EQUINOX®
an Avocent Company

CCM4850

Installer/User Guide

INSTRUCTIONS

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

DANGEROUS VOLTAGE

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

POWER ON

This symbol indicates the principal on/off switch is in the on position.

POWER OFF

This symbol indicates the principal on/off switch is in the off position.

PROTECTIVE GROUNDING TERMINAL

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

CCM4850
Installer/User Guide

USA Notification

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

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

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 édicté par le Ministère des Communications du Canada.

Japanese Approvals

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。

European Union

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

Taiwanese Notification

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Product Overview

Features and Benefits

Overview

The CCM console management appliance provides non-blocked access and control for serial devices such as serial-managed Linux (or other UNIX) servers, routers, power management devices and firewalls. You may connect up to 48 serial devices to a CCM4850 appliance.

A single 10/100/1000 Ethernet port provides network connectivity on each CCM4850 appliance. The unit also has a console port that uses a Command Line Interface (CLI) for configuration, management and optionally, connection to other ports.

A CCM4850 appliance 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 CCM appliance and its attached serial devices:

- The AVWorks® cross-platform management application 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 the appliance serial CLI, plus PPP (Point to Point Protocol) and other types of dial-in connections to a modem on the console port.

User authentication and data security

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

Extensive command set

The CCM appliance offers a wide range of commands that allow administrators to easily configure, control and display information about the CCM appliance operating environment, including its ports, user accounts and active sessions. The serial CLI is always available on the unit's console port, and may be easily accessed during a session with an attached serial device.

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 CCM appliances in the field.

Port history

Each CCM 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.

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 Equinox 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 CCM appliance off the supply.

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 rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Using AVWorks Software

The AVWorks cross-platform management application may be used to manage CCM4850 appliances and access attached devices. Using AVWorks software, you may perform most of the operations that are described in this manual. This manual describes how to manage a CCM4850 appliance by entering commands using the CLI. The AVWorks Installer/User Guide describes how to manage a CCM4850 appliance using the graphic interface.

CHAPTER 2

Installation and Configuration

Hardware Overview

Figure 2.1 shows the front panel of a CCM4850 appliance.

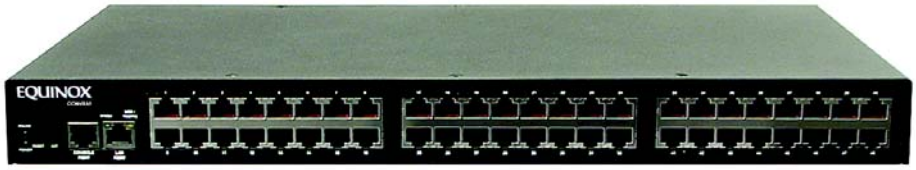

Figure 2.1: CCM4850 Appliance Front Panel

The front panel contains the 48 serial port connectors. The lower left area of the front panel contains the following LEDs, buttons and connectors:

- The *ONLINE* LED illuminates steadily (not blinking) when the CCM self-test and initialization procedures complete successfully.
- The *POWER* LED illuminates when the CCM appliance is connected to a power source and the power switch is on (|).
- The RESET button reboots the CCM appliance when pressed.
- The INIT button restores the CCM factory defaults when pressed and held. See *Reinitializing the CCM Appliance* on page 9.
- A console device may be connected to the RJ-45 CONSOLE PORT.
- A 10BaseT, 100BaseT or 1000BaseT interface cable may be connected to the LAN PORT.
- Two LEDs adjacent to the LAN PORT (*SPEED* and *LINK/TRAFFIC*) indicate the link speed and whether there is traffic on the link. Table 2.1 describes the possible values.

Table 2.1: LAN LED Values

SPEED LED	LINK/TRAFFIC LED	Description
Off	Off	No link
Off	On	Link at 10 Mbps

Table 2.1: LAN LED Values (Continued)

SPEED LED	LINK/TRAFFIC LED	Description
Green	On	Link at 100 Mbps
Orange	On	Link at 1000 Mbps
Off	Flashing	Traffic at 10 Mbps
Green	Flashing	Traffic at 100 Mbps
Orange	Flashing	Traffic at 1000 Mbps

Figure 2.2 shows the back panel of a CCM4850 appliance.

