JUNE 2004

BLACK BOX® ServSelect™ IP SCPS

KV119A
KV119E
KV129A
KV129E

BLACK BOX®
NETWORK SERVICES

Welcome to the ServSwitch™ Family!

Thank you for purchasing a BLACK BOX® ServSelect™ brand console port server (SCPS)! We appreciate your business, and we think you'll appreciate the many ways that this product will save you money, time, and effort.

Our ServSwitch family is all about breaking away from the traditional, expensive model of device management and display. You know, the one-size-fits-all-even-if-it-doesn't model that says, "One computer gets one dedicated monitor or user station, no more, no less." Why not a single user station (monitor, keyboard, and mouse) or serial console for multiple computers, routers, etc.— even computers of different platforms? Why not a pair of user stations, each of which can control multiple computers? Why not many monitors or user stations for the same computer? Why not access or display any of your devices, anywhere in the world, with any of your user stations, monitors, or consoles?

With our ServSwitch products, there's no reason why not. We carry a broad line of robust solutions for all these applications:

- Do you have just two PCs and need an economical alternative to keeping two mice, keyboards, and monitors on your desk? Or do you need to share many computers, including a mix of IBM® PC, RS/6000®, Apple® Macintosh®, Sun Microsystems®, and SGI™ types among multiple worldwide users with different access levels?
- Do you have to send video from one computer to two different local monitors? Or do you need to send video from multiple computers to dozens of remote monitors?
- Do you need centralized terminal-based serial control over many sites?
- Does your switch have to sit solidly on a worktable and use regular everyday cables? Or does it have to be mounted in an equipment rack, use convenient many-to-one cables, and have a rackmounted user station that folds and slides into 1U of space?

No matter how large or small your setup is, no matter how simple or how complex, we're confident we have a ServSwitch system that's just right for you. Welcome to the BLACK BOX ServSwitch™ family—the one-stop answer for all your video, serial console, and KVM (Keyboard, Video and Mouse) switching and extension needs!

*

This manual will tell you all about your new ServSelect IP SCPS, including how to install and operate it. For an introduction to the SCPS, see Chapter 2. The Summit product codes covered in this manual are:

KV119A KV119E KV129A KV129E

This manual also includes information about the ServSelect™ IP SCPS Rackmount Kit, which has its own installation instructions:

RMK19I

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA

RADIO-FREQUENCY INTERFERENCE STATEMENTS

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

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

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

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

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in the European standard EN55022. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio-frequency energy, and if not installed and used in accordance with the instructions, might cause harmful interference to radio or television reception.

However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, you can correct the interference with one or more of the following measures:

a. Reorient or relocate the receiving antenna.

b. Increase the separation between the equipment and the receiver.

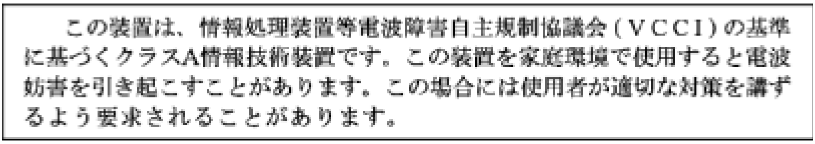
c. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

d. Consult the supplier or an experienced radio/TV technician for help.

Shielded cables must be used with this equipment to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances. This equipment has also been found to comply with European standards EN50082 and EN60950.

CE

Japanese Compliance Statement



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Other Agency Approvals

UL 1950, CSA C22. 2 No. 950, IEC 950
Republic of Korea EMI Standard Certificate Number: E-F900-01-2012 (A)

TRADEMARKS USED IN THIS MANUAL

BLACK BOX and the logo are registered trademarks, and ServSwitch, ServSelect, and ServSelect IP are trademarks of BLACK BOX Corporation.

Apple, Mac, and Macintosh are registered trademarks of Apple Computer, Inc.

IBM, PS/2, and RS/6000 are registered trademarks of International Business Machines Corporation.

Microsoft, Windows, Windows NT, and Windows XP are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. HyperTerminal is a trademark of Hilgraeve, Inc.

Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UL is a registered trademark of Underwriters Laboratories, Inc.

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

Normas Oficiales Mexicanas (NOM)

Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

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

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Contents

1. Specifications

During the course of this product’s lifetime, modifications might be made to its hardware or firmware that could cause these specifications to change without notice.

Agency Approvals	
	FCC P15 Class A, EN55022, EN61000-3-2, EN61000-3-3, EN60950, EN55024, ETL (UL1950), CSA 22.2 No. 950
Server Ports	
Number	8 (SCPS-8); 16 (SCPS-16)
Type	Serial ports
Connectors	Serial port RJ45
Network Connection	
Number	1
Type	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT
Connector	RJ45
Other Characteristics	
Dimensions (H x W x D)	4.45 x 22.23 x 20.32 cm 1U form factor (1.75 x 8.75 x 8.00 in)
Weight	5 lbs (2.3 kg) without cables
Heat Dissipation	75 BTU/hr (SCPS-8); 102 BTU/hr (SCPS-16)
Airflow	2.5 cfm
Power Consumption	22 W (SCPS-8); 30 W (SCPS-16)
AC-input power	50 W maximum
AC-input maximum	90 to 267 VAC
AC-input current rating	0.5 A
AC-input cable	18 AWG three-wire cable, with a three-lead IEC-320 receptacle on the power supply end and a country dependent plug on the power resource end
Frequency	50 to 60 Hz
Temperature	Ø˚ to 40˚ Celsius (32˚ to 104˚ Fahrenheit) operating -20˚ to 65˚ Celsius (-4˚ to 149˚ Fahrenheit) nonoperating
Humidity	10 to 90% noncondensing

2. Introduction

2.1 Features and Benefits

The BLACK BOX® ServSelect™ IP SCPS serial over IP network appliances provide non-blocked access and control for serial devices such as routers, power management devices and firewalls.

You may connect up to 8 serial devices to an SCPS-8, and up to 16 serial devices to an SCPS-16. A single 10/100 Ethernet port provides network connectivity on each SCPS. Two SCPS appliances may be mounted in 1U of vertical space in a standard 19 inch rack.

Serial device access options

You may choose from among several available Telnet options to access the SCPS and its attached serial devices:

- The ServSelect IP Software multiplatform graphic management interface that offers a built-in enhanced Telnet client and a Secure Shell (SSH) client
- Third-party Telnet clients
- Third-party SSH clients

Access to attached serial devices is also possible through a serial Command Line Interface (CLI) connection, a PPP (Point to Point Protocol) dial-in connection to a serial CLI modem or from a third party SSH client.

User authentication and data security

The SCPS user database supports up to 64 user accounts, which include usernames, passwords and/or keys, plus specifications of access rights to SCPS ports and commands. User definitions may be changed at any time. You may choose to have user access authenticated locally at the SCPS user database or at one or more RADIUS (Remote Access Dial-In User Service) servers. Data security may be enhanced via industry-standard SSH encryption.

Extensive command set

The SCPS offers a wide range of commands that allow administrators to easily configure, control and display information about the SCPS operating environment, including its ports, user accounts and active sessions. The user interface also offers descriptive error message data and built-in command help information. On-board Trivial File Transfer Protocol (TFTP) support allows administrators to upload new functionality to SCPS units in the field.

Port history

Each SCPS port has a buffer that holds the most recent 64K bytes of online and offline serial data. A separate history command mode lets you navigate within a port’s current history file and conduct tailored searches.

2.2 Safety Precautions

To avoid potential device problems, if the building has 3-phase AC power, ensure that a computer and its monitor (if used) are on the same phase. For best results, they should be on the same circuit.

To avoid potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Do not use a 2-wire extension cord in any product configuration.
- Test AC outlets at the computer and monitor (if used) for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup Uninterruptible Power Supply (UPS), power the computer, the monitor and the SCPS unit off the supply.

NOTE:
The AC inlet is the main disconnect.

Rack mount safety considerations

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operation temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the unit.
- Reduced Airflow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable Earthing: Reliable earthing of rackmounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

2.3 Using ServSelect IP Software

The ServSelect IP Software graphical management interface may be used to manage SCPS appliances and access attached devices. Using ServSelect IP Software, you may perform most of the operations that are described in this manual. This manual describes how to manage an SCPS by entering commands using the CLI. The ServSelect IP Software Installer/User Guide describes how to manage an SCPS using the graphical interface.

3. Installation and Configuration

3.1 Hardware Overview

Figure 3-1 shows the front of an SCPS-16.

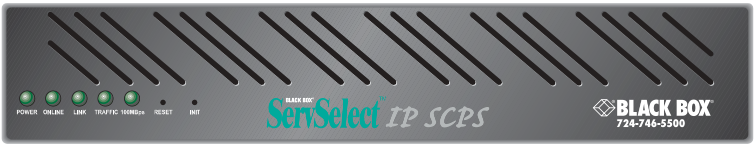


Figure 3-1. SCPS-16 Front View

The lower left area of the front panel contains the following LEDs and buttons:

- The *POWER* LED illuminates when the SCPS is connected to a power source.
- The *ONLINE* LED illuminates steadily (not blinking) when the SCPS self-test and initialization procedures complete successfully.
- The *LINK* LED illuminates when the SCPS establishes a connection to the network.
- The *TRAFFIC* LED blinks when there is network traffic.
- The *100MBps* LED illuminates when the SCPS is connected to a 100 MBps LAN.
- The RESET button, when pressed, reboots the SCPS.
- The INIT button, when pressed, restores the SCPS to factory defaults. See *Reinitializing the SCPS* in this chapter.

Figure 3-2 shows the back panel of an SCPS-16.

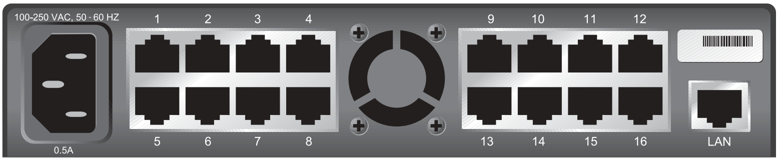


Figure 3-2. SCPS-16 Back Panel

The back panel contains:

- 8 (SCPS-8) or 16 (SCPS-16) RJ45 connectors for serial cabling
- A LAN connector for a 10BaseT or 100BaseT interface cable
- The AC line cord connector

3.2 Installing the SCPS

WARNING:
The power outlet should be installed near the equipment and should be easily accessible.

To install the SCPS hardware:

1. Locate the SCPS where you can connect cables between the serial devices and the SCPS serial ports, and where you can connect a LAN interface cable between the Ethernet hub or switch and the SCPS LAN connector.

   If you are using a rackmount kit, follow the instructions included with the kit.

2. Connect serial devices to the SCPS serial ports; see Chapter 8 for cabling information. Connect each serial device to its appropriate power source, following the device's documentation.

3. Attach a 10BaseT or 100BaseT LAN interface cable to the LAN connector on the back of the SCPS. A CAT 5 cable is required for 100BaseT operation.

4. Insert the power cord into the back of the SCPS. Insert the other end of the power cord into a grounded electrical receptacle.

5. Check that the *POWER* LED on the front of the SCPS is illuminated. If not, check the power cable to ensure that it is inserted snugly into the back of the unit. The *ONLINE* LED will illuminate within one minute to indicate that the unit self-test is complete. If the *ONLINE* LED blinks, contact Technical Support for assistance.

6. Check that the *LINK* LED is illuminated. If not, check the Ethernet cable to ensure that both ends are correctly inserted into their jacks. If the unit is connected to a 100 MB Ethernet hub, the *100MBps* LED will be illuminated.

7. Once the *POWER*, *ONLINE* and *LINK* LEDs are illuminated, remove power from the SCPS and proceed with the configuration process.

WARNING:
The SCPS and all attached devices should be powered down before servicing the unit. Always disconnect the power cord from the wall outlet.

3.3 Configuring the SCPS

To configure the SCPS, you must enter a unique IP address and the network's subnet mask. This information will be stored in the unit's configuration database. During initial login, you will specify a password for the Admin user.

Configuring the IP address and subnet mask

You may use any of four methods to configure the SCPS IP address and subnet mask: ServSelect IP Software, BootP, Telnet Command Line Interface (CLI) or the serial CLI on port 1.

These methods work as documented on most Windows® and UNIX® systems; however, the actual implementation on your system may differ from the instructions provided. Refer to your system administrator guide, or use ServSelect IP Software to simplify SCPS configuration.

To configure the IP address and subnet mask using ServSelect IP Software:

Using the ServSelect IP Software installation wizard is the easiest method to configure the SCPS IP address and subnet mask. See the ServSelect IP Software Installer/User Guide for instructions. After the IP address and subnet mask are configured, see *Initial SCPS login* in this chapter.

To configure the IP address and subnet mask using BootP:

1. Ensure that there is a BootP server on your network that is configured to correctly respond to a BootP request from the SCPS. BootP servers require the Ethernet MAC address of network devices. The SCPS Ethernet MAC address is located on the back of the unit. See your BootP server's system administrator guide for information about configuring the BootP server.

2. After you have configured your network's BootP server with the SCPS Ethernet MAC address, IP address and subnet mask, restore power to the SCPS and wait for the *ONLINE* LED to illuminate. Once this occurs, the SCPS has completed the BootP protocol, obtained its IP address and subnet mask and stored these in FLASH.

