number or “console”.)	receiver	bytes	
		breaks	
		parity errors	
		framing errors	
		overrun errors	
		no receive buffer errors	
		queued bytes	
		flow control	
	transmitter	bytes	
		breaks	
		queued bytes	
		flow control	
	line levels	cts input	
		rts output	
		dsr input	
		dtr output	<control>
line	state		enable, disable
	protocol		
	baud rate		
	parity		
	data bits		
	stop bits		
	flow control		
	xon char		<control>Q
	xoff char		<control>Q
memory	main heap	total memory	
		available memory	
network	dns	primary	
		secondary	
processes	process (Attribute of an instance is a number.)	stack used	
		stack size	
		cpu %	
		thread name	

Group Name	Item Name	Value Name	Valid Values
query port	status		enabled, disabled
	last connection	ip address	
		port	
	in	discoveries	
		unknown queries	
		erroneous packets	
	out	discovery replies	
		errors	
reserved ports	reserved port	port	
		protocol	
		reserved	
rss	url		
	data	entries	
		bytes	
sessions			
tcp	snmp	RtoAlgorithm	
		RtoMin	
		RtoMax	
		MaxConn	
		ActiveOpens	
		PassiveOpens	
		AttemptFails	
		EstabResets	
		CurrEstab	
		InSegs	
		OutSegs	
		RetransSegs	
		InErrs	
		OutRsts	

Group Name	Item Name	Value Name	Valid Values
tcp (continued)	netstat	SyncookiesSent	
		SyncookiesRecv	
		SyncookiesFailed	
		EmbryonicRsts	
		PruneCalled	
		RcvPruned	
		OfoPruned	
		OutOfWindowIcmps	
		LockDroppedIcmps	
		ArpFilter	
		TW	
		TWRecycled	
		TWKilled	
		PAWSPassive	
		PAWSActive	
		PAWSEstab	
		DelayedACKs	
		DelayedACKLocked	
		DelayedACKLost	
		ListenOverflows	
		ListenDrops	
		TCPPrequeued	
		TCPDirectCopyFromBacklog	
		TCPDirectCopyFromPrequeue	
		TCPPrequeueDropped	
		TCPHPHits	
		TCPHPHitsToUser	

Group Name	Item Name	Value Name	Valid Values
tcp (continued)	netstat (continued)	TCPPureAcks	
		TCPHPAcks	
		TCPRenoRecovery	
		TCPSackRecovery	
		TCPSACKReneging	
		TCPFACKReorder	
		TCPSACKReorder	
		TCPRenoReorder	
		TCPTSReorder	
		TCPFullUndo	
		TCPPartialUndo	
		TCPDSACKUndo	
		TCPLossUndo	
		TCPLostRetransmit	
		TCPRenoFailures	
		TCPSackFailures	
		TCPLossFailures	
		TCPFastRetrans	
		TCPForwardRetrans	
		TCPSlowStartRetrans	
		TCPTimeouts	
		TCPRenoRecoveryFail	
		TCPSackRecoveryFail	
		TCPSchedulerFailed	
		TCPRcvCollapsed	
		TCPDSACKOldSent	
		TCPDSACKOfoSent	
		TCPDSACKRecv	
		TCPDSACKOfoRecv	
		TCPAbortOnData	
		TCPAbortOnClose	
		TCPAbortOnMemory	
		TCPAbortOnTimeout	
		TCPAbortOnLinger	
		TCPAbortFailed	
		TCPMemoryPressures	
		TCPSACKDiscard	

Group Name	Item Name	Value Name	Valid Values
tcp (continued)	netstat (continued)	TCPDSACKIgnoredOld	
		TCPDSACKIgnoredNoUndo	
		TCPSpuriousRTOs	
		TCPMD5NotFound	
		TCPMD5Unexpected	
		TCPSackShifted	
		TCPSackMerged	
		TCPSackShiftFallback	
		TCPBacklogDrop	
		TCPMinTTLDrop	
		TCPDeferAcceptDrop	
		IPReversePathFilter	
		TCPTimeWaitOverflow	
		TCPReqQFullDoCookies	
		TCPReqQFullDrop	
		TCPRetransFail	
		TCPRcvCoalesce	
		TCPOFOQueue	
		TCPOFODrop	
		TCPOFOMerge	
		TCPChallengeACK	
		TCPSYNChallenge	
		TCPFastOpenActive	
tunnel modem	echo commands		enable, disable
	verbose response		enable, disable
	response type		
	error unknown commands		enable, disable
	incoming connection		enabled, disabled

Group Name	Item Name	Value Name	Valid Values
tunnel (Attribute of an instance is a number.)	aggregate	completed connects	
		completed accepts	
		disconnects	
		dropped connects	
		dropped accepts	
		octets from device	
		octets from network	
		connect 0 connection time	
		connect 1 connection time	
		connect 2 connection time	
		connect 3 connection time	
		connect 4 connection time	
		connect 5 connection time	
		connect 6 connection time	
		connect 7 connection time	
		connect 8 connection time	
		connect 9 connection time	
		connect 10 connection time	
		connect 11 connection time	
		connect 12 connection time	
		connect 13 connection time	
		connect 14 connection time	
		connect 15 connection time	
		accept connection time	
		connect dns address changes	
		connect dns address invalids	
udp	snmp	InDatagrams	
		NoPorts	
		InErrors	
		OutDatagrams	
		RcvbufErrors	
		SndbufErrors	
xsr	out	bytes	
		lines	
		elements	
	errors		

5: Configuration Using Web API

The Web APIs are restful APIs that allow access to a subset of gateway functions through a standard HTTP request.

Overview

EDS3000 provides the following APIs:

Device Actions API

- Export Status Group - Retrieve device status
- Export Configuration Group - Retrieve device configuration
- Import Configuration Group - Import device configuration
- Take Status Action - Take device status action

File System API

- HTTP GET - Read the contents of files and directories
- HTTP PUT - Create new files and update existing files
- HTTP MKCOL - Create new directories
- HTTP DELETE - Remove files and directories from the file system

Device Actions API

The Device Actions API provide functions to export and import the configuration as well as export status and take a status action.

Export Status Group

An HTTP POST request can be sent to the device to retrieve status information.

- Protocol: HTTP
- Method: POST
- URL: http://<hostname>/export/status

Parameters:

- optionalLine: Optional line index for line oriented XML groups
- optionalGroupList: Optional list of XML groups separated by semicolon. If omitted, all status groups will be returned.
- optionalBoolListOnly: Optional parameter if set to ‘true’ returns supported group list.

CURL example:

```
curl -u admin:PASSWORD http://<ip-address>/export/status -X POST
curl -u admin:PASSWORD http://<ip-address>/export/status -X POST -d
   “optionalGroupList=device”
```

Javascript example:

```
myXmlhttprequest.open(
    "POST",
    "/export/status",
    true
);
request.send(
    "optionalGroupList=device"
);
```

Export Configuration Group

An HTTP POST request can be sent to the device to retrieve configuration information.

- Protocol: HTTP
- Method: POST
- URL: http://<hostname>/export/config

Parameters:

- optionalLine: Optional line index for line oriented XML groups
- optionalGroupList: Optional list of XML groups separated by semicolon. If omitted, all status groups will be returned.
- optionalBoolListOnly: Optional parameter if set to 'true' returns supported group list.

CURL example:

```
curl -u admin:PASSWORD http://<ip-address>/export/config -X POST
curl -u admin:PASSWORD http://<ip-address>/export/config -X POST -d
    "optionalGroupList=Interface:eth0"
```

Javascript example:

```
myXmlhttprequest.open(
    "POST",
    "/export/status",
    true
);
request.send(
    "optionalGroupList=Interface:eth0"
);
```

Import Configuration Group

An HTTP POST request can be sent to the device to set configuration.