Figure 2.2: CCM4850 Appliance Back Panel

The back panel contains:

- The AC line cord connector.
- On/off switch (**O** = off, **|** = on).
- Outflow openings for the two internal fans.
- A DB-9 DEBUG PORT connector. This port should be used only on the advice and with the guidance of Equinox Technical Support.

Installing the CCM Appliance

WARNING: This unit is not user serviceable. To avoid electrical shock, do not attempt to open the unit or operate with the cover off. Do not attempt to make any repairs. See *Appendix E* on page 81 for information.

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

To install the CCM appliance hardware:

1. Place the unit where you can connect cables between the serial devices and the CCM serial ports, and where you can connect a LAN interface cable between the Ethernet hub or switch and the CCM LAN PORT connector.
2. Connect serial devices to the CCM serial ports; see *Device Cabling* on page 73 for cable information. Connect each serial device to its appropriate power source, following the device's documentation.

3. Attach a 10BaseT, 100BaseT or 1000BaseT LAN interface cable to the LAN PORT connector on the back of the CCM appliance. A CAT 5 cable is required for 100BaseT operation. A CAT 6 cable is required for 1000BaseT operation.
4. Insert the power cord into the back of the unit. Insert the other end of the power cord into a grounded electrical receptacle. Toggle the power switch on the back of the unit to the on position (|).
5. Check that the *POWER* LED on the front of the unit 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 two to three minutes to indicate that the self-test is complete. If the *ONLINE* LED blinks, contact Equinox Technical Support for assistance.
6. Check that the LAN port LEDs indicate that a 10, 100 or 1000 Mbps link exists. 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 also be illuminated.
7. Once the *POWER* and *ONLINE* LEDs and a valid LAN LED link sequence are illuminated, proceed with the configuration process (if you will be using BootP, remove power from the CCM appliance).

Configuring the CCM Appliance

To configure the CCM appliance, you must specify a unique IP address, plus other network address information. This information will be stored in the CCM configuration database. During initial login, you will specify a password for the Admin user.

Configuring the network address settings

You may configure the CCM appliance network address settings using AVWorks software, BootP or the serial CLI on the console port.

To configure the network address settings using AVWorks software:

Using the AVWorks New Appliance Wizard is the easiest method to configure the CCM appliance network address settings. See the AVWorks Installer/User Guide for instructions. After the network address settings are configured, see *Initial CCM appliance login* on page 9.

To configure the network address settings 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 CCM appliance. BootP servers require the Ethernet MAC address of network devices. The 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 CCM appliance Ethernet MAC address, IP address, subnet mask and gateway, restore power to the CCM appliance and wait for the *ONLINE* LED to illuminate. Once this occurs, the CCM appliance has completed the BootP protocol, obtained its network address information 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 a CCM appliance with the IP address 192.168.0.5.

   ```
   ping 192.168.0.5
   ```

4. If the CCM appliance 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 CCM appliance 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 address information provided to the BootP server to confirm they are correct. Verify that the Ethernet LAN adaptor cable is correctly installed on the CCM appliance and the Ethernet hub.

After the network address settings are configured successfully, launch a Telnet session to the assigned IP address. Then, see *Initial CCM appliance login* on page 9.

To configure the CCM appliance using the serial CLI:

1. Attach a compatible device to the console port. The compatible device types are: ASCII, VT52, VT100, VT102, VT220 and VT320.

   For cable and adaptor information, see *Device Cabling* on page 73. You may 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
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 CCM appliance login* on page 9.

Initial CCM appliance login

The CCM appliance ships with a single user defined in its user database. The first time you connect to the CCM appliance, you are prompted for a username.