3. You may verify that the BootP process was successful with a ping command, which tests network connectivity. The ping command is entered as:

   ```
   ping <ip_address>
   ```

   For example, the following command tests the network connectivity of an SCPS with the IP address 192.168.0.5.

   ```
   ping 192.168.0.5
   ```

4. If the SCPS completes the BootP successfully, you will see a display similar to the following.

   ```
   Pinging 192.168.0.5 with 32 bytes of data:
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   ```

```
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
```

If the SCPS did not successfully obtain its IP address with the BootP protocol, you will see a display similar to the following.

```
Pinging 192.168.0.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

In this case, check the MAC address and IP address provided to the BootP server to confirm they are correct. Verify that the Ethernet LAN adaptor cable is correctly installed on the SCPS and the Ethernet hub.

After the IP address is configured successfully, launch a Telnet session to the SCPS IP address. Then, see *Initial SCPS login* in this chapter.

To configure the IP address and subnet mask using a Telnet CLI:

1. Ensure that your server or workstation has a Telnet client and is located on the same LAN segment as the SCPS.

2. Use the arp command to update the server or workstation with the SCPS IP address and Ethernet MAC address. The SCPS Ethernet MAC address is located on the back panel above the LAN connector. The arp command is entered as:

   ```
   arp -s <ip_address> <mac_address>
   ```

   For example, the following command assigns the IP address 192.168.0.5 and the Ethernet MAC address 00-80-7d-54-01-54 to the SCPS.

   ```
   arp -s 192.168.0.5 00-80-7d-54-01-54
   ```

   On a UNIX platform, the MAC address may require colons (:) instead of dashes (-), for example, 00:80:7d:54:01:54.

3. You may verify that you entered the information correctly by using an arp command with the -a option.

   ```
   arp -a
   ```

   This command shows all arp entries for the server or workstation. See your system administrator guide if you need additional help with the arp command.

4. After the above arp command is entered correctly, launch a Telnet client to the assigned IP address. Then, continue with *Initial SCPS login* in this chapter.

To configure the SCPS using the serial CLI:

1. By factory default, port 1 of the SCPS is configured for the serial CLI. To access the serial CLI, attach a compatible device to port 1. The compatible device types are: ASCII, VT52, VT100, VT102, VT220 and VT320.

   Chapter 8 lists the required cables and adaptors. You may also use any terminal emulation program that is available on your system.

2. Configure your terminal or terminal emulation program as follows.

Baud rate	9600
Bits per character	8
Parity	None
Stop bits	1
Flow control	None

3. Press the **Return** or **Enter** key until a prompt appears, requesting your username. If you do not receive a prompt after pressing the key five times, check your cable and serial settings to be sure that they are correct.

4. Proceed to *Initial SCPS login* in this chapter.

After you complete the SCPS configuration, you may reconfigure the CLI on another port or disable it completely and use port 1 with an attached device. For more information, see *Connecting to devices from the serial CLI port* in Chapter 4.

Initial SCPS login

The SCPS ships with a single user defined in its user database. The first time you connect to the SCPS via Telnet or serial CLI, you are prompted for a username.

To log in to the SCPS for the first time:

1. At the Username prompt, type **Admin**. There is no factory default password for the Admin user. At the Password prompt, press **Return**.

   ```
   Username: Admin
   Password:
   Authentication Complete
   SCPS configuration is required.
   ```

2. Once authentication completes, the SCPS prompts for any missing configuration values that are required for operation.

   If you already provided the IP address and subnet mask, you will not be prompted for those values again.

If you have not already provided the IP address and subnet mask, you will be prompted for them. Enter the SCPS IP address and subnet mask using standard dot notation.

```
SCPS configuration is required
Enter SCPS IP address > 192.168.0.5
Enter SCPS Subnet mask > 255.255.255.0
```

3. You are prompted for a new Admin password. Passwords are case sensitive and must contain 3-16 alphanumeric characters. You must enter the new password twice to confirm that you entered it correctly.

```
Enter SCPS New Admin Password > *****
Confirm New Admin Password > *****
```

After you have provided the required configuration information, a confirmation message appears while the SCPS stores the values in its configuration database.

You have now completed the initial login, and you may enter additional commands at the CLI prompt (>). To configure SCPS ports, see *Configuring Serial Port Settings* in Chapter 4.

3.4 Reinitializing the SCPS

Reinitializing the SCPS removes configured information. This may be useful when reinstalling the SCPS at another location in your network.

The SCPS stores configuration information in FLASH databases. During reinitialization, the FLASH erase has two phases. The first phase erases the SCPS configuration database, which contains all nonvolatile data except the IP address. The second phase erases the IP address and restores the SCPS to its factory default settings.

To reinitialize the SCPS:

1. Locate the recessed INIT button on the front of the SCPS. You will need a tool that fits inside the recess, such as an opened paper clip.

2. Insert the tool in the recess, then depress and hold the button. The *ONLINE* LED will blink, indicating an SCPS initialization has been requested. You have approximately seven seconds to release the button before any action is taken.

   After seven seconds, the *ONLINE* LED will blink more rapidly to confirm that the SCPS configuration database has been erased. Continuing to hold the INIT button for a few more seconds will erase the IP address as well. The *ONLINE* LED will blink faster to confirm the deletion.

If any portion of FLASH is erased, the SCPS reboots when the INIT button is released.

4. Operations

4.1 Overview

The SCPS and its ports may be easily configured and managed to meet your requirements for device connection, user authentication, access control, power status monitoring, port history information display and SNMP compliance for use with third party network management products.

4.2 Configuring Serial Port Settings

By default, SCPS ports are configured with the following settings.

Target device	Console
Name	xx-xx-xx Pn (last 3 octets of MAC address plus the port number)
Baud rate	9600
Bits per character	8
Parity	None
Stop bits	1
Flow control	None
Time-out	15 minutes
CLI access character	Use Server CLI setting (^D)
Power	None

Most of these settings are standard serial port operating characteristics.

The CLI access character parameter specifies how you access the CLI. For more information, see *Telnet CLI mode* in this chapter.

The Power parameter instructs the SCPS to monitor the state of a specified control signal. Signal transitions may be configured to trigger SNMP alerts. The parameter value indicates an inbound control signal (CTS, DCD or DSR) and the state of that signal (low or high). When the defined signal is true, the SCPS interprets it as a power on condition for the attached device; when the signal is false, a power off condition for the device is assumed. The signal specified for flow control cannot be used for power control, and vice versa.

To configure serial console port settings:

Issue a Port Set command. You may specify settings for one or all ports.

PORT [<*port*>|ALL] SET [NAME=<*name*>] [BAUD=<*baud*>]
[SIZE=<*size*>] [PARITY=<*parity*>] [STOP=<*stop_bits*>]
[FLOW=<*flow_ctrl*>] [TIMEOUT=<*time-out*>] [SOCKET=<*socket*>]
[CHAR=^<*cli_char*>] [TOGGLE=NONE|DTR] [POWER=<*signal*>]

For more information and descriptions of all valid parameters, see *Port Set command* in Chapter 6.

To display serial port settings:

Issue a Show Port command.

```
SHOW PORT [<port>|ALL|NAMES]
```

When you request information about a port, the display includes configuration information, current power status (if power status monitoring has been enabled), plus transmit, receive and error counts. When you request information about a single port and a user is currently accessing that port, the display also includes the username, access rights and other information about the current session.

When you request information about port names, the display includes the port numbers and names. If a port's name has not been changed with a Port Set command, the logical name is displayed.

For more information, see *Show Port command* in Chapter 6.

4.3 Connecting to Serial Devices

The SCPS offers several methods for connecting to attached serial devices: Telnet, serial CLI, PPP and SSH.

Preemption

Depending on configured access levels, a user who is connecting to a port (the connecting user) may disconnect another user of equal or lower access (the current user).

If the connecting user's access level is lower than the current user's access level, the connecting user will receive an *In Use* message and the connection will be dropped.

If the connecting user's access level is equal to or higher than the owning user's access level, an *In Use by owning user* message will be displayed. The connecting user may then choose to preempt the current user's session. If the current user's session is preempted, an appropriate message is displayed.

For more information about access levels, see *Access rights and levels* in this chapter.

Connecting to devices using Telnet

Each SCPS serial port is directly addressable through a unique TCP port number that provides a connection to the attached serial device.

Plain text (non-encrypted) Telnet connections are enabled by default. For information about enabling both plain text Telnet and SSH connections, see *Enabling plain text Telnet and SSH connections* in this chapter.

To connect to a device using Telnet:

Type **telnet,** followed by the SCPS IP address and the appropriate TCP port number, which by default is 3000 plus the physical port number, in decimal format. (The TCP port number may be changed for any SCPS port.)

For example, the following Telnet command connects to the serial device attached to physical port 14 of an SCPS-16.

```
    telnet 192.168.0.5 3014
```

If an authentication method other than None has been configured for the SCPS, you will be prompted for credentials (username and password). Once authentication completes, your connection is confirmed. When you successfully connect to the serial device, you will see a display similar to the following.

```
    Username: Myname
    Password: ******
    Authentication Complete
    Connected to Port: 14 9600,8,N,1,XON/XOFF
```

If the authentication method is configured as None, you may Telnet and connect to a serial device without entering credentials; however, credentials are always required when connecting to the SCPS CLI.

Data entered at the Telnet client is written to the attached serial device. Any data received by the SCPS from the serial device is output to your Telnet client.

A cross-platform Telnet client is bundled with the ServSelect IP Software application. Third-party Telnet client applications may be used in combination with ServSelect IP Software or standalone.

You may connect using either SSH (ServSelect IP Software provides built-in support for SSH2) or plain text.

ServSelect IP Software Telnet

ServSelect IP Software is a cross-platform client application provided with each SCPS. ServSelect IP Software provides a convenient way to select an SCPS or attached device and launch a Telnet session to manage it.

ServSelect IP Software includes a built-in Serial Console Viewer Telnet application that offers several features not found in other Telnet clients. For maximum flexibility, ServSelect IP Software allows you to associate a unique Telnet client with each SCPS port.

You may specify the built-in Telnet client or a third party Telnet client. The ServSelect IP Software can provide an SSH2 tunnel for use with the specified third party Telnet client. For more information, see the ServSelect IP Software Installer/ User Guide.

Standalone third party Telnet clients

You may use third party Telnet clients to access the SCPS directly without ServSelect IP Software.

Connecting to devices from the serial CLI port

By factory default, port 1 of the SCPS is configured with the serial CLI, which prohibits the use of port 1 with an attached serial device. You may configure the CLI on a different port, but only one port may be configured as the serial CLI port at one time. For example, when you enable the CLI interface on port n, and it is already active on port p, then the CLI will automatically be disabled on port p.

You may connect to one serial device at a time through the serial CLI port using a local terminal or a local PC using a terminal emulation program. If you connect an external modem to the serial CLI port, you may also access devices through a remote terminal or PC that can dial into the SCPS external modem. For information about modem connections, see *Configuring and using dial-in connections* in this chapter and *Server CLI command* in Chapter 6.

To configure a port for the serial CLI:

1. Issue a Server CLI command, using the Port parameter to specify the CLI port and the Type parameter to specify the terminal type.

   SERVER CLI PORT=<*port*> TYPE=<*type*>

2. To disable the CLI that was previously configured on a port, issue a Server CLI command, indicating Type=Off.

For more information, see *Server CLI command* in Chapter 6.

To display CLI port information:

Issue a Show Server CLI command.

```
SHOW SERVER CLI
```

The display includes the CLI port number and terminal type, plus the CLI access character. For more information, see *Show Server CLI command* in Chapter 6.

To connect to a device from the serial CLI port:

1. Issue a Server CLI command, using the Connect parameter to enable the use of the Connect command from the serial CLI port.

   SERVER CLI CONNECT=ON

2. Issue a Connect command to the desired port.

   CONNECT <*port*>

3. To end a device session that was initiated with a Connect command, issue a Disconnect command.

   DISCONNECT

For more information, see *Server CLI command*, *Connect Command* and *Disconnect Command* in Chapter 6.

Configuring and using dial-in connections

You may attach an external modem to the serial CLI port for dial-in serial CLI access to the SCPS. This may be used as a backup connection if the unit is not accessible from the network. It may also be used as a primary connection at remote sites that do not have Ethernet network capability. The modem must be Hayes compatible.

To specify a modem initialization string:

1. Issue a Show Server CLI command to ensure that the port where the modem is connected has been defined as the serial CLI port.

   SHOW SERVER CLI

2. Issue a Server CLI command, using the Modeminit parameter to specify the modem initialization string.

   SERVER CLI MODEMINIT="<*string*>"

   The string must be enclosed in quotes and must include at least the command settings ATV1 and SO=1, which cause the modem to issue verbose response strings and auto-answer the phone on the first ring. For more information, see *Server CLI command* in Chapter 6.

   The modem initialization string is sent to the cabled modem when any of the following conditions occur:

   - SCPS initialization
   - Detection of a transition of DSR from low to high
   - Completion of a call when DCD changes from high to low

3. Upon successful modem connection, press the **Enter** key until the login prompt appears.

To display modem configuration information:

Issue a Show Server CLI command.

```
SHOW SERVER CLI
```

For more information, see *Show Server CLI command* in Chapter 6.