- Protocol: HTTP
- Method: POST
- Content-Type: multipart/form-data
- URL: http://<hostname>/import/config

Parameters:

- configrecord: Content of configuration group in XML format.

CURL example (configuration is saved in a local file config.xml):

```
curl -u admin:PASSWORD http://<ip-address>/import/config -X POST --form
   configrecord=@config.xml
```

CURL example (configuration as part of command):

```
curl -u admin:PASSWORD http://<ip-address>/import/config -X POST --form-string
   'configrecord=<?xml version="1.0" standalone="yes"?>
<!-- Automatically generated XML -->
<!DOCTYPE configrecord [
<!ELEMENT configrecord (configgroup+)>
<!ELEMENT configgroup (configitem+)>
<!ELEMENT configitem (value+)>
<!ELEMENT value (#PCDATA)>
<!ATTLIST configrecord version CDATA #IMPLIED>
<!ATTLIST configgroup name CDATA #IMPLIED>
<!ATTLIST configgroup instance CDATA #IMPLIED>
<!ATTLIST configitem name CDATA #IMPLIED>
<!ATTLIST configitem instance CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
]>
<configrecord version = "0.1.0.1">
<configgroup name = "ftp server">
<configitem name = "state">
<value>disable</value>
</configitem>
</configgroup>
</configrecord>'
```

HTTP example:

```
<form method="post" enctype="multipart/form-data" action="/import/config"
   target="_blank">
<input name="configrecord" type="file" size="32">
<input name="submit" type="submit" value="Import Configuration">
</form>
```

Take Status Action

An HTTP POST request can be sent to take a status action.

- Protocol: HTTP
- Method: POST
- URL: http://<hostname>/action/status

Parameters:

- group: Required. The status group where action is defined.
- optionalGroupInstance: Optional instance of status group.
- optionalItem: Optional item of status group where action is defined.
- optionalItemInstance: Optional instance of status item.
- action: Required. The action to be taken.

Actions Definitions

The following are action definitions related to the Take Status Action API.

Note: *When you see "NULL" after optionalGroupInstance, optionalItem, or optionalItemInstance, it means that item or instance should be omitted.*

group "Clock" optionalGroupInstance NULL

optionalItem NULL optionalItemInstance NULL

action "Current Time <value>"

The format for setting time is YYYY-MM-DD hh:mm:ss, where the hours are in 24-hour format. The device supports dates in the range 2007-01-01 00:00:00 to 2039-12-31 23:59:59 UTC.

group "Device" optionalGroupInstance NULL

optionalItem NULL optionalItemInstance NULL

action "Save"

The Save action works like the "write" command. Any cached configuration changes are committed, so they will apply after a reboot.

Without a Save, any cached configuration changes are lost after a reboot.

optionalItem NULL optionalItemInstance NULL

action "Reboot"

The Reboot action shuts the device down and restarts it. Any cached configuration changes (those which have not been saved) are lost.

optionalItem NULL optionalItemInstance NULL

action "Factory Defaults"

The Factory Defaults action restores the device configuration as it came from the factory. Any user changes to configuration are lost.

group "Filesystem" optionalGroupInstance NULL

optionalItem NULL optionalItemInstance NULL

action "Format"

Format clears out the flash file system, preserving only system configuration data. Be careful! All other files are destroyed.

group "Line" optionalGroupInstance Required

optionalItem NULL optionalItemInstance NULL

action "Command <value>"

The Command action sends bytes to the Line and picks up bytes in response. The bytes are hex encoded.

Maximum number of characters to read (n) may be specified; default is unlimited.

Milliseconds total time limit (m) may be specified; default is 1000.

Terminating byte (t) may be specified; default is <None>.

Syntax of <value> is:

[n=<decimal number>][m=<decimal number>][t=<hex number>]<hex bytes to send>

First it must successfully open the Line; select Line Protocol of "None" so it may open it successfully.

optionalItem "Receiver" optionalItemInstance NULL

action "Receive"

The Receive action picks up characters from the Line.

First it must successfully open the Line; select Line Protocol of "None" so it may open it successfully.

optionalItem "Receiver" optionalItemInstance NULL

action "Hex Receive"

The Hex Receive action picks up bytes from the Line.

First it must successfully open the Line; select Line Protocol of "None" so it may open it successfully.

optionalItem "Transmitter" optionalItemInstance NULL

action "Transmit <value>"

The Transmit action sends characters to the Line.

First it must successfully open the Line; select Line Protocol of "None" so it may open it successfully.

optionalItem "Transmitter" optionalItemInstance NULL

action "Hex Transmit <value>"

The Hex Transmit action sends bytes to the Line.

First it must successfully open the Line; select Line Protocol of "None" so it may open it successfully.

group "NTP" optionalGroupInstance NULL

optionalItem NULL optionalItemInstance NULL

action "Sync"

The Sync action requests immediate clock synchronization with the NTP server.

group "Tunnel" optionalGroupInstance Required

optionalItem "Current Connection" optionalItemInstance Required

action "Kill"

The Kill action manually disconnects an active Tunnel connection.

CURL example:

```
curl -u admin:PASSWORD http://<ip-address>/action/status -X POST -d
   "group=Interface&optionalGroupInstance=eth0&action=Renew"
```

Javascript example:

```
myXmlhttprequest.open(
   "POST",
   "/action/status",
   true
```

```
);
request.send(
    " group=Interface&optionalGroupInstance=wlan0&action=Renew "
);
```

File System Web API

The File System Web API is a RESTful cloud API that allows basic manipulation of file system nodes (files and directories). It is intended to support web-based file system access without the need of a browser, and as such can be used in scripts with HTTP programs such as cURL.

Supported file system node operations are implemented via various HTTP request types. The File System Web API uses standard HTTP requests as well as HTTP extensions from the Web Distributed Authoring and Versioning (WebDAV) standard.

Four principal HTTP requests are implemented by the API: GET, PUT, MKCOL, and DELETE.

HTTP GET

Used to read the contents of files and directories in the file system.

URL: `http://<hostname>/fs/[node]`

Where node can be a file, in which case the file content is returned, or a directory, in which case an XML-formatted list of directory objects is returned.

HTTP Response Codes:

200: Success

404: Node not found

Example:

```
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/embedded
<!-- Automatically generated XML -->
<!DOCTYPE directorylist [
<!ELEMENT dentry (name,size)>
<!ELEMENT name (#CDATA)>
<!ELEMENT size (#CDATA)>
<!ATTLIST dentry type CDATA #IMPLIED>
<!ATTLIST directorylist path CDATA #IMPLIED>
]>
<directorylist path = "/embedded">
<dentry type = directory>
<name>main</name>
<size>0</size>
</dentry>
<dentry type = directory>
<name>modem_emulation</name>
<size>0</size>
</dentry>
<dentry type = directory>
<name>monitor</name>
<size>0</size>
</dentry>
<dentry type = directory>
<name>ntp</name>
<size>0</size>
```

```
</dentry>
<dentry type = directory>
<name>query_port</name>
<size>0</size>
</dentry>
<dentry type = directory>
<name>tunnel</name>
<size>0</size>
</dentry>
<dentry type = directory>
<name>user_data</name>
<size>0</size>
</dentry>
</directorylist>
```

HTTP PUT

Used to place new files in the file system and update existing files. Directories cannot be created using PUT; the MKCOL request must be used.

Note that PUT will overwrite an existing file by the same name.

URL: `http://<hostname>/fs/[path]/file`

HTTP Response Codes:

201: File successfully created. This code is part of the WebDAV standard.