To log in to the CCM appliance 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
   CCM configuration is required.
   ```

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

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

   If you have not already provided the network information, you will be prompted for them. Enter the addresses using standard dot notation.

   ```
   CCM configuration is required
   Enter CCM IP address > 192.168.0.5
   Enter CCM Subnet mask > 255.255.255.0
   Enter CCM Gateway address > 0.0.0.0
   ```

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 CCM New Admin Password > *****
   Confirm New Admin Password > *****
   ```

After you have provided the required configuration information, a confirmation message appears while the CCM appliance 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 other CCM appliance ports, see *Configuring Serial Port Settings* on page 11.

Reinitializing the CCM Appliance

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

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

To reinitialize the CCM appliance:

1. Locate the recessed INIT button on the front of the CCM appliance. An opened paper clip may be used to depress the button.
2. Insert the end of the opened paper clip in the recess, then depress and hold the button. The *ONLINE* LED will blink, indicating an 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 CCM 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 CCM appliance reboots when the INIT button is released.

You may also use the Server FLASH command to update the CCM FLASH application or boot program. For more information, see *Server FLASH command* on page 50.

CHAPTER 3

Operations

Overview

The CCM console management appliance and its ports are easily configured and managed to meet your requirements for device connection, user authentication, access control, power status monitoring, port history information display and Simple Network Management Protocol (SNMP) compliance for use with third party network management products.

Configuring Serial Port Settings

By default, ports are configured with the settings listed in Table 3.1.

Table 3.1: Default Port Settings

Parameter	Value
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 *CLI mode* on page 19.

The Power parameter instructs the CCM appliance to monitor the state of a specified control signal. Signal transitions may be configured to trigger SNMP traps. 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 CCM appliance 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 may not be used for power control, and vice versa.

To configure serial 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* on page 45.

To display serial port settings:

Issue a Show Port command.

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

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* on page 59.

Connecting to Serial Devices

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

Connecting to devices using Telnet

Each CCM serial port is directly addressable through a unique TCP port 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, *Enabling plain text Telnet and SSH connections* on page 18 and *Server Security command* on page 53.

You may access the CCM appliance and its ports using Equinox-provided or third party Telnet client applications. Third party Telnet applications may be used in combination with AVWorks software or standalone.

AVWorks software Telnet client

Each CCM appliance is shipped with the AVWorks cross-platform management application. AVWorks software provides a convenient way to select a CCM appliance or an attached device and launch a Telnet session to manage it.

AVWorks software includes a built-in Serial Console Viewer Telnet application that offers several features not found in other Telnet clients. For maximum flexibility, AVWorks software allows you to associate a unique Telnet client with each CCM port. AVWorks software also provides built-in support for SSH2.

You may specify the built-in Telnet client or a third party Telnet client. For more information, see the AVWorks Installer/User Guide.

Standalone third party Telnet clients

You may use third party Telnet clients to access the CCM appliance directly without AVWorks software.

To connect to a device using Telnet:

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

For example, the following Telnet command connects to the serial device attached to physical port 24 of the CCM appliance.

```
telnet 192.168.0.5 3024
```

If an authentication method other than None has been configured for the CCM appliance, you will be prompted for a 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: 7 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 CCM CLI.

NOTE: When using AVWorks software, the configuration of the credential caching feature may affect whether you are prompted for a username and password. See the AVWorks Installer/User Guide for more information.

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

Connecting to devices from the console port

You may connect to one serial device at a time from the console port, using a local terminal or a local PC using a terminal emulation program. If you connect an external modem to the console

port, you may also access devices through a remote terminal or PC that can dial into the external modem. For information about modem connections, see *Configuring and using dial-in connections* on page 14 and *Server CLI command* on page 49.

To connect to a device from the console port:

1. Issue a Server CLI command, using the Connect parameter to enable the use of the Connect command from the console 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* on page 49, *Connect Command* on page 41 and *Disconnect Command* on page 41.

Configuring and using dial-in connections

You may attach an external modem to the console port for dial-in serial CLI access to the CCM appliance. 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 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 autoanswer the phone on the first ring. For more information, see *Server CLI command* on page 49.

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

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

2. 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* on page 61.

Connecting to devices using PPP

The CCM appliance supports remote PPP access using an autoanswer modem that answers calls and establishes the PPP protocol with a dial-in client. You may establish Telnet or SSH connections over PPP.