Connecting to devices using PPP

The SCPS supports remote PPP access using an auto-answer modem that answers calls. A dial-in client and the SCPS establish the PPP protocol.

The PPP dial-in may be used to access a remote SCPS that does not warrant a WAN (Wide Area Network) link to the Ethernet interface. In this case, the PPP connection allows a remote PC with Telnet capability to dial the SCPS and then establish a Telnet connection to an SCPS port.

The PPP dial-in may also be used to access a subnet containing remote SCPS devices in the event of a WAN link failure. In this case, the PPP provides an alternate path to one or more remote SCPS devices.

Once the PPP connection is established, you must launch an application that connects to the SCPS or to one of its ports. The PPP connection is only a communications interface to the SCPS.

The SCPS implements a PPP server that uses CHAP (Challenge Authentication Protocol). Passwords are not accepted in the clear on PPP connections.

PPP is disabled by default.

To enable or disable a PPP server on the serial CLI port:

1. To enable a PPP server on the serial CLI port, issue a Show Server CLI command to ensure that a serial CLI port has been defined.

   ```
   SHOW SERVER CLI
   ```

2. Issue a Server PPP command with the Enable parameter.

   SERVER PPP ENABLE LOCALIP=<*local_ip*> REMOTEIP=<*rem_ip*> [MASK=<*subnet*>]

   You must specify local and remote IP addresses to be used for the SCPS and client ends of the PPP connection respectively. You are prompted to confirm or cancel the changes. Enter **Y** to confirm or **N** to cancel.

3. To disable a PPP server, issue a Server PPP command with the Disable parameter.

```
SERVER PPP DISABLE
```

For more information, see *Show Server CLI command* and *Server PPP command* in Chapter 6.

To display PPP configuration information:

Issue a Show Server PPP command.

```
SHOW SERVER PPP
```

For more information, see *Show Server PPP command* in Chapter 6.

Connecting to devices using SSH

The SCPS supports version 2 of the SSH protocol (SSH2). The SCPS SSH server operates on the standard SSH port 22. The shell for this connection provides a CLI prompt as if you had established a Telnet connection on port 23. The shell request for this connection is for CLI access.

Additional SCPS SSH servers operate on TCP ports that are numbered with values 100 greater than the standard 30xx Telnet ports for the SCPS. For example, if port 7 is configured for Telnet access on port 3007, then port 3107 will be a direct SSH connection for port 7. When SSH is enabled, Telnet port 23 connections will be accepted from other clients if the Server Security command includes Encrypt=SSH,None. Connecting to Telnet port 23, or any other Telnet port, may be tunneled through a connection to SSH port 22.

SSH server keys

When SSH is enabled for the first time, the SCPS generates an SSH server key. The key generation process may take up to ten minutes. The key is computed at random and is stored in the SCPS configuration database.

In most cases, the SSH server key should not be modified because most SSH clients will associate the key with the IP address of the SCPS. During the first connection to a new SSH server, the client will display the fingerprint of the SSH server key and prompt you to indicate if you wish to store it on the SSH client. After the first connection, most SSH clients will validate the key when connecting to the SCPS. This provides an extra layer of security because the SSH client can verify the key sent by the server each time it connects.

If you disable SSH and later reenable it, you may either use the existing server key or compute a new one. If you are reenabling the same server at the same IP address, it is recommended that you use the existing key, as SSH clients may be using it for verification. If you are moving the SCPS to another location and changing the IP address, you may wish to generate a new SSH server key.

Authenticating an SSH user

SSH is enabled and disabled with the Server SSH command. When you enable SSH, you may specify the authentication method(s) that will be used for SSH connections. The method may be a password, an SSH key or both. A user's password and SSH key are specified with a User Add or User Set command. All SSH keys must be RSA keys. DSA keys are not supported.

The following table lists and describes the valid SSH authentication methods that may be specified with a Server SSH command.

SSH Authentication Methods

Method	Description
PW (default)	SSH connections will be authenticated with a username/password. With this method, a user's definition must include a valid password in order for that user to authenticate an SSH session. A password may authenticate to a RADIUS server or to the local user database.
KEY	SSH connections will be authenticated with an SSH key. With this method, a user's definition must include valid SSH key information in order for that user to authenticate an SSH session. Key authentication is always local; RADIUS is not supported. For more information, see *SSH user keys* in this chapter.
PW|KEY or KEY|PW	SSH connections will be authenticated with either a username/password or an SSH key. If a user has only a password defined, that user must authenticate an SSH session with a username/password. If a user has only an SSH key defined, that user must authenticate an SSH session using the key. If a user has both a password and an SSH key defined, that user may use either a username/password or the SSH key to authenticate an SSH session. This method allows the SCPS administrator to define how each user will authenticate an SSH session based on information provided in the User Add/Set command. PW authentication will be local or RADIUS as specified in the Auth parameter of the Server Security command. Key authentication is always local.
PW&KEY or KEY&PW	SSH connections will be authenticated using both a username/password and an SSH key. With this method, a user's definition must include a password and SSH key information for that user to authenticate an SSH session. PW authentication will be local or RADIUS as specified in the Auth parameter of the Server Security command. Key authentication is always local.

A user’s access rights are determined from the authentication method used. SSH key authentication always uses the access rights from the local user database. Depending on the server authentication mode specified with the Server Security command, SSH password authentication will use either the access rights from the local user database or the values returned by the RADIUS server.

With either of the “or” methods (PW|KEY and KEY|PW), the user access rights are determined from the method used to authenticate the user.

With either of the “and” methods (PW&KEY and KEY&PW), the user access rights are determined from the first method specified. If PW&KEY is specified, the access rights from the password authentication will be used. If KEY&PW is specified, the access rights from the key authentication will be used.

For more information, see *Using Authentication Modes* in this chapter.

SSH user keys

A user’s SSH key is specified in a User Add or User Set command. You may define a key even if SSH is not currently enabled. The key may be specified in one of two ways:

- When using the SSHKEY and FTPIP keyword pair to define the network location of a user’s SSH key file, the SSHKEY parameter specifies the name of the uuencoded (UNIX to UNIX encoded) public key file on an FTP server. The maximum file size that can be received is 4K bytes. The FTPIP parameter specifies the FTP server’s IP address.

  When this method is specified, the SCPS initiates an FTP client request to the specified IP address. The SCPS then prompts the user for an FTP username and password for connection. When connected, the SCPS will GET the specified key file and the FTP connection will be closed. The SCPS then stores the SSH key with the username in the SCPS user database.

- When using the KEY keyword to specify the SSH key, the KEY parameter specifies the actual uuencoded SSH key. This is for configurations that do not implement an FTP server. The SCPS stores the specified key in the SCPS user database.

The SCPS processes a uuencoded SSH2 public key file with the format described in the IETF document draft-ietf-secshpublickeyfile-02. The key must follow all format requirements. The UNIX ssh-keygen2 generates this file format. The SCPS also processes a uuencoded SSH1 public key file. The UNIX ssh-keygen generates this file format.

You may also generate SSH user keys via ServSelect IP Software. See the ServSelect IP Software Installer/User Guide.

To enable SSH session access to the SCPS:

1. Issue a Show Server Security command to ensure that you are using an authentication method other than None.

   ```
   SHOW SERVER SECURITY
   ```

2. Issue a Server SSH command with the Enable parameter. You may also specify an authentication method.

   SERVER SSH ENABLE AUTH=<*auth*>

   If an authentication method is not specified, the previous authentication parameter will be used. The default value is AUTH=PW.

3. If you are enabling SSH for the first time, you are advised that all other SCPS sessions will be terminated. Enter **Y** to continue or **N** to cancel.

4. If you are reenabling SSH, you are prompted to use the existing SSH server key or generate a new key. Enter **Y** to use the existing key or **N** to generate a new key.

For more information, see *Server SSH command* in Chapter 6.

To disable SSH session access to the SCPS:

Issue a Server SSH command with the Disable parameter.

```
SERVER SSH DISABLE
```

When SSH is disabled, the SCPS operates in plain text mode.

To display SSH information:

Issue a Show Server Security command.

```
SHOW SERVER SECURITY
```

If SSH is enabled, the display will include SSH2. Regardless of whether SSH is enabled, the display will indicate the authentication method that was specified with the Server SSH command.

Enabling plain text Telnet and SSH connections

Plain text (non-encrypted) Telnet connections are enabled by default.

If you enable SSH connections using the Server Security command and the Encrypt=SSH parameter, plain text Telnet connections will be disabled. However, if you enable SSH connections with the Server SSH command, both plain text and SSH connections will be allowed.

To enable both Telnet and SSH connections:

Issue a Server Security command, indicating Encrypt=SSH,None.

Telnet CLI mode

While you are connected to an attached serial device, you may enter CLI mode and enter SCPS commands.

To enter or exit CLI mode when connected to a serial device:

1. To enter CLI mode, type the CLI access character, which is **Ctrl-D** by default. At the CLI prompt (>), you may enter SCPS commands.
2. To exit CLI mode and return to the session with the attached device, issue a Resume command.

   RESUME

For more information, see *Resume Command* in Chapter 6.

To change the CLI access character:

Issue a Server CLI command or a Port Set command, using the Char parameter to specify the CLI access character.

SERVER CLI CHAR=^<*char*>
- or -
PORT SET CHAR=^<*char*>

If you issue a Port Set command with Char=None, then the CLI access character specified in the Server CLI command will be used. The Port Set command may be used to override the Server CLI access character on a per-port basis. For more information, see *Server CLI command* and *Port Set command* in Chapter 6.

To display CLI access character information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* in Chapter 6.

Ending device sessions

To end your device session:

Enter CLI mode and issue a Quit command or a User Logout command.

QUIT

- or -

If you initiated the device session with a Connect command, enter CLI mode and issue a Disconnect command.

```
DISCONNECT
```

- or -

Allow the port to time-out due to inactivity. In this case, a notification message is issued and the serial CLI session returns to CLI mode. This time-out may occur while you are in CLI mode.

- or -

For modem connections, if a carrier drop occurs, the serial CLI session is automatically logged off.

Session time-outs

The SCPS monitors data traffic when you are connected to an attached serial device. You may specify a time-out value with the Server CLI command. You may also specify a time-out value for each port with the Port Set command. When no data is received from the connected user for the configured number of minutes, the connection is terminated.

The following time-out values are used:

- For a Telnet session, the Server CLI time-out value is used.
- For a serial port session, if the port's configured time-out value is Ø, the Server CLI time-out value is used, even if it is also Ø.
- For a serial port session, if the port's configured time-out value is non-Ø, that value is used.

4.4 Managing User Accounts

The SCPS user database may store information for up to 64 user accounts.

To add a user:

Issue a User Add command.

USER ADD <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>]
[FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>]

You must specify a username. You must also specify a password or SSH user key information, or you may specify both. You may also include an access level or access rights. For more information, see *Connecting to devices using SSH* and *Access rights and levels* in this chapter and *User Add command* in Chapter 6.

To change a user's configuration information:

Issue a User Set command.

USER SET <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>]

You may change your own password at any time. You must have USER access rights to change another user's password or to change any user's SSH user key information and access rights.

To remove an SSH user key or password, specify Key="" or Password="". You cannot remove both the password and the SSH key from a user's definition; one must remain in the user database. Also, you cannot remove a user's key or password if that removal would result in no valid users having USER access rights.

For more information, see *Connecting to devices using SSH* and *Access rights and levels* in this chapter and *User Set command* in Chapter 6.

To end another user's SCPS session:

Issue a User Logout command.

USER LOGOUT <*username*>

A message is sent and the Telnet or SSH connection is dropped. For more information, see *User Logout command* in Chapter 6.

To delete a user:

Issue a User Delete command.

USER DELETE <*username*>

If the specified user is currently logged in, a message is sent to the user indicating that access is no longer permitted, and the user's Telnet session is terminated. For more information, see *User Delete command* in Chapter 6.

To display user configuration information:

1. To display information about one user, issue a Show User command, specifying the username.

   SHOW USER <*username*>

2. To display information about all users, issue a Show User command with the All parameter.

    SHOW USER ALL

For more information, see *Show User command* in Chapter 6.

Access rights and levels

Most SCPS commands require the user to have access rights to use the commands. The access rights for each SCPS command are listed in Chapter 5. The following table describes the access rights a user may be given.

Access Rights

Access Right	Description
PCON	The Port Configuration access right should be given to users who must modify port settings. Grant PCON access rights only to users who need to issue the Port Set command.
SCON	The Server Configuration access right should be given to users who must change the SCPS configurations, including setting the IP address and updating the SCPS program load in FLASH. Grant SCON access only to users who need to administer the SCPS.
SMON	The Server Monitor access right should be given to users who need to view SCPS status and monitor serial port activity. Grant SMON access only to users who need to assist other users in accessing attached serial devices.
USER	The User access right should be given to users who need to modify the user database. Grant USER access only to users who must add, change or delete user accounts. At least one user must have USER access rights; otherwise, the user database cannot be changed.
BREAK	The Break access right allows users to send a serial break sequence to the attached serial device. On certain devices, this sequence has a special meaning. Grant BREAK access only to users who need to use the Port Break command.
P	The Port access right gives users access to one or more serial ports. This confers the right to access that serial port and connect to the attached serial device. You may grant Port access rights to specific ports (Pn), a range of ports (Px-y) or all ports (PALL).