509: Not enough space

500: Other failure

Example:

```
# ls -l
-rw-r--r-- 1 user wheel 166 Oct 22 2013 file.txt
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/ -T file.txt
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/
<!-- Automatically generated XML -->
<!DOCTYPE directorylist [
<!ELEMENT dentry (name,size)>
<!ELEMENT name (#CDATA)>
<!ELEMENT size (#CDATA)>
<!ATTLIST dentry type CDATA #IMPLIED>
<!ATTLIST directorylist path CDATA #IMPLIED>
]>
<directorylist path = "/embedded">
<dentry type = file>
<name>file.txt</name>
<size>166</size>
</dentry>
</directorylist>
```

HTTP MKCOL

Used to create new directories (not files) in the file system. MKCOL ?is an HTTP extension from the WebDAV standard.

URL: `http://<hostname>/fs/[path]/directory`

HTTP Response Codes:

201: Directory successfully created. This code is part of the WebDAV standard.

409: Directory already exists

500: Other failure

Example:

```
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/dir1 -X MKCOL
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/
<!-- Automatically generated XML -->
<!DOCTYPE directorylist [
<!ELEMENT dentry (name,size)>
<!ELEMENT name (#CDATA)>
<!ELEMENT size (#CDATA)>
<!ATTLIST dentry type CDATA #IMPLIED>
<!ATTLIST directorylist path CDATA #IMPLIED>
]>
<directorylist path = "/embedded">
<dentry type = file>
<name>file.txt</name>
<size>166</size>
</dentry>
<dentry type = directory>
<name>dir1</name>
<size>0</size>
</dentry>
</directorylist>
```

HTTP DELETE

Used to remove files and directories from the file system.

URL: `http://<hostname>/fs/[path]/node`

Where node can be either a file or directory.

HTTP Response Codes:

204: No content (node successfully removed). This code is part of the WebDAV standard.

404: Node not found

500: Other failure

Example:

```
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/file.txt -X DELETE
# curl -s -u admin:PASSWORD http://192.168.0.1/fs/
<!-- Automatically generated XML -->
<!DOCTYPE directorylist [
<!ELEMENT dentry (name,size)>
<!ELEMENT name (#CDATA)>
<!ELEMENT size (#CDATA)>
<!ATTLIST dentry type CDATA #IMPLIED>
<!ATTLIST directorylist path CDATA #IMPLIED>
]>
<directorylist path = "/embedded">
<dentry type = directory>
<name>dir1</name>
<size>0</size>
</dentry>
</directorylist>
```

6: Commands and Levels

Click the level in the tree structure and it will take you to the command list for that level.

- root
  - enable (enable)
    - configure (config)
      - arp (config-arp)
      - cli (config-cli)
        - ssh (config-cli-ssh)
        - telnet (config-cli-telnet)
      - clock (config-clock)
        - ntp (config-clock-ntp)
      - percepxion (config-percepxion)
        - connection <*number*> (config-percepxion-connection:<*number*>)
        - line <number> (config-percepxion-line:<number>)
      - diagnostics (config-diagnostics)
        - log (config-diagnostics-log)
      - discovery (config-discovery)
      - ftp (config-ftp)
      - host <*number*> (config-host:<*number*>)
      - http (config-http)
      - icmp (config-icmp)
      - if 1 (config-if:eth0)
        - link (config-ethernet:eth0)
      - ip (config-ip)
      - ip address filter (config-ipaddrfilter)
        - ip address filter <*number*> (config-ipaddrfilter-ip_address_filter:<*number*>)
      - rss (config-rss)
      - smtp (config-smtp)
      - snmp (config-snmp)
        - snmpd (config-snmp-snmpd)
        - traps (config-snmp-traps)
      - syslog (config-syslog)
      - terminal <*line*> (config-terminal:<*line*>)
      - terminal network (config-terminal:network)
      - user management (config-user-management)
    - device (device)
      - cp functions (device-cp-functions)
      - reboot schedule (device-reboot-schedule)
    - dns (dns)
    - email <*number*> (email:<*number*>)
    - filesystem (filesystem)
    - line <*line*> (line:<*line*>)
    - ssh (ssh)
      - client (ssh-client)
      - server (ssh-server)
    - ssl (ssl)
      - credentials (ssl-credentials)
      - trusted authorities (ssl-auth)
    - tunnel <*line*> (tunnel:<*line*>)
      - accept (tunnel-accept:<*line*>)
        - password (tunnel-accept-password:<*line*>)

- connect (tunnel-connect:<*line*>)
  - host 1 (tunnel-connect-host:<*line*>:<*number*>)
- disconnect (tunnel-disconnect:<*line*>)
- modem (tunnel-modem:<*line*>)
- packing (tunnel-packing:<*line*>)
- serial (tunnel-serial:<*line*>)

- xml (xml)

accept (tunnel-accept:<*line*>) level commands (<*line*> is the number of the line)	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <*hexadecimal*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as 'always'.
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + n, where 'n' is the line number for this tunnel.
default protocol	Restores the default accept mode tunneling protocol as 'TCP'.
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive	Defaults the TCP keep alive time.

default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary <*binary*>	Sets the accept tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <*text*>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.
kill connection	Disconnects the active accept mode tunneling connection.
local port <*number*>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection for the SSL server.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
no tcp user timeout	Restores the default.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocol ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
secure protocols tls1.3 disable	Disables the protocol.
secure protocols tls1.3 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character *<control>*	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
tcp keep alive *<milliseconds>*	Sets the TCP keep alive time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.
tcp keep alive interval *<milliseconds>*	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = TCP keep alive for accept mode in milliseconds.
tcp keep alive probes *<number>*	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.
write	Stores the current configuration in permanent memory.
arp (config-arp) level commands	
add *<IP address> <MAC address> <Interface name>*	Adds an entry to the ARP table, mapping an IP address to a MAC address. <ip address> = IP address to be mapped. <mac address> = MAC address in colon-separated form. <interface name> = Interface name
clrscrn	Clears the screen.
exit	Exits to the configuration level.
remove all	Removes all entries from the ARP cache.
remove ip *<IP address> <Interface name>*	Removes an entry from the ARP cache. <ip address> = address of the entry being removed. <interface name> = Interface name
show cache	Displays the ARP cache table.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
cli (config-cli) level commands	
clrscrn	Clears the screen.
default inactivity timeout	The default inactivity timeout will apply to CLI sessions.
default quit connect line	Restores the default string to quit the 'connect line', 'telnet', and 'ssh' commands.
enable level password *<text>*	Sets the enable-level password.
exit	Exits to the configuration level.
inactivity timeout *<minutes>*	Sets the inactivity timeout for all CLI sessions.
line authentication disable	No password required for Line CLI users.
line authentication enable	Challenges the Line CLI user with a password.
no enable level password	Removes the enable-level password.
no inactivity timeout	No inactivity timeout will apply to CLI sessions.