PPP dial-in may be used to access a remote CCM appliance that does not warrant a WAN (Wide Area Network) link to the Ethernet interface. The PPP dial-in may also be used to access a subnet containing remote devices in the event of a WAN link failure. In this case, the PPP provides an alternate path to one or more remote devices.

To use PPP, you must configure a modem in autoanswer mode on the console port; see *Configuring and using dial-in connections* on page 14. Once the PPP connection is established, you must launch an application that connects to the CCM appliance or to one of its ports. The PPP connection is only a communications interface to the CCM appliance.

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

To enable or disable a PPP server on the console port:

1. To enable a PPP server on the console port, 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 CCM appliance 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.
2. To disable a PPP server, issue a Server PPP command with the Disable parameter.

   SERVER PPP DISABLE

For more information, see *Server PPP command* on page 51.

To display PPP configuration information:

Issue a Show Server PPP command.

SHOW SERVER PPP

For more information, see *Show Server PPP command* on page 62.

Connecting to devices using SSH

The CCM console management appliance supports version 2 of the SSH protocol (SSH2). The CCM 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 CCM SSH servers operate on TCP ports that are numbered with values 100 greater than the standard 30xx Telnet ports for the CCM appliance. 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 the Encrypt=SSH,None parameter, which indicates that both SSH and plain text connections will be allowed. Connecting to Telnet port 23 may also be tunneled through a connection to SSH port 22.

SSH server keys

When SSH is enabled for the first time, all sessions are terminated and the CCM appliance generates an SSH server key. The key generation process may take up to three minutes. The key is computed at random and is stored in the CCM 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 CCM appliance. During the first connection to a new SSH server, the client will display the SSH server's key. You will be prompted to indicate if it should be stored on the SSH client. After the first connection, most SSH clients will validate the key when connecting to the CCM appliance. This provides an extra layer of security because the SSH client can verify the key sent by the server each time it connects.

When 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 CCM appliance 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.

Table 3.2 lists and describes the valid SSH authentication methods that may be specified with a Server SSH command.

Table 3.2: 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.
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* on page 17.

Table 3.2: SSH Authentication Methods (Continued)

Method	Description
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 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 Methods* on page 23.

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

The CCM appliance 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 CCM appliance also processes a uuencoded SSH1 public key file. The UNIX ssh-keygen generates this file format.

To enable SSH session access to the CCM appliance:

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 CCM appliance 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* on page 57.

To disable SSH session access to the CCM appliance:

Issue a Server SSH command with the Disable parameter.

SERVER SSH DISABLE

When SSH is disabled, the CCM appliance 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.

CLI mode

While you are connected to an attached serial device, you may enter Telnet CLI mode and enter CCM appliance 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 CCM 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* on page 48.

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. You may use the Port Set command to override the Server CLI access character on a per-port basis.

For more information, see *Server CLI command* on page 49 and *Port Set command* on page 45.

To display CLI access character information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* on page 61.

Ending Device Sessions

To end your session:

Enter CLI mode and issue a Quit 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.

For more information, see *Quit Command* on page 48 and *Disconnect Command* on page 41.

To end another user's 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* on page 67. For information about preempting a user's session, see *Connecting to devices using Telnet* on page 12.

Session time-out

The CCM console management appliance 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 zero, the Server CLI time-out value is used, even if it is also zero.
- For a serial port session, if the port's configured time-out value is non-zero, that value is used.

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). For preemption purposes, the hierarchy of access levels is APPLIANCEADMIN > ADMIN > 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, see *Access rights and levels* on page 21.

Managing User Accounts

The CCM user database can 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* on page 15, *Access rights and levels* on page 21 and *User Add command* on page 65.

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* on page 15, *Access rights and levels* on page 21 and *User Set command* on page 67.

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* on page 66.

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* on page 63.

Access rights and levels

Most CCM appliance commands require the user to have the appropriate permission to issue CCM appliance commands. Permissions are expressed as access rights or access levels. The access rights

for each command are listed in Table 4.4 on page 36. Table 3.3 describes the access rights a user may be given.