The Admin user is preconfigured in the user database with all access rights.

Access levels

When you specify a user's access rights, you may either specify the individual rights or you may use a shortcut that specifies an access level. The APPLIANCEADMIN and ADMIN levels (which are used in ServSelect IP Software in lieu of individual specifications other than port access rights) are equivalent to the following individual specifications:

- The APPLIANCEADMIN level is equivalent to PALL, USER, SCON, SMON, PCON and BREAK.
- The ADMIN level is equivalent to PALL, USER, SMON, PCON and BREAK.

A user's access level may be used for preemption. For example, assume User A is connected to a port. User B tries to connect to the same port. If User B has an access level equal to or greater than User A's access level, then User B will be given the option of preempting User A.

To manage a user's access rights/level:

1. To configure a user's access rights/level, issue a User Add command, using the Access parameter to specify the rights or a level.

   USER ADD <*username*> ACCESS=<*access*>

2. To change a user's access rights/level, issue a User Set command, using the Access parameter to specify the rights or a level.

   USER SET <*username*> ACCESS=<*access*>

3. To display the access rights and level for one or all users, issue a Show User command.

   SHOW USER <*username*>|ALL

For more information, see *Managing User Accounts* in this chapter, plus *User Add command*, *User Set command* and *Show User command* in Chapter 6.

4.5 Using Authentication Modes

The SCPS supports several methods for authenticating users: RADIUS, local and none. Multiple connection and authentication methods may operate concurrently. By default, authentication is done at the local SCPS user database.

Local authentication

Local authentication uses the SCPS internal user database to authenticate users.

RADIUS authentication

RADIUS authentication uses an external third party RADIUS server containing a user database to authenticate SCPS users. The SCPS, functioning as a RADIUS client, sends usernames and passwords to the RADIUS server. If a username and password do not agree with equivalent information on the RADIUS server, the SCPS is informed and the user is denied SCPS access. If the username and password are successfully validated on the RADIUS server, the RADIUS server returns an attribute that indicates the access rights defined for that username.

To use RADIUS authentication, you must specify information about the primary RADIUS server and optionally, a secondary RADIUS server to be used as a backup.

The RADIUS server definition values specified in SCPS commands must match corresponding values configured on the RADIUS server. On the RADIUS server, you must include SCPS-specific information: the list of valid users and their access rights for the SCPS. Each user-rights attribute in the RADIUS server's dictionary must be specified as a string containing the user's access rights for the SCPS, exactly matching the syntax used in the SCPS User Add command.

Consult your RADIUS administrator's manual for information about specifying users and their attributes. The exact process depends on the RADIUS server you are using.

No authentication

When authentication is disabled, users are not authenticated. Telnet sessions to serial ports are accepted immediately, and users are not prompted for a username or password. In this case, users are granted access only to the port to which they are connected, including Break access.

Connections to the Telnet port (23), serial CLI and PPP are still authenticated, even when authentication is expressly disabled. Generally, these communications paths are used only by administrators, and authentication is enforced in order to establish appropriate access rights.

Authentication may not be disabled when SSH session access is enabled.

Authentication summary

The SCPS allows concurrent use of multiple authentication modes. This allows Telnet and SSH clients to all access a single SCPS as long as the appropriate values are enabled.

You may optionally specify both RADIUS and local authentication, in either order. In this case, authentication will be attempted initially on the first method specified. If that fails, the second method will be used for authentication.

For example, if you enable local and RADIUS authentication (in that order), authentication uses the SCPS user database. If that fails, authentication goes to the defined RADIUS servers. If you enable RADIUS and local authentication (in that order), authentication goes first to the defined RADIUS servers. If that fails, the local user database is used.

To specify the authentication mode:

1. For RADIUS authentication, issue a Server RADIUS command.

   SERVER RADIUS PRIMARY|SECONDARY IP=<*radius_ip*>
   SECRET=<*secret*> USER-RIGHTS=<*attr*> [AUTHPORT=<*udp*>]
   [TIMEOUT=<*time-out*>] [RETRIES=<*retry*>]

   You must specify the server’s IP address, the UDP port to be used and a “secret” to be used. You must also specify a user-rights attribute value that matches a value in the RADIUS server’s dictionary.

   You may also use this command to delete a RADIUS server definition.

   SERVER RADIUS PRIMARY|SECONDARY DELETE

   For more information, see *Server RADIUS command* in Chapter 6.

2. Issue a Server Security command, using the Authentication parameter to specify the authentication mode. Use the Encrypt parameter to enable plain text Telnet connections, SSH connections or both.

   SERVER SECURITY AUTHENTICATION=<*auth_mode*>
   ENCRYPT=<*conns*>

3. You are prompted to save the information. Enter **Y** to confirm or **N** to cancel.

To display authentication configuration information:

1. Issue a Show Server Security command.

   SHOW SERVER SECURITY

   The display includes the current SCPS authentication settings that were configured with the Server Security command. If SSH access has been enabled, the display indicates SSH2. Regardless of whether SSH is enabled, the display includes the authentication method specified with the Server SSH command.

2. To display SCPS RADIUS settings that were configured with the Server RADIUS command, issue a Show Server RADIUS command.

SHOW SERVER RADIUS

For more information, see *Server Security command, Show Server Security command* and *Show Server RADIUS command* in Chapter 6, plus *Connecting to devices using SSH* and *Enabling plain text Telnet and SSH connections* in this chapter.

4.6 Using Security Lock-out

When the Security Lock-out feature is enabled, a user will be locked-out after five consecutive authentication failures. A successful authentication will reset the counter to zero. You may configure a lock-out period of from 1-99 hours. Specifying a lock-out period of zero disables the feature; that is, users will not be locked-out.

A locked-out user will remain locked-out until the specified time elapses, the SCPS is power-cycled or the user is unlocked by an administrator with the User Unlock command.

A user with the ADMIN access level may unlock all users except a user with the APPLIANCEADMIN level. A user with the APPLIANCEADMIN level may unlock all users.

To enable or disable Security Lock-out:

1. To enable Security Lock-out, issue a Server Security command, using the Lockout parameter with a value between 1-99.
2. To disable Security Lock-out, issue a Server Security command, using the Lockout=Ø parameter.

To unlock a locked-out user:

Issue a User Unlock command with the username.

4.7 Managing the Port History Buffer

Each SCPS serial port has a circular history buffer that contains the latest 64K bytes of data received from the attached serial device. This information may be helpful in analyzing attached device anomalies.

The history buffer begins filling with received data upon completion of SCPS initialization, even if no user is connected. When you connect to a serial port, the data that was received from the attached serial device prior to the connection is available in the buffer. Once online, new data continues to be stored in the buffer. You may choose whether to display the history buffer’s content automatically when you connect and whether to keep or discard the history buffer’s content at the end of a session.

When more than 64K bytes of data are sent to the history buffer, data at the top of the buffer is discarded to make room for the new data. As a result, the buffer always contains the most recent 64K bytes of port history.

Using port history mode commands

Once you issue a Port History command to enter port history mode, you may issue the commands listed in the following table. Only the first letter of the command is required.

Port History Mode Commands

Command	Description
Bottom	**B** sets the view location to the bottom of the file minus 23 history display lines, if available.
Clear	**C** clears the port history buffer.
Next	**N** increments the current history display line by the number of lines per page and outputs a new history display page.
Prev	**P** decrements the current history display line by the number of lines per page and outputs a new history display page.
Quit	**Q** returns to the normal CLI.
Resume	**R** leaves port history mode and CLI mode and resumes the session with the attached serial device. This single command is equivalent to sequentially using the Quit and Resume commands.
Search	**S** searches the port history buffer for a specified text string. Search strings with embedded spaces must be enclosed in quotes. By default, the search is case sensitive. To ignore case, enter **-i** before the string. To specify direction, type **-u** to search up from the current line toward the top of the buffer or **-d** to search down from the current line toward the bottom of the buffer. The search direction remains in effect for subsequent searches until you change the search direction. If the string is found, the current history display line is set to the line containing the string, and the SCPS outputs a history display page. If the string is not found, an error message is displayed, no other information is output and the current history display line is not changed. Entering the Search command with no parameters searches again for the previous string in the same direction as the previous search.
Top	**T** sets the current history display line to one and outputs a history display page.

The following examples assume the user is in port history mode.

The following command searches the history buffer in the upward direction for the Abort Process string.

```
PORT HISTORY> s -u “Abort Process”
```

The following command searches the history buffer for the Process string, ignoring case.

```
PORT HISTORY> s -i Process
```

For more information, see *Server CLI command* and *Port History command* in Chapter 6.

To access port history mode:

Issue a Port History command.

```
PORT HISTORY
```

The PORT HISTORY > prompt appears.

To control the port history buffer display when you connect:

Issue a Server CLI command, using the History parameter to specify the Hold or Auto option:

```
SERVER CLI HISTORY=HOLD|AUTO
```

- If Hold is specified, the number of bytes in the history buffer is displayed, but none of the history data is output. In this case, you must access the CLI and use the Port History command to view the port’s history buffer content. This is the default mode.
- If Auto is specified, the number of bytes in the history buffer is displayed and the entire content of the buffer is output to the Telnet session. In this mode, the history buffer’s content may be reviewed in the Telnet client’s scrolling window. You may also use the Port History command to view the port’s history buffer content.

To control the port history buffer content when you end a session:

Issue a Server CLI command, using the History parameter to specify the Clear or Keep option:

```
SERVER CLI HISTORY=CLEAR|KEEP
```

- If Clear is specified, the port history buffer is cleared and all data is discarded at the end of a session.

- If Keep is specified, the port history buffer's content is retained at the end of a session.

To clear and discard all data in a port history buffer:

Issue a Clear command while you are in port history mode.

```
CLEAR
```

- or -

Issue a Server CLI command, indicating History=Clear.

```
SERVER CLI HISTORY=CLEAR
```

In this case, the port's history buffer is cleared at the end of each device session.

4.8 Managing the SCPS Using SNMP

The SCPS provides a set of commands that create and manage SNMP structures for use by third party network management products. These commands cover the following operations:

- Enabling and disabling SNMP UDP port 161 SNMP processing
- Defining read, write and trap community names
- Defining and deleting up to four SNMP management entity IP addresses
- Enabling and disabling SNMP traps
- Defining and deleting up to four trap destination IP addresses
- Defining, copying and deleting up to ten alert strings for each port

SNMP is disabled by default.

To enable or disable SNMP processing:

1. To enable SNMP processing, issue a Server SNMP command with the Enable parameter. This is the default setting.

   ```
   SERVER SNMP ENABLE
   ```

2. To disable SNMP processing, issue a Server SNMP command with the Disable parameter.

   ```
   SERVER SNMP DISABLE
   ```

For more information, see *Server SNMP command* in Chapter 6.

To specify SNMP community names:

Issue a Server SNMP Community command, using the Readcomm, Writecomm and Trapcomm parameters to specify community names.

NOTE:
The default community names are “public”; if you enable SNMP, you are encouraged to change the community values to prevent access to the MIB.

```
SERVER SNMP COMMUNITY READCOMM=<name>
WRITECOMM=<name> TRAPCOMM=<name>
```

Although all three community names default to public, if you specify a trap community name with this command, it must be different from the read and write community names.

For more information, see *Server SNMP Community command* in Chapter 6.

To add or delete SNMP management entity addresses:

1. To add an SNMP management entity address, issue a Server SNMP Manager command with the Add parameter and the management entity’s IP address. You may define up to four SNMP management entity addresses, using separate commands.

   ```
   SERVER SNMP MANAGER ADD <ip_address>
   ```

   When you define at least one SNMP manager, SNMP requests are processed if they are from one of the defined SNMP managers. If a request is not from one of the defined SNMP managers, the SNMP request is discarded.

2. To delete an SNMP management entity address, issue a Server SNMP Manager command with the Delete parameter and the management entity’s IP address.

   ```
   SERVER SNMP MANAGER DELETE <ip_address>
   ```

If no management entities are defined, any SNMP manager may access the MIB. For more information, see *Server SNMP Manager command* in Chapter 6.

To enable or disable SNMP traps:

1. To enable SNMP traps, issue a Server SNMP Trap command with the Enable parameter.

   ```
   SERVER SNMP TRAP ENABLE
   ```

   The SCPS will display a numbered list of traps that are currently disabled with a prompt requesting you to select trap(s) to enable. Indicate the traps to be enabled by entering a trap’s list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with

commas and dashes. To enable all traps, type **ALL**. To cancel the command, press **Enter**.
- or -
To enable all SNMP traps, issue a Server SNMP Trap command with the Enable and All parameters. In this case, the numbered list is not displayed.

```
SERVER SNMP TRAP ENABLE ALL
```

2. To disable SNMP traps, issue a Server SNMP Trap command with the Disable parameter.

   ```
   SERVER SNMP TRAP DISABLE
   ```

   The SCPS will display a numbered list of traps that are currently enabled with a prompt requesting you to select trap(s) to disable. Indicate the traps to be disabled by entering a trap's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To disable all traps, type **ALL**. To cancel the command, press **Enter**.
   - or -
   To disable all SNMP traps, issue a Server SNMP Trap command with the Disable and All parameters. In this case, the numbered list is not displayed.