quit connect line <*control*>	Sets the string used to quit the 'connect line', 'telnet', and 'ssh' commands. The characters may be input as text or control. A control character has the form <control>C.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh	Change to menu level for SSH configuration and status.
telnet	Change to menu level for Telnet configuration and status.
write	Stores the current configuration in permanent memory.
client (ssh-client) level commands	
clrscrn	Clears the screen.
default user <*username*> command	Restore the user command to the default login shell
delete all known hosts	Remove all known hosts
delete all users	Remove all users
delete known host <*server*>	Remove known host
delete user <*username*>	Delete the named user
exit	Exits to the ssh level.
known host <*server*>	Set known host RSA or DSA key
no known host <*server*> dsa	Remove known host DSA key
no known host <*server*> rsa	Remove known host RSA key
no user <*username*> dsa	Remove user DSA key
no user <*username*> rsa	Remove user RSA key
show	Show SSH Client settings
show history	Displays the last 20 commands entered during the current CLI session.
show known host <*server*>	Show known host RSA and DSA keys
show user <*username*>	Show information for a user
user <*username*>	Set username and RSA or DSA keys
user <*username*> command <*command*>	Customizes the user command
user <*username*> generate dsa 1024	Generate DSA public and private keys
user <*username*> generate dsa 2048	Generate DSA public and private keys
user <*username*> generate dsa 4096	Generate DSA public and private keys
user <*username*> generate dsa 512	Generate DSA public and private keys
user <*username*> generate dsa 768	Generate DSA public and private keys
user <*username*> generate rsa 1024	Generate RSA public and private keys
user <*username*> generate rsa 2048	Generate RSA public and private keys
user <*username*> generate rsa 4096	Generate RSA public and private keys
user <*username*> generate rsa 512	Generate RSA public and private keys

user <*username*> generate rsa 768	Generate RSA public and private keys
user <*username*> password <*password*>	Set username with password and optional RSA or DSA keys
write	Stores the current configuration in permanent memory.
clock (config-clock) level commands	
clock set <*time(hh:mm:ss)*> <*day (1-31)*> <*month text*> <*year*>	Sets the system clock.
clock timezone	Shows possible time zone names.
clock timezone <*time zone*>	Sets the timezone to be displayed. Use "clock timezone" to show choices.
clrscrn	Clears the screen.
default clock timezone	Restores the default timezone, which is UTC.
default synchronization method	Restores the default time synchronization method (Manual).
exit	Exits to the configuration level.
ntp	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show system clock	Displays the system clock.
synchronization method manual	Set time manually.
synchronization method sntp	Synchronize time with a NTP server.
write	Stores the current configuration in permanent memory.
configure (config) level commands	
arp	Changes to the command level for ARP configuration and status.
cli	Change to menu level for CLI configuration and status
clock	Change to menu level for Clock configuration and status
clrscrn	Clears the screen.
percepxion	Enters the percepxion level.
diagnostics	Enters the diagnostics level.
discovery	Enters the discovery level.
exit	Exits to the enable level.
ftp	Enters the ftp level.
host <*number*>	Change to config host level
http	Enters the http level.
icmp	Changes to the command level for ICMP configuration and status.
if <*instance*>	Changes to the interface configuration level.
ip	Changes to the command level for IP configuration and status.
ip address filter	Enters the ipfilter level.
kill ssh <*session*>	Kills SSH session with index from "show sessions"
kill telnet <*session*>	Kills Telnet session with index from "show sessions"
rss	Change to menu level for RSS configuration and status
show	Displays system information.
show history	Displays the last 20 commands entered during the current CLI session.

show lines	Displays line information.
smtp	Changes to the command level for SMTP configuration and status.
snmp	Enters the snmp level.
syslog	Enters the syslog level.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
user management	Enters the config-user-management level.
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:<*line*>) level commands (<*line*> is the number of the line)	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as 'disable'.
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <*instance*>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.

kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <*number*>	Sets a specific port for use as the local port. <number> = the number of the port to use.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <*number*>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <*milliseconds*>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <*control*>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
connection <*number*> (config-percepxion-connection:<*number*>) level commands (<*number*> is 1 or 2)	
clrscrn	Clears the screen.
connect to cloud	Sets the connection to Cloud based server.
connect to on-premise	Sets the connection to On-Premise server.
default connect to	Restores the default connection to Cloud based server.
default host	Restores the Hostname or IP address of percepxion.
default local port	Clears the local port for percepxion client.
default mqtt local port	Clears the local port for percepxion MQTT client.
default port	Restores the Port of percepxion.
default proxy port	Restores the Port of proxy server.
default proxy type	Restores the default Proxy server type (SOCKS5).
exit	Exits to the next higher level.
host <*text*>	Sets the Hostname or IP address of percepxion.
local port <*number*>	Sets the local port for percepxion client. When configured, a total of 16 consecutive ports will be reserved.
mqtt local port <*number*>	Sets the local port for percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
mqtt security disable	Disables SSL for MQTT.
mqtt security enable	Enables SSL for MQTT.
mqtt state disable	Disables MQTT.
mqtt state enable	Enables MQTT.
no proxy host	Restores the Hostname or IP address of the proxy server.
no proxy password	Restores the password for proxy server.
no proxy username	Clears the user name for the proxy server.
port <*number*>	Sets the Port of percepxion.
proxy host <*text*>	Sets the Hostname or IP address of the proxy server.
proxy password <*text*>	Sets the password the proxy server.
proxy port <*number*>	Sets the Port of the proxy server.

proxy type socks5	Sets the Proxy server type to SOCKS5
proxy username <text>	Sets the user name for the proxy server.
secure port disable	Disables HTTPS for Percepxion client.
secure port enable	Enables HTTPS for Percepxion client.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
use proxy disable	Disables use of proxy server for this connection.
use proxy enable	Enables use of proxy server for this connection.
validate certificates disable	Disables certificate validation for Percepxion client.
validate certificates enable	Enables certificate validation for Percepxion client.
write	Stores the current configuration in permanent memory.
percepxion (config-percepxion) level commands	
active connection connection <number>	Sets active connection to Connection <number>.
allow remote connections disable	Disables Percepxion Remote Access.
allow remote connections enable	Enables Percepxion Remote Access
apply configuration updates always	Sets the action on configuration updates to Always, signifying that the device will always apply configuration updates.
apply configuration updates if unchanged	Sets the action on configuration updates to If unchanged, signifying that the device will only apply configuration updates if no changes have been made locally.
apply configuration updates never	Sets the action on configuration updates to Never, signifying no configuration updates will be applied.
apply firmware updates disable	Restores the default action on new firmware (do not apply).
apply firmware updates enable	Automatically apply new firmware.
audit log disable	Disables audit log
audit log enable	Enables audit log.
clrscrn	Clears the screen.
connection <instance>	Enters the next lower level. Specify the instance for the next lower level.
content check interval <hours>	Sets the firmware and configuration check interval.
default active connection	Restores the default active connection, which is Connection 1.
default apply configuration updates	Restores the default setting for configuration updates (Never).
default content check interval	Restores the default firmware and configuration check interval.
default remote access local port	Clears the local port for Percepxion Remote Access.
default status update interval	Restores the default status update interval.
device description <text>	Sets the Device Description.
device id <text>	Sets the Device ID.
device key <text>	Sets the Device Key.

device name <text>	Sets the Device Name.
exit	Returns to the config level.
line <number>	Change to line configuration level.
no device description	Removes the Device Description.
no device id	Removes the Device ID.
no device key	Removes the Device Key.
no device name	Removes the Device Name.
reboot after firmware update disable	Restores the default action when new firmware is applied (reboot)
reboot after firmware update enable	Enables automatic reboot when new firmware is applied.
reboot after update disable	Restores the default action when new configuration is applied (do not reboot)
reboot after update enable	Enables automatic reboot when new configuration is applied.
remote access local port <number>	Sets the local port for Percepxion Remote Access.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the percepxion statistics.
state disable	Disables the percepxion client.
state enable	Enables the percepxion client.
status update interval <minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
cp functions (device-cp-functions) level commands	
clrscrn	Clears the screen.
exit	Returns to the previous level.
reset to factory defaults cp disable	Disables reset to factory defaults CP (Configurable Pins) function. Note that the CP function is not implemented on the EDS3000 hardware.
reset to factory defaults cp enable	Enables reset to factory defaults CP function.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
credentials (ssl-credentials) level commands	
clrscrn	Clears the screen.
create *<credential name>*	Create a new credential name
delete *<credential name>*	Delete existing credential by name
edit *<credential name>*	View or edit an existing credential
exit	Exits to the ssl level.
show	Show existing credential names
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
device (device) level commands	
auto show tlog	Continuously displays the internal trouble log.
clrscrn	Clears the screen.