Table 3.3: Access Rights

Access Right	Description
PCON	The Port Configuration access right allows the user to modify port settings. Grant PCON access only to users who need to issue the Port Set command.
SCON	The Server Configuration access right allows the user to change the CCM configurations, including setting the IP address and updating the program load in FLASH. Grant SCON access only to users who need to administer the CCM appliance.
SMON	The Server Monitor access right allows the user to view CCM appliance 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 allows the user to modify the user database. Grant USER access only to users who need to add users, change user specifications or delete users. At least one user must have USER access rights; otherwise, the user database cannot be changed.
BREAK	The BREAK access right allows the user 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 a user access to one or more serial ports and the attached serial devices. You may grant Port access rights to specific ports (Pn), a range of ports (Px-y) or all ports (PALL).

Access levels

When you specify a user's permissions, you may either indicate the individual rights as listed in Table 3.3 or you may indicate a predefined access level. The APPLIANCEADMIN and ADMIN levels 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

The third level (not APPLIANCEADMIN or ADMIN) is user. For preemption purposes, the following hierarchy is used: APPLIANCEADMIN > ADMIN > user.

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. For more information, see *Preemption* on page 20.

To manage a user's access rights/levels:

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* on page 20 plus *User Add command* on page 65, *User Set command* on page 67 and *Show User command* on page 63.

Using Authentication Methods

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

Local authentication

Local authentication uses the CCM appliance internal user database to authenticate users. You may optionally specify both local and RADIUS 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.

RADIUS authentication

RADIUS authentication uses an external third party RADIUS server containing a user database to authenticate CCM appliance users. The CCM appliance, 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 CCM appliance is informed and the user is denied CCM 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 CCM appliance commands must match corresponding values configured on the RADIUS server. On the RADIUS server, you must include CCM appliance-specific information: the list of valid users and their access rights for the CCM appliance. Each user-rights attribute in the RADIUS server's dictionary must be specified as a string containing the user's access rights for the CCM appliance, exactly matching the syntax used in the CCM 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.

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.

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 using the local CCM user database, 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

Table 3.4 indicates how authentication is performed according to the authentication method specified and the type of connection to the CCM appliance.

Table 3.4: Authentication Method Summary

Mode	Connection Type and Authentication Action
Local	All sessions are authenticated using the CCM user database.
RADIUS	Telnet and SSH sessions are authenticated using RADIUS. Serial CLI sessions are authenticated using the CCM user database.
Local,RADIUS	Telnet and SSH sessions are authenticated using the CCM user database. If that fails, authentication uses RADIUS. Serial CLI sessions are authenticated using the CCM user database.
RADIUS,Local	Telnet and SSH sessions are authenticated using RADIUS. If that fails, authentication uses the CCM user database. Serial CLI connections are authenticated using the CCM user database.
None	Telnet to serial port sessions use no authentication. Telnet CLI and serial CLI sessions are authenticated using the CCM user database. This authentication mode cannot be used for SSH connections.

To specify the authentication method:

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* on page 52.

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

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

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

   When SSH session access is enabled, you must specify an authentication method other than None.

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 CCM appliance 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 CCM 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* on page 53, *Show Server Security command* on page 62, *Show Server RADIUS command* on page 62 and *Connecting to devices using SSH* on page 15.

Using security lock-out

When the security lock-out feature is enabled, a user account 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 1-99 hours. A lock-out period of zero disables the feature; that is, user accounts will not be locked-out.

A locked account will remain locked until the specified time elapses, the CCM appliance is power-cycled or the account 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=0 parameter.

To unlock a locked-out user:

Issue a User Unlock command with the username.

Managing the Port History Buffer

Each CCM appliance 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 CCM appliance 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 are in port history mode, you may issue the commands listed in Table 3.5. Only the first letter of the command is required.

Table 3.5: 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.

Table 3.5: Port History Mode Commands (Continued)

Command	Description
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 unit 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 string Abort Process.

```
PORT HISTORY> s -u "Abort Process"
```

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

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

For more information, see *Server CLI command* on page 49 and *Port History command* on page 44.