   ```
   SERVER SNMP TRAP DISABLE ALL
   ```

For more information, see *Server SNMP Trap command* in Chapter 6. The supported traps are listed in Chapter 7.

To add or delete SNMP trap destination addresses:

1. To add an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Add parameter and the destination's IP address. You may define up to four destination addresses, using separate commands.

   SERVER SNMP TRAP DESTINATION ADD <*ip_address*>

2. To delete an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Delete parameter and the destination's IP address.

   SERVER SNMP TRAP DESTINATION DELETE <*ip_address*>

For more information, see *Server SNMP Trap Destination command* in Chapter 6.

To add, copy or delete port alert strings:

1. To add a port alert string, issue a Port Alert Add command, specifying the port number and a 3-32 character string. You may define up to ten strings for each port, using separate commands. The alert string will only generate a trap if the portAlert trap is enabled with a Server SNMP Trap command.

PORT <*port*> ALERT ADD "<*string*>"

2. To delete a port alert string, issue a Port Alert Delete command, specifying a port number.

   PORT <*port*> ALERT DELETE

   The SCPS displays a numbered list of alert strings that have been defined for the specified port with a prompt requesting you to select alert string(s) to delete. Indicate the alert strings to be deleted by entering an alert string's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To delete all alert strings, type **ALL**. To cancel the command, press **Enter**.

3. To copy the defined alert strings from one port to another port, issue a Port Alert Copy command, specifying the port numbers to be copied to and from.

   PORT <*to_port*> ALERT COPY <*from_port*>

   At the confirmation prompt, press **Y** to confirm or **N** to cancel. When the copy operation occurs, all previously defined strings on the port to which you are copying will be replaced.

For more information, see *Port Alert Add command*, *Port Alert Copy command* and *Port Alert Delete command* in Chapter 6.

To display SNMP configuration information:

Issue a Show Server SNMP command.

SHOW SERVER SNMP

The display includes information specified with the Server SNMP, Server SNMP Community, Server SNMP Manager, Server SNMP Trap and Server SNMP Trap Destination commands.

For more information, see *Show Server SNMP command* in Chapter 6.

To display port alert string information:

Issue a Show Port Alert command, specifying a port number.

SHOW PORT <*port*> ALERT

The display lists all the port's defined alert strings.

For more information, see *Show Port Alert command* in Chapter 6.

5. Using SCPS Commands

5.1 Accessing the CLI

You may access the CLI in three ways: using the Telnet CLI, using the serial CLI or entering the CLI access character during a session to a serial device. When the CLI is accessed, its prompt appears (>), indicating you may type a command.

5.2 Entering Commands

At the command prompt, type a command and then press **Return** or **Enter**. When the key is pressed, the command line comprises all characters to the left of the cursor. The character at the cursor and any characters to the right of the cursor are ignored. The following table lists the line editing operations for VT100 compatible devices.

Line Editing Operations for VT100 Compatible Devices

Operation	Action
Backspace	The character immediately before the cursor is erased and all text at and to the right of the cursor moves one character to the left.
Left Arrow	If the cursor is not at the beginning of the line, the cursor moves one character to the left. If the cursor is at the beginning of the line, no action is taken.
Right Arrow	If the cursor is not at the end of the line, the cursor moves one character to the right. If the cursor is at the end of the line, no action is taken.
Up Arrow	The CLI maintains a buffer containing the last 16 typed command lines. If there is a previous command line, it will be output as the current command line and may be edited. If there is no previous command line in the command line buffer, the command line is set to blanks and you may enter a new command.
Down Arrow	The next command in the CLI command line buffer is made available for edit. If there is no next command line, the command line is set to blanks and you may enter a new command.
Delete	The character at the cursor position is deleted and all characters to the right of the cursor position are moved left one character.

The following table lists the line editing operations for ASCII TTY devices. There is no command line buffer available on an ASCII TTY device.

Line Editing Operations for ASCII TTY Devices

Operation	Action
Backspace	Erases the last character typed.
Esc	Erases the current command line.

When commands take effect

Each command is completely processed before the next command may be entered. Some commands prompt for confirmation before they are processed. In these cases, you must confirm or cancel by entering **Y** or **N** respectively.

If you enter a Server FLASH command or if you change the SCPS IP address with a Server Set command, an SCPS reboot is required before the change becomes effective. In these cases, the SCPS database is updated when you enter the command and you are prompted that the change will not take effect until the SCPS reboots. You may choose to reboot at that time, or you may decline. When the SCPS reboots, your session and all other sessions on the SCPS are terminated.

5.3 Understanding Conventions

This section describes the parts of an SCPS command and the conventions used in this document to describe a command’s syntax.

Command syntax

A command may have four types of syntax: positional commands, positional parameters, keyword parameters and keyword values. The following examples demonstrate the syntax types.

The following Set Port command changes the baud rate and flow control settings for port 2.

```
    > PORT 2 SET BAUD=57600 FLOW=XONXOF
```

Command Syntax Types in Example Command

Value	Syntax
PORT	Positional command.
2	Positional parameter that indicates the port number for the command.
SET	Positional command that indicates port settings are to be changed.
BAUD	Keyword parameter, which is always followed by an equal (=) sign.
57600	Keyword value indicating the baud rate value for the BAUD keyword parameter.
FLOW	Keyword parameter, which is always followed by an equal (=) sign.
XONXOF	Keyword value.

Not every command will contain all syntax types. For example, the following command reboots the SCPS.

```
>SERVER REBOOT
```

In this case, both SERVER and REBOOT are positional commands.

In most cases, one or more spaces separate positional commands, positional parameters and keyword parameters.

For most positional commands, positional parameters or keyword parameters, you only need to enter the first three characters. The exceptions are:

- When you specify a terminal type with the Type parameter in the Server CLI command, you must enter all characters.
- When you specify an authentication method with the Auth parameter in the Server SSH command, you must enter all characters.
- When you specify control signal monitoring with the Power parameter in the Port Set command, you must enter all characters.

With the exception of usernames and passwords, commands are not case sensitive; they may be entered in uppercase, lowercase or a combination. For example, all of the following commands are correct.

```
> PORT 2 SET BAUD=57600 FLOW=XON
> POR 2 SET BAU=57600 FLOW=XON
> por 2 Set Baud=57600 flow=xon
> port 2 set baud=57600 flow=xon
```

NOTE:
Usernames and passwords are case sensitive. These values are stored exactly as you enter them. For example, the username “Ann” must be entered with an uppercase “A” and all other letters lowercase. The username “ANN” will not be accepted by the SCPS as the username “Ann.” Usernames and passwords must contain 3-16 alphanumeric characters.

Any syntax errors are displayed, and where applicable, the error is underlined.

In the following example, the keyword parameter “baud” is misspelled. Even if more than three characters are entered, they must all be correct.

```
> port 2 Set Baux=57600 flow=xon
             ----
ERR 26 - SET keyword parameter invalid
```

In the following example, the keyword value “576” is not valid. Numeric keyword values must be fully specified and may not be shortened to
three characters.

```
> POR 2 SET BAUD=576 FLOW=XON
                 ---
ERR 27 - SET keyword value invalid
```

In the following example, there are spaces between BAUD, the equal sign and the value 57600. Spaces are not permitted between keyword parameters and their values.

```
> POR 2 SET BAUD = 57600 FLOW=XON
            ------------
ERR 26 - SET keyword parameter invalid
```

Syntax conventions

This manual uses the following command syntax conventions:

- Brackets [ ] surround optional keywords and values.
- Angle brackets < > surround user-supplied positional parameters and keyword parameter values.
- In most cases, choices are separated by a vertical bar |. The description indicates if you may specify more than one of the choices and how to separate multiple values. The exception is the Server SSH command. In this case, the vertical bar is specified on the command line when you enable the “password or key” method (PW|KEY) or the “key or password” method (KEY|PW).

5.4 Command Summary

The following table lists the SCPS commands, including a brief description plus the required access rights and level.

SCPS Command Summary

Command	Description, Access Right and Access Level
Connect	Accesses devices from the serial CLI port. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN **
Disconnect	Ends a device session initiated with Connect command. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN **
Help	Displays information about commands. Access right: none needed Access level: all
Port Alert Add	Adds a port alert string. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Alert Copy	Copies a port’s alert strings to another port. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Alert Delete	Deletes one or more port alert strings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Break	Sends a break signal to the attached device. Access right: BREAK Access level: ADMIN or APPLIANCEADMIN
Port History	Accesses the port history buffer. Access right: none needed Access level: all
Port Logout	Terminates the SCPS session on a specified port. Access right: USER Access level: ADMIN or APPLIANCEADMIN
Port Set	Changes port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Quit	Terminates the current SCPS session. Access right: none needed Access level: all
Resume	Resumes device connection after being in CLI mode. Access right: none needed Access level: all

SCPS Command Summary (Continued)

Command	Description, Access Right and Access Level
Server CLI	Specifies the serial CLI port, port type and access character; enables/disables device connection from the CLI port; specifies a modem initialization string; specifies port history mode operations and a port time-out value. Access right: SCON Access level: APPLIANCEADMIN
Server FLASH	Updates the SCPS FLASH. Access right: SCON Access level: APPLIANCEADMIN
Server PPP	Enables/disables a PPP server on the serial CLI port. Access right: SCON Access level: APPLIANCEADMIN
Server RADIUS	Specifies RADIUS server parameters. Access right: SCON Access level: APPLIANCEADMIN
Server Reboot	Reboots the SCPS. Access right: SCON Access level: APPLIANCEADMIN
Server Security	Specifies user authentication mode, allowed access methods and security lock-out. Access right: SCON Access level: APPLIANCEADMIN
Server Set	Changes SCPS addresses. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP	Enables/disables UDP port 161 SNMP processing. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Community	Defines read, write and trap SNMP community strings. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Manager	Defines/deletes SNMP management entities. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Trap	Enables/disables SNMP traps. Access right: SCON Access level: APPLIANCEADMIN

SCPS Command Summary (Continued)

Command	Description, Access Right and Access Level
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps. Access right: SCON Access level: APPLIANCEADMIN
Server SSH	Enables/disables SSH session access to the SCPS and specifies the SSH authentication method. Access right: SCON Access level: APPLIANCEADMIN
Show Port	Displays port configuration information and statistics. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Port Alert	Displays a port's alert strings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server	Displays SCPS configuration, statistics and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server CLI	Displays information specified with the Server CLI command. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server PPP	Displays PPP settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server RADIUS	Displays RADIUS settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server Security	Displays authentication, encryption and lock-out settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server SNMP	Displays SNMP configuration information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show User	Displays user configuration and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
User Add	Adds a new user. Access right: USER Access level: ADMIN or APPLIANCEADMIN

SCPS Command Summary (Continued)

Command	Description, Access Right and Access Level
User Delete	Deletes a user. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Logout	Terminates a user's session. Access right: USER Access level: ADMIN*** or APPLIANCEADMIN
User Set	Changes a user's configuration information. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Unlock	Unlocks a locked-out user. Access right: USER Access level: ADMIN*** or APPLIANCEADMIN

** Users who do not have the ADMIN or APPLIANCEADMIN level must have the appropriate port access configured to issue this command.
*** A user with ADMIN level may issue a User Logout or User Unlock command for users with any level other than APPLIANCEADMIN.

6. SCPS Commands

6.1 Connect Command

The Connect command establishes a connection from the SCPS serial CLI port to a device attached to another port on that SCPS. If the specified port is already in use, you will receive an error message. To use this command, you must have previously issued a Server CLI command with the Connect=On parameter. For more information, see *Connecting to Serial Devices* in Chapter 6.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or others with access to port

Syntax

CONNECT <*port*>

Connect Command Parameter

Parameter	Description
<*port*>	Port number in range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.

Example

The following command establishes a connection from the serial CLI port to port 6.

```
> connect 6
```

6.2 Disconnect Command

The Disconnect command terminates a session with a serial device that was previously initiated with a Connect command. This command frees the attached serial device and allows other users to access it.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or others with access to port

Syntax

DISCONNECT

6.3 Help Command

The Help command displays information about SCPS commands.

Access right: none needed
Access level: none needed

Syntax

HELP [<*command_name*>]

Help Command Parameter

Parameter	Description
<command_name>	Command name. Default: Displays list of all commands

Examples

The following command displays information about the Show Server CLI command.

```
help sho ser cli
```

The following command displays a list of all commands.

```
help
```

6.4 Port Commands

The Port command has several forms, as listed in the following table.

Port Command Summary

Command	Description
Port Alert Add	Adds a port alert string to a specified port.
Port Alert Copy	Copies port alert strings from one port to another port.
Port Alert Delete	Deletes one or more port alert strings from a specified port.
Port Break	Sends a serial break signal to the attached device.
Port History	Accesses a port’s history mode.
Port Logout	Terminates the SCPS session on a specified port.
Port Set	Changes SCPS serial port settings for one or all ports.

Port Alert Add command

The Port Alert Add command adds a port alert string to a specified port. Each port may have up to ten port alert strings. Duplicate strings are not allowed on the same port. To generate a trap, the Server SNMP Trap command must be issued to enable the portAlert trap. For more information, see *Managing the SCPS Using SNMP* in Chapter 6.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT ADD "<*string*>"

Port Alert Add Command Parameters

Parameter	Description
<*port*>	Port number in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.
<*string*>	3-32 character string.