cp functions	Enters the cp functions level
default long name	Restores the default product long name.
default short name	Restores the default product short name.
exit	Exit to the enable level.
long name <*name*>	Sets the product long name, displayed in command mode and the Web interface.
reboot schedule	Enters the reboot schedule level
short name <*name*>	Sets the product short name, displayed in command mode and the Web interface. <name> = maximum of eight characters.
show	Show system information
show hardware information	Displays information about the hardware.
show history	Displays the last 20 commands entered during the current CLI session.
show lines	Show line information
show memory	Displays current memory usage information.
show task state	Displays current task states.
show tlog	Displays the internal trouble log.
write	Stores the current configuration in permanent memory.
diagnostics (config-diagnostics) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
log	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:<*line*>) level commands (<*line*> is the number of the line)	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <*control*>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
timeout <*milliseconds*>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.
write	Stores the current configuration in permanent memory.
discovery (config-discovery) level commands	

clear counters	Zeros Query Port counters
clrscrn	Clears the screen.
exit	Returns to the config level.
no clear counters	Unzeros Query Port counters
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays statistics and information about the discovery services.
state disable	Disables the Query Port server.
state enable	Enables the Query Port server.
write	Stores the current configuration in permanent memory.
dns (dns) level commands	
clrscrn	Clears the screen.
exit	Exits to the enable level.
lookup *<host_or_ip>*	Return a lookup on the DNS name or IP address.
show	Show DNS status.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
email *<number>* (email:*<number>*) level commands (*<number>* is between 1 and 16)	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show log	Displays the email log.
show statistics	Displays email statistics.
subject <*text*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
enable (enable) level commands	
auto show interfaces	Show interface statistics
auto show processes	Continuously show thread runtime information
clrscrn	Clears the screen.
configure	Enters the configuration level.
connect	Show name and number for lines.
connect line <*line*>	Begin session on serial port.
device	Enters the device level.
disable	Exits the enable level.
dns	Enters the DNS level.
email <*number*>	Enters the configure email level.
exit	Exit from the system
filesystem	Enters the filesystem level.
iperf <*params*>	Run iperf with command line parameters passed in quoted string.
kill ssh <*session*>	Kills SSH session with index from "show sessions"
kill telnet <*session*>	Kills Telnet session with index from "show sessions"
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
ping <*host*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	Ping destination n times with x timeout (in seconds)
reload	Reboot system
reload factory defaults	Reload factory defaults to permanent storage
show	Show system information
show history	Displays the last 20 commands entered during the current CLI session.
show interfaces	Show interface statistics
show ip sockets	Show UDP/TCP state information
show lines	Show line information
show multicast routes	show state of VIFs and multicast routing tables
show processes	Show thread runtime information
show routes	show system routing table
show rules	show system rules
show sessions	Show active Telnet and SSH Sessions
ssh	Enters the SSH configuration level.
ssh <*optClientUsername*> <*host*>	Begin SSH session on network <host>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.

ssh <*optClientUsername*> <*host*> <*port*>	Begin SSH session on network <host>:<port>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.
ssl	Enters the SSL configuration level.
tcpdump <*parameters*>	dump traffic on a network
telnet <*host*>	Begin telnet session on network <host>.
telnet <*host*> <*port*>	Begin telnet session on network <host>:<port>.
trace route <*host*>	Trace route to destination
trace route <*host*> <*protocol*>	Trace route to destination using TCP, ICMP, or UDP
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xml	Enters the XML level.
filesystem (filesystem) level commands	
cat <*file*>	Show the contents of a file
cd <*directory*>	Change the current directory to the specified directory
clrscrn	Clears the screen.
cp <*source file*> <*destination file*>	Copy an existing file
dump <*file*>	Show contents of a file as a hex dump
exit	Exits to the enable level.
format	Format the file system and lose all data
ls	Show all files and directories in the current directory
ls <*directory*>	Show all files and directories in the specified directory
mkdir <*directory*>	Create a directory
mv <*source file*> <*destination file*>	Move a file on the file system
pwd	Print working directory
rm <*file*>	Remove a file
rmdir <*directory*>	Remove a directory
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Show file system statistics
show tree	Show all files and directories from current directory
tftp get <*source file*> <*destination file*> <*host*>	Get a file using TFTP
tftp get <*source file*> <*destination file*> <*host*> <*port*>	Get a file using TFTP
tftp put <*source file*> <*destination file*> <*host*>	Put a file using TFTP
tftp put <*source file*> <*destination file*> <*host*> <*port*>	Put a file using TFTP
touch <*file*>	Create a file
ftp (config-ftp) level commands	
clrscrn	Clears the screen.

data port <*number*>	Sets the FTP server data-port.
default data port	Restores the FTP server data-port to default: 20.
default passive mode ports	Clears the FTP server number of passive ports.
default passive mode start port	Clears the FTP server passive mode start port.
default port	Restores the FTP server port to default: 21.
exit	Returns to the config level.
passive mode ports <*number*>	Sets the FTP server number of passive ports.
passive mode start port <*number*>	Sets the FTP server passive mode start port.
port <*number*>	Sets the FTP server port.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the FTP statistics.
state disable	Disables the FTP server.
state enable	Enables the FTP server.
write	Stores the current configuration in permanent memory.
host <*number*> (tunnel-connect-host:<*line*>:<*number*>) level commands (<*line*> is the number of the line and <*number*> is between 1 and 16)	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default connect mode tunneling protocol as 'TCP'.
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary <*binary*>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <*text*>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection for the SSL client.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
secure protocols tls1.3 disable	Disables the protocol.
secure protocols tls1.3 enable	Enables the protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.

tcp keep alive <*milliseconds*>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.
tcp keep alive interval <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = TCP keep alive for connect mode in milliseconds.
tcp keep alive probes <*number*>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.
tcp user timeout <*milliseconds*>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host <*number*> (config-host:<*number*>) level commands (<*number*> is between 1 and 32)	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
http (config-http) level commands	
auth <*uri*>	Creates a new HTTP server authentication directive. <uri> = URI of the server.
auth type <*uri*> digest	Sets an HTTP server authentication directive to the Digest Access Authentication scheme. <uri> = URI of the server.
auth type <*uri*> none	Sets the authentication type for an HTTP server authentication directive to none. <uri> = URI of the server.
auth type <*uri*> basic	Sets the authentication directive to basic. <uri> = URI of the server.
authentication timeout <*minutes*>	For any Digest AuthType, sets the timeout for authentication. <minutes> = authentication timeout value.
clear counters	Sets the HTTP counters to zero.
clear log	Clears the HTTP server log.
clrscrn	Clears the screen.
default authentication timeout	Resets the authentication timeout to its default value.