Port Alert Copy command

The Port Alert Copy command copies the alert strings from one port (from_port) to another (to_port). Any alert strings that were previously defined on the to_port will be deleted. When you enter this command, you are prompted to confirm or cancel the copy operation.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*to_port*> ALERT COPY <*from_port*>

Port Alert Copy Command Parameters

Parameter	Description
<*to_port*>	Port number where alert strings will be copied, in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.
<*from_port*>	Port number from which alert strings will be copied, in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.

Example

The following command copies the alert strings defined on port 1 to port 7, replacing any previously-defined alert strings on port 7.

```
port 7 alert copy 1
```

Port Alert Delete command

The Port Alert Delete command deletes one or more alert strings from a port. When you issue this command, a numbered list of defined alert strings is displayed, from which you choose those to be deleted. You may enter one or more numbers separated by commas, a range of numbers separated by a hyphen or type **ALL** to specify all strings. Pressing **Enter** cancels the command.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT DELETE

Port Alert Delete Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.

Example

The following command deletes defined alert strings from port 3.

```
> PORT 3 ALERT DELETE

Alert-strings assigned to port 3:
1) The first alert string
2) The second alert string
3) The third alert string
4) The fourth alert string

Select Alert-string(s) to delete>
```

The alert string numbers specified at the prompt will be deleted.

Port Break command

The Port Break command sends a serial break signal to the device to which you are attached.

Access right: BREAK
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT BREAK

Port History command

The Port History command accesses an SCPS serial port's history mode while you are attached to the port. When you are in history mode, the PORT HISTORY> prompt appears, and you may search the port's history buffer for specified strings.

For more information, see *Managing the Port History Buffer* in Chapter 4.

Access right: none needed
Access level: all

Syntax

PORT HISTORY

When you are in port history mode, you may issue the following commands.

Port History Mode Commands

Command	Description
Bottom	**B** sets the history view location to the bottom of the file minus 23 history display lines, if available.
Clear	**C** clears the port's history buffer.
Next	**N** increments the current history display line by the number of lines per page and a new history display page is output.
Prev	**P** decrements the current history display line by the number of lines per page and a new history display page is output.
Quit	**Q** returns to the normal CLI.
Resume	**R** exits port history mode and CLI mode, and resumes the serial session with the attached serial device.
Search	**S** searches the port history buffer for a specified string. Enclose strings containing embedded spaces in quotes. To specify search direction, type **-u** (up) or **-d** (down). To ignore case, type **-i**.
Top	**T** sets the current history display line to 1 and outputs a history display page.

Examples

The following command accesses the serial port's history mode.

```
> port history
```

In history mode, the following command searches the history buffer in the downward direction for the string “connected to,” ignoring case.

```
    PORT HISTORY > s -d -i “connected to”
```

Port Logout command

The Port Logout command terminates the SCPS session on a specified port.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> LOGOUT

Port Logout Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.

Port Set command

The Port Set command changes SCPS port settings in the SCPS configuration database. At least one keyword parameter and value must be specified. For more information, see *Configuring Serial Port Settings* in Chapter 4.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT [<*port*>|ALL] SET
[TD=<*device*>] [NAME=<*name*>] [BAUD=<*baud*>] [SIZE=<*size*>]
[PARITY=<*parity*>] [STOP=<*stopbits*>] [FLOW=<*signal*>]
[TIMEOUT=<*time-out*>] [SOCKET=<*socket*>] [CHAR=^<*cli_char*>]
[TOGGLE=NONE|DTR] [POWER=<*signal*>]

Port Set Command Parameters

Parameter	Description
<*port*>|ALL	Either a port number in range 1-8 for an SCPS-8 or 1-16 for an SCPS-16, or All which indicates that the settings that follow should be applied to all ports. Default = port to which you are attached

Port Set Command Parameters (Continued)

Parameter	Description
TD=<*device*>	Target device type. The valid value is Console. Default = Console
NAME=<*name*>	Port name, up to 32 characters. If the name contains spaces, enclose the name in double quotes. To return one or all port names to default values, specify Name="". The port name is used only by ServSelect IP Software. Default = last 3 octets of MAC address plus the port number
BAUD=<*baud*>	Baud rate. Valid values are: 0, 75, 110, 134, 150, 200. 300, 600, 1200, 2400, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 57600, 115200. Default = 9600
SIZE=<*size*>	Number of data bits per character. Valid values are 7 and 8. Default = 8
PARITY=<*parity*>	Parity. Valid values are: None No parity. Even Even parity. Odd Odd parity. Mark Mark parity. Space Space parity. Default = None
STOP=<*stopbits*>	Number of stop bits per character. Valid values are 1 and 2. Default = 1
FLOW=<*signal*>	Flow control signal. For hardware flow control, be sure the control signals are correctly wired, or data loss may occur. The flow control signal cannot also be used for power status monitoring. Valid values are: XONXOF Software XON/XOFF flow control. RTSCTS Hardware RTS/CTS flow control. DTRDCD Hardware DTR/DCD flow control. None No flow control. Default = None
TIMEOUT=<*time-out*>	Number of time-out minutes in the range Ø-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. This value overrides the time-out value set with a Server CLI command. Default = use value set with Server CLI command

Port Set Command Parameters (Continued)

Parameter	Description
SOCKET=<*socket*>	TCP port that must be entered on the Telnet client to connect to this serial port. The new value becomes effective upon the next connection to the port. When SSH is enabled, the SCPS automatically adds 100 to the specified value. When All is specified, port 1 will be assigned the specified socket value plus 1, port 2 will be assigned the specified value plus 2, and so on. When All is specified and SSH is enabled, port 1 will be assigned the specified socket value plus 101, port 2 will be assigned the specified value plus 102, and so on. When both plain text Telnet and SSH connections are enabled, the +100 value will not appear in displays. Default = 3000 plus the port number, 3100 plus the port number if SSH is enabled; see above for action taken if All is specified
CHAR=^<*cli_char*>	CLI access character in the range A to _ (underscore) or NONE. (The allowable ASCII range is Øx41-Øx5F and Øx61-Øx7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. If None is specified, the value specified in the Char parameter of the Server CLI command will be used. Default = None
TOGGLE=NONE|DTR	When set to DTR, the SCPS will toggle the port's DTR-out signal off for 1/2 second each time a connection is made to the port. This toggle is required to awaken the console port of some devices. Default = None
POWER=<*signal*>	Control signal to monitor and the state that indicates the target device has power on. The entire value must be specified; abbreviations are not allowed. The power status monitoring signal cannot also be used for flow control. Valid values are: None — Disables power status monitoring. HICTS — CTS high indicates power on. LOCTS — CTS low indicates power on. HIDCD — DCD high indicates power on. LODCD — DCD low indicates power on. HIDSR — DSR high indicates power on. LODSR — DSR low indicates power on. Default = None

Example

The following command sets a baud rate of 57600 and enables XON/XOFF flow control on port 2.

```
    > port 2 set baud=57600 flow=xonxof
```

6.5 Quit Command

The Quit command terminates the current SCPS session and terminates your Telnet connection to the SCPS.

Access right: none needed
Access level: all

Syntax

QUIT

6.6 Resume Command

The Resume command exits the CLI and resumes your connection to the attached serial device. The history buffer contains any data received while you were in CLI mode.

Access right: none needed
Access level: all

Syntax

RESUME

6.7 Server Commands

The Server command has several forms.

Server Command Summary

Command	Description
Server CLI	Specifies the serial CLI port, type and access character; modem initialization string; port history mode operations and port time-out value. It also enables/disables device connection from the CLI port.
Server FLASH	Updates the SCPS program FLASH.
Server PPP	Enables/disables PPP connections to the serial CLI port.
Server RADIUS	Specifies RADIUS parameters.

Server Command Summary (Continued)

Command	Description
Server Reboot	Reboots the SCPS.
Server Security	Specifies the authentication mode and lock-out.
Server Set	Changes SCPS addresses.
Server SNMP	Enables/disables SNMP processing.
Server SNMP Community	Defines read, write and trap community strings.
Server SNMP Manager	Defines/deletes SNMP management entities.
Server SNMP Trap	Enables/disables SNMP traps.
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps.
Server SSH	Enables/disables SSH session access to the SCPS.

Server CLI command

The Server CLI command:

- Specifies the CLI port, type and access character
- Enables or disables device connection from the CLI port
- Specifies a modem initialization string
- Specifies port history mode operations
- Specifies a port time-out value

At least one parameter must be specified.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER CLI [PORT=<port>] [TYPE=<type>] [CHAR=^<char>]
      [CONNECT=ON|OFF] [HISTORY=HOLD|AUTO,CLEAR|KEEP]
      [MODEMINIT="<string>"] [TIMEOUT=<time-out>]
```

Server CLI Command Parameters

Parameter	Description
PORT=<*port*>	CLI port number in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16. Default = current CLI port number; 1 is the manufacturing default

Server CLI Command Parameters (Continued)

Parameter	Description
TYPE=<*type*>	Terminal type to be used on CLI port. The entire type name must be specified; abbreviations are not permitted. Valid types are: ASCII, VT52, VT100, VT102, VT220, VT320 and OFF. Specifying Type=Off disables the CLI. Default: ASCII
CHAR=^<*char*>	CLI access character in the range A through **_** (underscore). (The allowable ASCII range is Øx41-Øx5F and Øx61-Øx7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. This value will be used if a port's Port Set command contains a Char=None parameter. Default = ^d is the manufacturing default
CONNECT=ON|OFF	Enables or disables the ability to use the Connect command from the serial CLI port. When enabled, a serial CLI user may use the Connect command to establish a connection to the serial device attached to another SCPS serial port. When disabled, you cannot use the Connect command from the serial CLI port. Default = ON
HISTORY= HOLD|AUTO, CLEAR|KEEP	Port history file processing options during connection (Hold or Auto) and when a session ends (Clear or Keep): When Hold is specified, upon connection you are informed of how much data is in the history buffer, but the data is not displayed. When Auto is specified, upon connection you are informed of how much data is in the history buffer, and it is then displayed. When Clear is specified, the history buffer's content is cleared when a session ends. When Keep is specified, the history buffer's content is retained when a session ends. You cannot specify both Clear and Keep or both Hold and Auto. Default = HOLD,CLEAR
MODEMINIT= "<*string*>"	Modem initialization string, enclosed in quotation marks. Must contain at least ATV1 and SØ=1. Default = "" (no modem is attached to serial CLI port)

Server CLI Command Parameters (Continued)

Parameter	Description
TIMEOUT=<*time-out*>	Number of time-out minutes in the range Ø-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. This value is used for any SCPS port that does not have a time-out value set with the Port Set command, during a Telnet session to port 23 or an SSH session to port 22. Default = 15 minutes is the manufacturing default

Server FLASH command

The Server FLASH command updates the SCPS program images in FLASH memory. You may wish to use this command to update the program with new features or to install a later release of the program.

There are two program images that you may update in the SCPS FLASH. The boot image file (scps40bt.img) contains the SCPS startup and self-test logic. The application image scps40app.img) contains the SCPS program that provides SCPS functionality.

You will need a TFTP server. Download the latest FLASH image. Save the image file to the appropriate directory on the TFTP server.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER FLASH BOOT|APP HOSTIP=<*tftp_add*> IMAGE=<*host_file*>

Server FLASH Command Parameters

Parameter	Description
BOOT	Indicates the BIOS/Bootstrap image should be updated.
APP	Indicates the application image should be updated.
HOSTIP=<*tftp_add*>	IP address of TFTP server host.
IMAGE=<*host_file*>	Name of file on TFTP server host containing the image file.

Example

The following command updates the SCPS boot image program using the image file name c:\winnt\system32\drivers\scps4Øbt.img, which is located on the TFTP server host located at 192.168.1.16.

```
> ser fla boot hostip=192.168.1.16 ima=c:\winnt\system32\
drivers\scps40bt.img
```

Server PPP command

The Server PPP command enables or disables the PPP server on the serial CLI port. For more information, see *Connecting to devices using PPP* in Chapter 4.

Once the PPP server has been configured with this command by specifying the required addresses and masks, those values remain in the database. Later, if you disable the PPP server and wish to reenable it with the same addresses, you don't need to specify the address values again.

When you enable the PPP server, the serial CLI port must already be defined.

When you enter this command, you are prompted to confirm or cancel the specified changes.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER PPP DISABLE|ENABLE
[LOCALIP=<*local_ip*>] [REMOTEIP=<*rem_ip*>] [MASK=<*subnet*>]

Server PPP Command Parameters

Parameter	Description
DISABLE	Disables the PPP server.
ENABLE	Enables the PPP server.
LOCALIP=<*local_ip*>	IP address to be used to connect the SCPS over the PPP connection. Must be on same subnet as REMOTEIP address.
REMOTEIP=<*rem_ip*>	IP address to assign to the PPP client end of the PPP connection. Must be on same subnet as LOCALIP address.
MASK=<*subnet*>	LAN subnet for the PPP dial-in client.

Examples

The following command enables the PPP server with a local IP address of 192.168.0.1, a remote IP address of 192.168.0.2 and a subnet mask of 255.255.255.0.