default log format	Restores the HTTP Server log format string to its default value.
default max bytes	Resets the maximum bytes to its default value.
default max log entries	Restores the default maximum number of HTTP Server log entries.
default max timeout	Resets the timeout to its default value.
default port	Resets the HTTP Server port to its default value.
default secure port	Resets the HTTP Server SSL port to its default value.
default secure protocols	Restores the default secure protocol selections.
delete auth <*uri*>	Deletes an existing HTTP Server authentication directive. <uri> = URI of the server.
exit	Returns to the config level.
https state disable	Disables the HTTPS server.
https state enable	Enables the HTTPS server.
log format <*text*>	Sets the log format string for the HTTP server, using the following directives: %a remote ip address (could be a proxy) %b bytes sent excluding headers %B bytes sent excluding headers (0 = '-') %h remote host (same as %a) %{h}i header contents from request (h = header string) %m request method %p ephemeral local port value used for request %q query string (prepend with '?' or empty '-') %t timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t') %u remote user (could be bogus for 401 status) %U URL path info %r first line of request (same as '%m %U%q <version>') %s return status
logging state disable	Disables HTTP server logging.
logging state enable	Enables HTTP server logging.
max bytes <*number*>	Sets the maximum number of bytes the HTTP server accepts when receiving a request.
max log entries <*number*>	Sets the maximum number of HTTP server log entries. <number> = maximum number of HTTP server log entries.
max timeout <*seconds*>	Sets the maximum time the HTTP server waits when receiving a request. <seconds> = maximum timeout value.
no clear counters	Restores the HTTP counters to the aggregate values.
no port	Disables the HTTP Server port.
no secure credentials	Clears the RSA/DSA certificate selection for the HTTP server.
no secure port	Disables the HTTP Server SSL port.
port <*number*>	Sets the port number the HTTP server will use. <number> = port number.
secure credentials <*text*>	Selects the RSA/DSA certificates by name for the HTTP server.
secure port <*number*>	Sets the port number the HTTP server will use over SSL. <number> = port number.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
secure protocols tls1.3 disable	Disables the protocol.
secure protocols tls1.3 enable	Enables the protocol.
show	Displays the current configuration.
show auth	Displays the HTTP server authentication settings.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the HTTP server log.
show statistics	Displays the HTTP statistics.
state disable	Disables the HTTP server.
state enable	Enables the HTTP server.
write	Stores the current configuration in permanent memory.
icmp (config-icmp) level commands	
clrscrn	Clears the screen.
exit	Exits to the configuration level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Prevents ICMP packets from being sent or received.
state enable	Allows ICMP packets to be sent and received.
write	Stores the current configuration in permanent memory.
if 1 (config-if:eth0) level commands	
clrscrn	Clears the screen.
default gateway *<IP address>*	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
dhcp client id *<text>*	Sets the DHCP client ID.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
dhcp renew	Force DHCP to renew
domain *<text>*	Sets the domain name. <text> = name of the domain.
exit	Exits to the config level.
hostname *<text>*	Sets the host name. <text> = name of the host.
ip address *<ip address/cidr>*	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu *<bytes>*	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.
no hostname	Clears the host name.
no ip address	Clears the IP address.

no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <*IP address*>	Sets the IP address of the primary DNS server.
secondary dns <*IP address*>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
write	Stores the current configuration in permanent memory.
ip (config-ip) level commands	
clrscrn	Clears the screen.
default ip time to live	Restores the default IP time to live.
default multicast time to live	Restores the default IP multicast time to live, which is one hop.
exit	Exits to the configuration level.
ip time to live <*hops*>	Sets the IP time to live, known by SNMP as 'ipDefaultTTL'. <hops> = number of hops that a typical IP packet is allowed to live.
multicast time to live <*hops*>	Sets the IP multicast time to live. <hops> = number of hops that a multicast IP packet is allowed to live.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
ip address filter (config-ipaddrfilter) level commands	
add ip address filter IP <ip address> <action>	Add an IP Address filter address & action.
clrscrn	Clears the screen.
default default ip address filter policy	Restores the default value of Default IP Address filter policy (ACCEPT).
default ip address filter policy accept	Sets the Default IP Address filter policy to ACCEPT.
default ip address filter policy drop	Sets the Default IP Address filter policy to DROP.
delete all ip address filters	Deletes all ip address filters.
delete ip address filter <instance>	Deletes an entry from the ip address filters.
exit	Returns to the config level.
ip address filter <instance>	Enters the next lower level. Specify the instance for the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show ip address filter configuration and status.
state disable	Disables IP Address filtering.
state enable	Enables IP Address filtering.
write	Stores the current configuration in permanent memory.
ip address filter <number> (config-ipaddrfilter-ip_address_filter:x) level commands	
action accept	Sets the action to ACCEPT.
action drop	Sets the action to DROP.
clrscrn	Clears the screen.

default action	Restores the default value of action (ACCEPT).
exit	Exits to the next higher level.
ip address <text>	Sets the filter IP Address.
no ip address	Removes the filter IP Address.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
line *<line>* (line:*<line>*) level commands (*<line>* is the number of the line)	
auto show statistics	Continuously displays line statistics.
baud rate *<bits per second>*	Sets the line speed. <bits per second> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string *<string>*	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
command mode signon message *<string>*	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
command mode wait time *<milliseconds>*	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer *<milliseconds>*	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.

kill session	Kills command mode session on the Line
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
name <*text*>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol managed device	Applies Managed device protocol on the line.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <*bytes*>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <*control*>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
xon char <*control*>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
line <number> (config-percepxion-line<number>) level commands	
clrscrn	Clears the screen.
command delimiter <*text*>	Sets the command delimiter.
content check interval <*hours*>	Sets the firmware and configuration check interval.

default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default local port	Clears the local port for percepxion client.
default status update interval	Restores the default status update interval.
exit	Exits to the config-percepxion level.
line <*number*>	Change to line configuration level.
local port <*number*>	Sets the local port for percepxion client. When configured, a total of 16 consecutive ports will be reserved.
no project tag	Restores the default Project Tag.
project tag <*text*>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <*minutes*>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth0) level commands	
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
default speed	Restores the default speed setting, which is auto-negotiate.
duplex auto	Sets duplex mode to auto.
duplex full	Sets duplex mode to full.
duplex half	Sets duplex mode to half.
exit	Exit back to interface configuration level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
speed 10	Sets the speed of the Ethernet link to 10 Mbps.
speed 100	Sets the speed of the Ethernet link to 100 Mbps.
speed 1000	Sets the speed of the Ethernet link to 1000 Mbps.
speed auto	Sets the speed of the Ethernet link to auto-negotiate.
write	Stores the current configuration in permanent memory.
log (config-diagnostics-log) level commands	
clrscrn	Clears the screen.
default max length	Restores the factory default maximum Log file size.
default output	Restores the default log output, which is disable.
exit	Exits to the next higher level.
max length <*Kbytes*>	Sets the maximum size in Kbytes for the Log file.
output disable	Disables log output.
output filesystem	Enables log to filesystem.
output line <*number*>	Enables log to serial line.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

write	Stores the current configuration in permanent memory.
modem (tunnel-modem:<*line*>) level commands (<*line*> is the number of the line)	
clrscrn	Clears the screen.
connect string <*text*>	Sets the CONNECT string used in modem emulation. <string> = connect string.
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
ntp (config-clock-ntp) level commands	
clrscrn	Clears the screen.
default server	Restores the default NTP server address.
exit	Exits to the next higher level.
server <*text*>	Sets the NTP server address.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:<*line*>) level commands (<*line*> is the number of the line)	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is 'Disable'

default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <*control*>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <*bytes*>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <bytes> = number of bytes in the threshold.
timeout <*milliseconds*>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.
trailing character <*control*>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:<*line*>) level commands (<*line*> is the number of the line)	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <*text*>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
reboot schedule (device-reboot-schedule) level commands	
clrscrn	Clears the screen.
default hours	Restores the default hour of day for reboot schedule time.
default interval	Restores the default schedule interval.
default minutes	Restores the default minutes on the hour for reboot schedule.
default schedule	Restores the default reboot schedule type.
default unit	Restores the default reboot schedule interval unit.
exit	Returns to the previous level.
hours <*hours*>	Sets the hour of day for reboot schedule (Use 24h time).
interval <*number*>	Sets the reboot schedule interval