```
> ser ppp ena loc=192.168.0.1 rem=192.168.0.2
mas=255.255.255.0
```

The following command enables the PPP server with previously configured IP and subnet mask values. This form of the command would not be valid unless the IP and subnet mask values had been previously configured.

```
> server ppp enable
```

Server RADIUS command

The Server RADIUS command defines or deletes RADIUS parameters for the SCPS RADIUS client. For more information, see *RADIUS authentication* in Chapter 4.

When you enter this command, you are prompted to confirm or cancel the specified changes.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER RADIUS PRIMARY|SECONDARY
        IP=<radius_ip> SECRET=<secret> USER-RIGHTS=<attr>
        [AUTHPORT=<udp>] [TIMEOUT=<time-out>] [RETRIES=<retry>]
- or -
SERVER RADIUS PRIMARY|SECONDARY DELETE
```

Server RADIUS Command Parameters

Parameter	Description
PRIMARY	Indicates the primary RADIUS server is being defined or deleted.
SECONDARY	Indicates the secondary RADIUS server is being defined or deleted.
IP=<*radius_ip*>	IP address of the RADIUS authentication server.
SECRET=<*secret*>	8-24 character text string for shared secret with the RADIUS server. Enclose the string in quotes if it contains spaces.
USER-RIGHTS=<*attr*>	Attribute number defined on the RADIUS server, in the range 1-255.
AUTHPORT=<*udp*>	UDP port for RADIUS authentication server, in the range 1-65535. This value is usually 1645, but may be 1812. Default = 1645
TIMEOUT=<*time-out*>	Number of seconds to wait for a response from the RADIUS server, in the range 1-60. Default = 5
RETRIES=<*retry*>	Number of attempts to make to authenticate a user after a time-out, in the range 1-10. Default = 3
DELETE	Deletes the RADIUS server definition.

Examples

The following command specifies primary RADIUS server information; default values will be used for the UDP port, time-out and retries values.

```
> ser radius primary ip=192.168.0.200 secret=ThePrimaryRadSe
cret user-rights=86
```

The following command deletes the primary RADIUS server definition.

```
> ser radius primary del
```

Server Reboot command

The Server Reboot command reboots the SCPS. During a reboot, any active Telnet sessions, including your own, are terminated, and all users are informed accordingly. Any SCPS configuration changes that require a reboot will become effective when the reboot completes.

When you enter this command, you are prompted to confirm or cancel the reboot.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER REBOOT

Server Security command

The Server Security command specifies how authentication will be performed and whether Security Lock-out is enabled. You may also enable/disable SSH connections, plain text Telnet connections or both. For more information, see *Using Authentication Modes* and *Using Security Lock-out* in Chapter 4.

When you enter this command, you are prompted to confirm or cancel the specified information.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SECURITY [AUTHENTICATION=<*auth_mode*>]
[ENCRYPT=<*conns*>] [LOCKOUT=<*hours*>]

Server Security Command Parameters

Parameter	Description
AUTHENTICATION= <*auth_mode*>	Authentication mode. Multiple values may be specified, separated by commas. Valid values are: LOCAL - Use the internal SCPS user database to authenticate users. RADIUS - Use the previously defined RADIUS server(s) to authenticate users. NONE - Do not authenticate users. This mode cannot be used when SSH access is enabled, and it cannot be combined with other authentication modes. Default = LOCAL
ENCRYPT=<*conns*>	Enables/disables plain text Telnet or SSH connections. You may enable both by specifying both values, separated by a comma. Valid values are: SSH Enables SSH connections. None Enables plain text Telnet connections. Default: None
LOCKOUT=<*hours*>	Enables or disables Security Lock-out. To enable, specify the number of hours in the lock-out period, in the range 1-99. To disable, specify a Ø value. Default = Ø (disabled)

Examples

The following command specifies that the SCPS user database will be used to authenticate users. SSH and plain text Telnet connections will be allowed.

```
    > server security authentication=local encrypt=ssh,none
```

Server Set command

The Server Set command changes SCPS address information.

If you change the IP address, you are prompted to confirm or cancel an SCPS reboot to effect the change (changing the mask or gateway address doesn't require a reboot).

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SET IP=<*ip_address*> MASK=<*subnet*> [GATEWAY=<*gtwy*>]

Server Set Command Parameters

Parameter	Description
IP=<*ip_address*>	SCPS IP address.
MASK=<*subnet*>	Subnet mask for the subnet on which the SCPS resides.
GATEWAY=<*gtwy*>	IP address of default gateway for routing IP packets.

Server SNMP command

The Server SNMP command enables or disables SNMP UDP port 161 SNMP processing. When you disable SNMP processing, you may still enable and disable traps with the Server SNMP Trap command.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER SNMP ENABLE|DISABLE
```

Server SNMP Command Parameter

Parameter	Description
ENABLE|DISABLE	Enables or disables SNMP processing. Default = Enabled

Server SNMP Community command

The Server SNMP Community command defines read, write and trap SNMP community strings. Community names are case sensitive.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER SNMP COMMUNITY [READCOMM=<name>]
        [WRITECOMM=<name>] [TRAPCOMM=<name>]
```

Server SNMP Community Command Parameters

Parameter	Description
READCOMM=<*name*>	1-64 alphanumeric character read community name. Default = public
WRITECOMM=<*name*>	1-64 alphanumeric character write community name. Default = public
TRAPCOMM=<*name*>	1-64 alphanumeric character trap community name. If you specify this parameter, the name must be different from the read and write community names. Default = public

Server SNMP Manager command

The Server SNMP Manager command defines or deletes SNMP management entities. You may define up to four management entities. If you delete all SNMP managers (or never add any), the SCPS may be accessed via SNMP from any IP address.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP MANAGER ADD|DELETE <*ip_address*>

Server SNMP Manager Command Parameters

Parameter	Description
ADD|DELETE	Adds or deletes the specified SNMP management entity.
<*ip_address*>	IP address of SNMP management entity.

Example

The following command adds an SNMP management entity with the IP address of 192.168.0.1.

```
server snmp manager add 192.168.0.1
```

Server SNMP Trap command

The Server SNMP Trap command enables or disables SNMP traps. When you issue this command with the Enable parameter, the SCPS displays a numbered list of all currently disabled traps. When you issue this command with the Disable parameter, the SCPS displays a numbered list of all currently enabled traps.

You may indicate the traps to be enabled/disabled by entering a single number, several numbers separated by commas, a range of numbers separated by a dash or a combinations of numbers separated by commas and dashes. You may also type **ALL** to select all traps in the list or press **Enter**, which cancels the operation.

If you specify **ALL** on the command line, the numbered list is not displayed.

If you enable a trap but there is no trap destination configured for it, a warning will be issued. In this case, issue a Server SNMP Trap Destination command.

NOTE:
By default, all traps are disabled. The portAlert trap must be enabled for port alert processing to be performed.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4. The supported traps are listed in Chapter 7.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP [ENABLE|DISABLE] [ALL]

Server SNMP Trap Command Parameter

Parameter	Description
ENABLE|DISABLE	Enable generates a numbered list of currently disabled traps from which you choose those to enable. Disable generates a numbered list of currently enabled traps from which you choose those to disable.

Example

The following command enables the linkUp, userDeleted and userLogin SNMP traps.

```
server snmp trap enable

Traps now disabled:
1) linkUp                   4) userLogin
2) userAdded                5) imageUpgradeStarted
3) userDeleted

Select trap(s) to enable>1,3-4
```

Server SNMP Trap Destination command

The Server SNMP Trap Destination command defines or deletes destinations for enabled SNMP traps. Once you define destinations for enabled SNMP traps, when a trap occurs, the SCPS will generate SNMP trap messages to each defined SNMP trap destination. You may define up to four trap destinations, using separate commands.

For more information, see *Managing the SCPS Using SNMP* in Chapter 4.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER SNMP TRAP DESTINATION ADD|DELETE <ip_address>
```

Server SNMP Trap Destination Command Parameters

Parameter	Description
ADD|DELETE	Defines or deletes the specified destination.
<*ip_address*>	IP address of trap destination.

Server SSH command

The Server SSH command enables or disables SSH session access to the SCPS and specifies the SSH authentication method. When you enable SSH, all SCPS sessions will be terminated if an SCPS SSH server key must be generated.

If you enable plain text Telnet connections with a Server Security command, enabling SSH session access with the Server SSH command will add that as a valid connection method (both plain text and SSH connections will be allowed).

For more information, see *Connecting to devices using SSH* in Chapter 4.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

```
SERVER SSH ENABLE|DISABLE [AUTH=<auth>]
```

Server SSH Command Parameters

Parameter	Description
ENABLE|DISABLE	Enables or disables SSH session access to the SCPS.
AUTH=<*auth*>	SSH authentication methods. You must enter the entire value; abbreviations are not permitted. Valid values are: PW Password authentication. KEY Key authentication. PW|KEY Password or key authentication. KEY|PW Key or password authentication. PW&KEY Password and key authentication. KEY&PW Key and password authentication. Default = PW

6.8 Show Commands

The Show command has several forms, as listed in the following table.

Show Command Summary

Command	Description
Show Port	Displays configuration information and statistics for one or all ports.
Show Port Alert	Displays port alert strings.
Show Server	Displays SCPS configuration information and statistics.
Show Server CLI	Displays SCPS CLI settings.
Show Server PPP	Displays SCPS PPP settings.
Show Server RADIUS	Displays SCPS RADIUS settings.
Show Server Security	Displays SCPS authentication, allowed access method and Security Lock-out settings.
Show Server SNMP	Displays SNMP configuration information.
Show User	Displays user configuration and session information.

Show Port command

The Show Port command displays configuration and status information about one or all ports.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW PORT [<port>|ALL|NAMES]
```

Show Port Command Parameter

Parameter	Description
<port>	Port number. Default = your port
ALL	Displays information about all ports.
NAMES	Displays only port numbers and names. If a port has not been given a name with a Port Set command, the default name is displayed. A default name contains the last three octets of the MAC address plus the port number.

The following tables list the display fields for a SHOW PORT command that specifies one or all ports.

Show Port Command Display Fields for Console Ports

Field	Content
Port	Port number.
Serial Port Settings	Comma-separated string of port values: baud rate, number of bits, parity, stop bits, flow control, socket number, time-out value and CLI access character. The CLI character is preceded by POR CLI= if it was defined with a Port Set command or by SER CLI= if it was defined with a Server CLI command.
TX Bytes	Number of bytes transmitted.
RX Bytes	Number of bytes received.
Errors	Number of TX/RX parity and framing errors.
Power	Device power status, if monitoring is enabled. ON indicates the device is on, OFF indicates the device is off. If monitoring is disabled, this field is blank.
Toggle **	Toggle value (from Port Set command).
Power Signal **	Signal and state being monitored for device power status (from Port Set command).
Logical name **	Logical port name, which contains last three octets of MAC address plus the port number.
User *	Username (from User Add command).
Level *	User's access level (from User Add and User Set commands).
Access *	User's access rights (from User Add and User Set commands).

Show Port Command Display Fields for Console Ports (Continued)

Field	Content
Duration *	Duration of user's session.

* Displayed only when the command specifies a single port that is currently being accessed.
** Displayed only when the command specifies a single port that is not in use.

Show Port Alert command

The Show Port Alert command displays a port's alert strings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW PORT <port> ALERT
```

Show Port Alert Command Parameter

Parameter	Description
<port>	Port number in the range 1-8 for an SCPS-8 or 1-16 for an SCPS-16.

Show Server command

The Show Server command displays SCPS configuration information and statistics.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER
```

Show Server Command Display Fields

Field	Content
Server	SCPS IP address (from initial configuration or Server Set command).
Mask	Subnet mask (from initial configuration or Server Set command).
Gateway	Gateway IP address (from initial configuration or Server Set command).

Show Server Command Display Fields (Continued)

Field	Content
Up Time	Days, hours, minutes and seconds since SCPS was rebooted.
MAC	Ethernet MAC address.
S/N	SCPS serial number.
Port	Port number.
Username	Username (from User Add command).
Duration	Duration of session.
Socket	Telnet SCPS socket number.
From Socket	Telnet client IP address with socket number in parentheses.
IP Input and Output	Network IP statistics, including number of packets delivered, discarded and fragments.
TCP	Network TCP statistics, including in segs, out segs, errors and retransmissions.
UDP	Network UDP statistics, including in, out, errors and no port events.
BOOT	BIOS/Bootstrap version, date and time.
APP	Application version that is running, plus its date and time.

Show Server CLI command

The Show Server CLI command displays the SCPS serial CLI settings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER CLI
```

Show Server CLI Command Display Fields

Field	Contents
CLI Port	Serial CLI port number and terminal type.
Access Character	Control character used to access CLI.
History	Indicates whether a port’s history buffer content is displayed (auto) or not displayed (hold) when a user connects to the port, and whether the buffer content is cleared (clear) or kept (keep) when a session ends.

Show Server CLI Command Display Fields (Continued)

Field	Contents
Connect	Indicates whether a valid user on the serial CLI port may use the Connect command.
Modeminit string	String used to initiate modem connections on the serial CLI port.
Server CLI Timeout	Session time-out value, shown in full minute or minute: second form (for example, 3m for 3 minutes, 3:30 for 3 minutes, 3 seconds).

Show Server PPP command

The Show Server PPP command displays the current SCPS PPP settings that were configured with the Server PPP command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER PPP
```

Show Server RADIUS command

The Show Server RADIUS command displays the current SCPS RADIUS settings that were configured with the Server RADIUS command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER RADIUS
```

Show Server Security command

The Show Server Security command displays the current SCPS authentication and lockout settings that were configured with the Server Security and Server SSH commands.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER SECURITY
```

Show Server Security Command Display Fields

Field	Contents
Authentication	Configured authentication method(s). This includes the SSH authentication method configured with the Server SSH command (or the default value), regardless of whether SSH is enabled.
Encryption	Configured connection methods.
Lockout	Configured security lock-out state (Enabled or Disabled). If Enabled, the number of hours in the lock-out period is included.
Fingerprint (Hex)	SSH key MD5 hash. This field is displayed only when SSH is enabled.
Fingerprint (BB)	SSH key bubble babble. This field is displayed only when SSH is enabled.

Show Server SNMP command

The Show Server SNMP command displays SNMP configuration information.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW SERVER SNMP
```

Show User command

The Show User command displays information about one or all users.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
SHOW USER [<username>|ALL]
```

Show User Command Parameter

Parameter	Description
<username>	Username. Default: user currently logged in
ALL	Requests a display of all defined users.

The Show User command display for one user includes the information in the following table.

Show User Command Display Fields

Field	Contents
User	Username.
Level	User’s access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User’s access rights.
Locked	YES if user is locked-out, NO if not.
Last Login	System up time value when the user logged in.
Port	Serial port to which user is connected.
Username	Username.
Duration	Duration of user’s session.
Socket	Telnet SCPS socket number.
From Socket	Telnet client IP address and socket number.

A Show User All command display includes the information in the following table.

Show User All Command Display Fields

Field	Contents
User	Username.
Pass	YES if user has a password defined, NO if not.
Key	YES if user has an SSH key defined, NO if not.
Lock	YES if user is locked-out, NO if not.
Level	User’s access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User’s access rights.

6.9 User Commands

The User command has several forms, as listed in the following table.

User Command Summary

Command	Description
User Add	Adds a new user to the SCPS user database.
User Delete	Deletes a user from the SCPS user database.
User Logout	Terminates a user's active SCPS session.
User Set	Changes a user's configuration information.
User Unlock	Unlocks a locked-out user.

User Add command

The User Add command adds a new user to the SCPS user database. The SCPS user database holds a maximum of 64 user definitions. For more information, see *Managing User Accounts, Connecting to devices using SSH* and *Access rights and levels* in Chapter 4.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
USER ADD <username>
        [PASSWORD=<pwd>] [SSHKEY=<keyfile>] [FTPIP=<ftpadd>]
        [KEY=<sshkey>] [ACCESS=<access>]
```

User Add Command Parameters

Parameter	Description
<*username*>	3-16 alphanumeric character username. Usernames are case sensitive.
PASSWORD=<*pwd*>	3-16 alphanumeric character password. Passwords are case sensitive.
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that can be received is 4K bytes. If this parameter is specified, you must also specify the FTPIP parameter.
FTPIP=<*ftpadd*>	FTP server's IP address. If this parameter is specified, you must also specify the SSHKEY parameter.
KEY=<*sshkey*>	Uuencoded SSH key.

User Add Command Parameters

Parameter	Description
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. Valid values for access rights are: P<*n*> Access to the specified port number. P<*x-y*> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK May issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON

Examples

The following command adds the username JohnDoe, with the password secretname, access to ports 2, 5, 6 and 7 and user and monitor access rights.

```
> user add JohnDoe password=secretname access=P2,5-
7,user,smon
```

The following command adds the username JaneDoe, with access to all ports. The name of the SSH public user key file is ccm_key2.pub. This file is located on the FTP server at IP address 10.0.0.3.

```
> user add JaneDoe ssh=ccm_key2.pub ftp=10.0.0.3 access=pall
```

The following command adds the username JDoe and gives that user the Appliance Administrator access level, which enables access to all ports and SCPS commands.

```
> user add JDoe access=applianceadmin
```

User Delete command

The User Delete command removes a username entry from the SCPS user database. The username may no longer be used to authenticate a session with the SCPS. If the specified user is currently logged in, a message is output to the user, indicating that access is no longer permitted, and the Telnet session is terminated.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

```
USER DEL <username>
```

User Delete Command Parameter

Parameter	Description
<username>	Username to be deleted.

User Logout command

The User Logout command terminates a user's active sessions on the SCPS. If the specified user has no active sessions, an error message is displayed. For all active sessions that are terminated, a message is sent to the Telnet client and the Telnet connection is dropped.

Access right: USER
Access level: APPLIANCEADMIN may log out any user; ADMIN may log out any other user except APPLIANCEADMIN

Syntax

```
USER LOGOUT <username>
```

User Logout Command Parameter

Parameter	Description
<username>	Username to be logged out.

User Set command

The User Set command changes a user's configuration in the SCPS user database. For more information, see *Managing User Accounts*, *Connecting to devices using SSH* and *Access rights and levels* in Chapter 4.

You may delete a user's password or key; however, each user must have a password or a key, so you cannot remove both. Also, you cannot remove a user's password or key if that action would result in no users having USER access rights.

Access right: none to change your own password, USER to change anything else
Access level: none to change your own password; ADMIN or APPLIANCEADMIN to change anything else

Syntax

```
USER SET <username> [PASSWORD=<pwd>] [SSHKEY=<keyfile>]
        [FTPIP=<ftpadd>] [KEY=<sshkey>] [ACCESS=<access>]
```

User Set Command Parameters

Parameter	Description
<*username*>	Username.
PASSWORD=<*pwd*>	New 3-16 alphanumeric character password. Passwords are case sensitive. This parameter is required when changing another user's password. The password is displayed on the screen. For security, clear your screen display after issuing this command. To delete a password, specify Password ="".
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that can be received is 4K bytes.
FTPIP=<*ftpadd*>	FTP server's IP address.
KEY=<*sshkey*>	Uuencoded SSH key. To delete an SSH key (whether it was originally specified with the SSHKEY and FTPIP parameters or with the KEY parameter), specify Key="".
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. If specifying access rights, you may use one of three forms: ACCESS=<*access*> to specify all access rights. ACCESS=+<*access*> to specify only access rights to be added. ACCESS=-<*access*> to specify only access rights to be deleted. Valid values for access rights are: P<n> Access to the specified port number. P<x-y> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK May issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON

Examples

The following command sets the access rights for JohnDoe enabling access to all ports with configuring and monitoring access rights.

```
> user set JohnDoe access=pall,scon,smon
```

The following command removes the server configuration access right for JohnDoe, and leaves other access rights intact.

```
    > user set JohnDoe access=-SCON
```

The following command deletes the SSH key information for JohnDoe. The command will complete successfully only if JohnDoe has a password configured in a previous User Add or User Set command, and if there are other users with User access rights.

```
    > user set key=“”
```

User Unlock command

The User Unlock command unlocks a user who was previously locked-out. After this command completes, the user will be able to attempt login authentication again.

Access right: USER
Access level: APPLIANCEADMIN may unlock any user; ADMIN may unlock any user except APPLIANCEADMIN

Syntax

USER UNLOCK <*username*>

User Logout Command Parameter

Parameter	Description
<*username*>	Username to be unlocked.

7. Traps

The SCPS supports the following MIB2 traps:

- snmpAuthenticationFailure
- linkUp
- linkDown
- coldStart

The following table lists the supported enterprise traps.

Enterprise Traps

Trap	Description
RebootStarted	The SCPS appliance is rebooting. The trap provides the name of the user who initiated the reboot.
UserLogin	A user logged in to the SCPS appliance. The trap provides the name of the user.
UserLogout	A user logged out of the SCPS appliance. The trap provides the name of the user.
SerialSessionStarted	A serial session has started. The trap provides the name of the user and the session identifier.
SerialSessionStopped	A serial session has stopped. The trap provides the name of the user and the session identifier.
SerialSessionTerminated	Another user has terminated a serial session. The trap provides the name of the user terminating the session, the name of the user who was terminated and the session identifier.
ImageUpgradeStarted	The SCPS appliance has started an image upgrade. The trap provides the name of the user who initiated the upgrade, the image type (boot or application), the version number of the image the SCPS appliance is upgrading to and the version number of the image currently running.
ImageUpgradeResults	An image upgrade has ended. The trap provides the image type (boot or application) and the upgrade results (successful or error code).
UserAdded	A new user has been added to the SCPS user database. The trap provides the name of the user who initiated the addition and the name of the new user.

Enterprise Traps (Continued)

Trap	Description
UserDeleted	A user has been deleted from the SCPS user database. The trap provides the name of the user who initiated the deletion and the name of the deleted user.
UserModified	A user's definition has been modified in the SCPS user database. The trap provides the name of the user who initiated the modification and the name of the modified user.
UserAuthenticationFailure	A user failed to authenticate with the SCPS appliance. The trap provides the name of the user.
FactoryDefaultsSet	The SCPS appliance has been set to its factory default values.
PortAlert	The SCPS appliance detected a port alert string on a serial port. The trap provides the port number and the alert string.
PortPowerOnDetect	The SCPS appliance detected that a port's power on/off control signal is in the state indicating power is on. The trap provides the port number. This trap is sent on initialization if the condition is detected. Subsequent traps are sent only if this signal changes state.
PortPowerOffDetect	The SCPS appliance detected that a port's power on/off control signal is in the state indicating power is off. The trap provides the port number. This trap is sent on initialization if the condition is detected. Subsequent traps are sent only if this signal changes state.
ConfigurationFileLoaded	The SCPS appliance has loaded a configuration file. The trap provides the file name and the name of the user who initiated the load operation.
UserDatabaseLoaded	The SCPS appliance has loaded a user database file. The trap provides the file name and the name of the user who initiated the load operation.

8. Device Cabling

Each SCPS serial port has an RJ45 connector for attaching a serial device. The following table lists the pin assignments.

Port Pin Assignments

Pin #	RS232 Signal	Direction	Description
1	RTS	Output	Request To Send
2	DSR	Input	Data Set Ready
3	DCD	Input	Data Carrier Detect
4	RxD	Input	Receive Data
5	TxD	Output	Transmit Data
6	GND	(N/A)	Signal Ground
7	DTR	Output	Data Terminal Ready
8	CTS	Input	Clear to Send

NOTE: RI (Ring Indicate) is not supported.

The following table lists the modular adaptors that are available from Black Box to convert RJ45 modular jacks to DB-25 or DB-9 connectors.

Reversing Adaptors

Part No.	Description
FA260	RJ45 to DB-25M (DTE) Adaptor
FA261	RJ45 to DB-25F (DTE) Adaptor
FA262	RJ45 to DB-25M (DCE) Adaptor
FA263	RJ45 to DB-25F (DCE) Adaptor
FA264	RJ45 to DB-9M Adaptor
FA265	RJ45 to DB-9F Adaptor

If you choose to use a non-Black Box cable, make sure the cable is reversing, as shown in Figure 8-1.

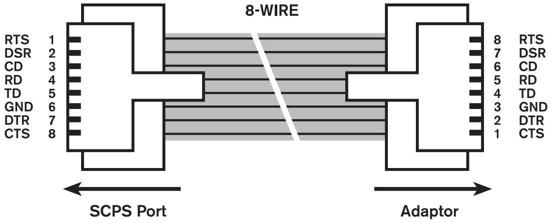


Figure 8-1. 8-wire RJ45 Reversing Cable

9. Ports Used

The following table lists the UDP and TCP port numbers used by the SCPS. The values assume a default SCPS configuration; some values are configurable.

Ports Used by SCPS

Port Type and Number	Used for
TCP 22	SSH2, if enabled.
TCP 23	Telnet.
UDP 161	SNMP, if enabled.
UDP 3211	Secure protocol used by ServSelect IP Software.
TCP 3211	Secure protocol used by ServSelect IP Software.
TCP 3001-3016	Telnet serial sessions with ports 1-16.
TCP 3101-3116	SSH serial sessions with ports 1-16.

10. Troubleshooting

10.1 Calling BLACK BOX

If you determine that your ServSelect IP SCPS is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact BLACK BOX Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem;
- when the problem occurs;
- the components involved in the problem;
- any particular application that, when used, appears to create the problem or make it worse; and
- the results of any testing you’ve already done.

10.2 Shipping and Packaging

If you need to transport or ship your ServSelect IP SCPS:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the ServSelect for repair, make sure you include its power cord and the cables you’re using with it. If you are returning the ServSelect IP SCPS, make sure you include everything you received with it. Before you ship, contact BLACK BOX to get a Return Authorization (RA) number.

NOTES

NOTES

BLACK BOX®
NETWORK SERVICES

Customer Support Information:
For FREE Technical Support 24 hours a day, 7 days a week, call **724-746-5500** or fax **724-746-0746**
Mailing address: **Black Box Corporation**, 1000 Park Dr., Lawrence, PA 15055-1018
World-Wide Web: **www.blackbox.com** • Email: **info@blackbox.com**

© Copyright 2004. Black Box Corporation. All rights reserved.