minutes <*minutes*>	Sets the minutes on the hour for reboot schedule.
schedule daily	Sets the reboot schedule type to 'daily'.
schedule interval	Sets the reboot schedule type to 'interval'.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables scheduled reboots.
state enable	Enables scheduled reboots.
unit days	Sets the reboot schedule interval to days.
unit hours	Sets the reboot schedule interval to hours.
unit months	Sets the reboot schedule interval to months.
unit weeks	Sets the reboot schedule interval to weeks.
write	Stores the current configuration in permanent memory.
root level commands	
clrscrn	Clears the screen.
enable	Enters the enable level.
exit	Exit from the system.
iperf <*params*>	Run iperf with command line parameters passed in quoted string.
ping <*host*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	Ping destination n times with x timeout (in seconds)
show	Show system information
show history	Displays the last 20 commands entered during the current CLI session.
show lines	Show line information
show multicast routes	show state of VIFs and multicast routing tables
show routes	show system routing table
show rules	show system rules
tcpdump <*parameters*>	dump traffic on a network
trace route <*host*>	Trace route to destination
trace route <*host*> <*protocol*>	Trace route to destination using TCP, ICMP, or UDP
rss (config-rss) level commands	
clear rss	Clear the RSS Feed data
clrscrn	Clears the screen.
default max entries	Restores the default number of RSS feed entries.
exit	Exits to the configuration level.
feed disable	Disables RSS feed.
feed enable	Enables RSS feed.
max entries <*number*>	Sets the maximum number of RSS feed entries.
persist disable	Disables RSS feed data persistence.
persist enable	Enables RSS feed data persistence.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Display the RSS Feed status
write	Stores the current configuration in permanent memory.

serial (tunnel-serial:<*line*>) level commands (<*line*> is the number of the line)	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
server (ssh-server) level commands	
authorized user <*username*> <*password*>	Sets authorized username, password, and optionally RSA and/or DSA public keys
clrscrn	Clears the screen.
delete all authorized users	Removes all authorized users
delete authorized user <*username*>	Remove an authorized user
exit	Exits to the ssh level.
host generate dsa 1024	Generate DSA public and private keys
host generate dsa 512	Generate DSA public and private keys
host generate dsa 768	Generate DSA public and private keys
host generate rsa 1024	Generate RSA public and private keys
host generate rsa 2048	Generate RSA public and private keys
host generate rsa 4096	Generate RSA public and private keys
host generate rsa 512	Generate RSA public and private keys
host generate rsa 768	Generate RSA public and private keys
host keys	Sets RSA or DSA public and/or private keys
no host dsa	Removes DSA public and private keys
no host rsa	Removes RSA public and private keys
show	Show SSH Server settings
show authorized user <*username*>	Show information for an authorized user
show history	Displays the last 20 commands entered during the current CLI session.
show host dsa	Show full DSA public key
show host rsa	Show full RSA public key
write	Stores the current configuration in permanent memory.
smtp (config-smtp) level commands	
clrscrn	Clears the screen.
default local port	Clears the local port for SMTP client.
default server port	Restores the SMTP server port to its default.
exit	Exits to the configuration level.
from address <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.

local port <*number*>	Sets the local port for SMTP client.
no from address	Removes the From address for email alerts.
no overriding domain	Removes the overriding domain name option.
no password	Removes the password.
no server address	Removes the SMTP server address.
no username	Removes the username.
overriding domain <*text*>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
password <*text*>	Sets the password for logging in to the mail server.
server address <*text*>	Sets an SMTP server address to direct all outbound email messages through a mail server.
server port <*number*>	Sets the SMTP server port.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <*text*>	Sets the username for logging in to the mail server.
write	Stores the current configuration in permanent memory.
snmp (config-snmp) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
no system location	Clears the SNMP system location.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays the SNMP agent status.
snmpd	Enters the next lower level.
system location <*text*>	Sets the SNMP system location. <text> = location of device.
traps	Enters the next lower level.
write	Stores the current configuration in permanent memory.
snmpd (config-snmp-snmpd) level commands	
authentication password <*text*>	Sets password used for authentication for agent.
authentication protocol md5	Uses MD5 for authentication for agent.
authentication protocol sha	Uses SHA for authentication for agent.
clrscrn	Clears the screen.
default authentication protocol	Restores to default SNMPv3 authentication method: MD5 for agent.
default port	Restores the SNMP agent port to default: 161.
default privacy protocol	Restores to default SNMPv3 privacy encryption method: DES for agent.
default read community	Restores the SNMP read-only community to default: public
default read-only authentication protocol	Restores to default SNMPv3 read-only authentication method: MD5 for agent.
default read-only privacy protocol	Restores to default SNMPv3 read-only privacy encryption method: DES for agent.
default read-only security	Restores to default SNMPv3 read-only security method: Authentication, No Privacy for agent.

default security	Restores to default SNMPv3 security method: Authentication, No Privacy for agent.
default system description	Restores the SNMP system description to its default.
default system name	Restores the SNMP system name to default: the product name.
default version	Restores to default SNMP version v2c for agent.
default write community	Clears the SNMP read/write community to default: private
exit	Exits to the next higher level.
no authentication password	Clears authentication password for agent.
no privacy password	Clears privacy password for agent.
no read-only authentication password	Clears read-only authentication password for agent.
no read-only privacy password	Clears read-only privacy password for agent.
no read-only username	Clears SNMPv3 read-only username for agent.
no system contact	Clears the SNMP system contact.
no username	Clears SNMPv3 username for agent.
port *<number>*	Sets the SNMP agent port.
privacy password *<text>*	Sets password used for privacy encryption for agent.
privacy protocol aes	Uses AES for privacy encryption for agent.
privacy protocol des	Uses DES for privacy encryption for agent.
read community *<text>*	Sets the SNMP read-only community string. <text> = name of the read-only community string to be set.
read-only authentication password *<text>*	Sets password used for read-only authentication for agent.
read-only authentication protocol md5	Uses MD5 for read-only authentication for agent.
read-only authentication protocol sha	Uses SHA for read-only authentication for agent.
read-only privacy password *<text>*	Sets password used for read-only privacy encryption for agent.
read-only privacy protocol aes	Uses AES for read-only privacy encryption for agent.
read-only privacy protocol des	Uses DES for read-only privacy encryption for agent.
read-only security authentication and privacy	Authentication and Privacy for agent.
read-only security authentication but no privacy	Authentication, No Privacy for agent.
read-only security no authentication and no priv	No Authentication, No Privacy for agent.
read-only username *<text>*	Sets SNMPv3 read-only username for agent.
security authentication and privacy	Authentication and Privacy for agent.
security authentication but no privacy	Authentication, No Privacy for agent.
security no authentication and no priv	No Authentication, No Privacy for agent.

show	Shows the current configuration.
show engine id	Displays the SNMP agent engine ID.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the SNMP agent.
state enable	Enables the SNMP agent.
system contact *<text>*	Sets the SNMP system contact information. <text> = system contact information.
system description *<text>*	Sets the SNMP system description. <text> = description of device.
system name *<text>*	Sets the SNMP system name. <text> = SNMP system name.
username *<text>*	Sets SNMPv3 username for agent.
version snmpv1	Uses SNMPv1 for agent.
version snmpv2c	Uses SNMPv2c for agent.
version snmpv3	Uses SNMPv3 for agent.
write	Stores the current configuration in permanent memory.
write community *<text>*	Sets the SNMP read-write community string. <text> = name of the read-write community string to be set.
ssh (ssh) level commands	
client	Enters the SSH Client configuration level.
clrscrn	Clears the screen.
exit	Exits to the enable level.
server	Enters the SSH Server configuration level.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
ssh (config-cli-ssh) level commands	
clrscrn	Clears the screen.
default max sessions	Restores the default maximum allowed concurrent incoming SSH sessions.
default port	Restores the default local port to the SSH server.
exit	Exits to the CLI level.
max sessions *<number>*	Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions.
port *<number>*	Sets the local port that the SSH server uses. <number> = local port number.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the SSH server statistics.
state disable	Disables the SSH Server.
state enable	Enables the SSH Server.
write	Stores the current configuration in permanent memory.
ssl (ssl) level commands	
clrscrn	Clears the screen.
credentials	Enters the SSL credentials configuration level.
delete csr	Delete generated CSR (Certificate Signing Request).
exit	Exits to the enable level.
generate csr	Generate a new CSR (Certificate Signing Request).
show history	Displays the last 20 commands entered during the current CLI session.

trusted authorities	Enters the SSL configuration level.
view csr	View generated CSR (Certificate Signing Request).
write	Stores the current configuration in permanent memory.
syslog (config-syslog) level commands	
clrscrn	Clears the screen.
default local port	Clears the syslog local port.
default remote port	Restores the default syslog remote port.
default severity log level	Restores the default to no logging.
exit	Returns to the config level.
host <*text*>	Sets the address of the syslog recipient. <text> = IP address or name of the host.
local port <*number*>	Sets the syslog local port.
no host	Removes the address of the syslog recipient.
remote port <*number*>	Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.
severity log level alert	Log only Alert and more severe events.
severity log level critical	Log only Critical and more severe events.
severity log level debug	Log all events.
severity log level emergency	Log only Emergency events.
severity log level error	Log only Error and more severe events.
severity log level information	Log only Information and more severe events.
severity log level none	No logging.
severity log level notice	Log only Notice and more severe events.
severity log level warning	Log only Warning and more severe events.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the syslog statistics.
state disable	Disables syslog logging.
state enable	Enables syslog logging.
write	Stores the current configuration in permanent memory.
telnet (config-cli-telnet) level commands	
authentication disable	No password required for Telnet users.
authentication enable	Challenges the Telnet user with a password.
clrscrn	Clears the screen.
default max sessions	Restores the default maximum allowed concurrent incoming Telnet sessions.
default port	Restores the default local port to the Telnet server.
exit	Exits to the CLI level.
max sessions <*number*>	Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions.
port <*number*>	Sets the local port that the Telnet server uses. <number> = local port number.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the Telnet statistics.

state disable	Disables the Telnet Server.
state enable	Enables the Telnet Server.
write	Stores the current configuration in permanent memory.
terminal *<line>* (config-terminal:*<line>*) level commands (*<line>* is the number of the line)	
break duration *<milliseconds>*	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, 'UNKNOWN'.
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line *<line>*	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break *<control>*	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal *<line>*	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type *<text>*	Sets the terminal type.
tunnel *<line>*	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal network (config-terminal:network) level commands	
break duration *<milliseconds>*	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, 'UNKNOWN'.
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.

exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*control*>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
traps (config-snmp-traps) level commands	
authentication password <*text*>	Sets password used for authentication for traps.
authentication protocol md5	Uses MD5 for authentication for traps.
authentication protocol sha	Uses SHA for authentication for traps.
clrscrn	Clears the screen.
community <*text*>	Sets the SNMP trap community string. <text> = name of the trap community string to be set.
default authentication protocol	Restores to default SNMPv3 authentication method: MD5 for traps.
default community	Restores the SNMP trap community to default: public
default primary destination port	Restores the primary SNMP trap host port to default: 162.
default privacy protocol	Restores to default SNMPv3 privacy encryption method: DES for traps.
default secondary destination port	Restores the secondary SNMP trap host port to default: 162.
default security	Restores to default SNMPv3 security method: Authentication, No Privacy for traps.
default version	Restores to default SNMP version v2c for traps.
exit	Exits to the next higher level.
no authentication password	Clears authentication password for traps.
no primary destination	Deletes the primary SNMP trap host.

no privacy password	Clears privacy password for traps.
no secondary destination	Deletes the secondary SNMP trap host.
no username	Clears SNMPv3 username for traps.
primary destination *<text>*	Sets the primary SNMP trap host. <text> = IP address or hostname of SNMP trap receiver.
primary destination port *<number>*	Sets the primary SNMP trap host port.
privacy password *<text>*	Sets password used for privacy encryption for traps.
privacy protocol aes	Uses AES for privacy encryption for traps.
privacy protocol des	Uses DES for privacy encryption for traps.
secondary destination *<text>*	Sets the secondary SNMP trap host. <text> = IP address or hostname of SNMP trap receiver.
secondary destination port *<number>*	Sets the secondary SNMP trap host port.
security authentication and privacy	Authentication and Privacy for traps.
security authentication but no privacy	Authentication, No Privacy for traps.
security no authentication and no priv	No Authentication, No Privacy for traps.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username *<text>*	Sets SNMPv3 username for traps.
version snmpv1	Uses SNMPv1 for traps.
version snmpv2c	Uses SNMPv2c for traps.
version snmpv3	Uses SNMPv3 for traps.
write	Stores the current configuration in permanent memory.
trusted authorities (ssl-auth) level commands	
add	Adds an Authority Certificate.
clrscrn	Clears the screen.
exit	Exits to the ssl level.
no intermediate authority *<cert>*	Removes an Intermediate Authority Certificate. <cert> = index displayed by "show authority" command.
no trusted authority *<cert>*	Removes a Trusted Authority Certificate. <cert> = index displayed by "show authority" command.
show	Displays Authority Certificate Information.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
tunnel *<line>* (tunnel:*<line>*) level commands (*<line>* is the number of the line)	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.

line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
user management (config-user-management) level commands	
admin password <*text*>	Sets the CLI login password. Password must be 4 to 15 characters and contain combination of the following characters: uppercase letters, lowercase letters, numbers, symbols (punctuation marks). Put double quotes around the password.
admin username <*text*>	Sets the CLI login username.
clrscrn	Clears the screen.
create role <*role name*>	Create a new role <role name> = role name.
create user <*user name*> <*password*> <*role name*>	Create a new user <user name> = user name. <password> = user password. Password must be 4 to 15 characters and contain combination of the following characters: uppercase letters, lowercase letters, numbers, symbols (punctuation marks). Put double quotes around the password. <role name> = user role name.
default admin password	Restores the default CLI login password.
default admin username	Restores the default CLI login username.
delete role <*role name or instance*>	Delete existing role <role name or instance> = role name or instance.
delete user <*user name or instance*>	Delete existing user <user name or instance> = user name or instance.
edit role <*role name or instance*>	Change to config-user-management-roles level.
edit user <*user name or instance*>	Change to config-user-management-users level.
exit	Returns to the config level.
show	Displays the current configuration.
show actions	List Actions to the console
show configuration groups	List Configuration Record group names to the console
show history	Displays the last 20 commands entered during the current CLI session.
show roles	Show existing roles
show users	Show existing users
write	Stores the current configuration in permanent memory.
xml (xml) level commands	
clrscrn	Clears the screen.

exit	Exits to the enable level.
jsr dump	Dump JSON Status Records to the console
jsr dump <*group list*>	Dump specified JSON Status Records to the console
jsr export <*file*>	Save JSON Status Record to a file
jsr export <*file*> <*group list*>	Save specified JSON Status Record to a local file
jsr list	List JSON Status Record groups to the console
jsr metadata dump <*group list*>	Dump specified JSON Status Records with metadata to the console
jsr metadata export <*file*>	Save JSON Status Record to a file
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
xcr dump	Dump XML configuration to the console
xcr dump <*group list*>	Dump specified XML configuration to the console
xcr export <*file*>	Save XML configuration to a file
xcr export <*file*> <*group list*>	Save specified XML configuration to a local file
xcr import <*file*>	Load XML configuration from a local file
xcr import <*file*> <*group list*>	Load specified XML configuration from a local file
xcr list	List XML Configuration Record groups to the console
xsr dump	Dump XML Status Records to the console
xsr dump <*group list*>	Dump specified XML Status Records to the console
xsr export <*file*>	Save XML Status Record to a file
xsr export <*file*> <*group list*>	Save specified XML Status Record to a local file
xsr list	List XML Status Record groups to the console