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.

Managing the CCM Appliance Using SNMP

The CCM console management appliance 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

By default, SNMP is enabled but no traps are enabled and no trap destinations are defined.

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* on page 55.

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* on page 55.

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* on page 56.

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 CCM appliance 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 CCM appliance 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* on page 56 and *Supported Traps* on page 78.

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* on page 57.

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 CCM appliance 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 being copied to will be replaced.

For more information, see *Port Alert Add command* on page 43, *Port Alert Copy command* on page 43 and *Port Alert Delete command* on page 44.

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* on page 63.

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* on page 60.

CHAPTER 4

Using CCM Appliance Commands

Accessing the CLI

You may access the CLI in three ways: using the Telnet CLI, using the console port 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.

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. Table 4.1 lists the line editing operations for VT100 compatible devices.

Table 4.1: 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.

Table 4.2 lists the line editing operations for ASCII TTY devices. There is no command line buffer available on an ASCII TTY device.

Table 4.2: 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 CCM appliance IP address with a Server Set command, a reboot is required before the change becomes effective. In these cases, the CCM database is updated when you enter the command and you are prompted that the change will not take effect until the CCM appliance reboots. You may choose to reboot at that time, or you may decline. When the unit reboots, your session and all other sessions on the CCM appliance are terminated.

Understanding Conventions

This section describes the parts of a CCM appliance 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
```

Table 4.3: 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.

Table 4.3: Command Syntax Types in Example Command (Continued)

Value	Syntax
XONXOF	Keyword value.

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

```
>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.
- When you specify the console port in commands such as Port Set and Show Port, you must enter the capitalized abbreviation **CON**.

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 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 wish to enable the “password or key” method (PW|KEY) or the “key or password” method (KEY|PW).

Command Summary

Table 4.4 lists the CCM appliance commands, including a brief description plus the required access rights and level.

Table 4.4: CCM Appliance Command Summary

Command	Description, Access Right and Access Level
Connect	Accesses devices from the console port. Access right: port-specific 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.)
Disconnect	Ends a device session initiated with Connect command. Access right: port-specific 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.)
Help	Displays information about commands. Access right: none needed Access level: all

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
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 CCM 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 CCM session. Access right: none needed Access level: all
Resume	Resumes device connection after being in CLI mode. Access right: none needed Access level: all
Server CLI	Specifies the console port type, CLI access character; enables/disables device connection from the console 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 unit's FLASH. Access right: SCON Access level: APPLIANCEADMIN
Server PPP	Enables/disables a PPP server on the console port. Access right: SCON Access level: APPLIANCEADMIN

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Server RADIUS	Specifies RADIUS server parameters. Access right: SCON Access level: APPLIANCEADMIN
Server Reboot	Reboots the unit. Access right: SCON Access level: APPLIANCEADMIN
Server Security	Specifies the user authentication mode, enables/disables security lock-out and connection methods. Access right: SCON Access level: APPLIANCEADMIN
Server Set	Changes the CCM appliance network configuration. 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
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 CCM appliance 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

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Show Server	Displays CCM appliance 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 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
SPC	Changes SPC port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
User Add	Adds a new user. Access right: USER Access level: ADMIN or APPLIANCEADMIN
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 (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)
User Set	Changes a user's configuration information. Access right: USER Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
User Unlock	Unlocks a locked-out user. Access right: USER Access level: ADMIN or APPLIANCEADMIN (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)

CHAPTER 5

CCM Appliance Commands

Connect Command

The Connect command establishes a connection from the CCM console management appliance console port to a device attached to another port on that CCM appliance. 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* on page 12.

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

Syntax

CONNECT <*port*>

Table 5.1: Connect Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-48.

Example

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

```
> connect 6
```

Disconnect Command

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

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

Syntax

DISCONNECT

Help Command

The Help command displays information about CCM appliance commands.

Access right: none needed
Access level: none needed

Syntax

HELP [<*command_name*>]

Table 5.2: 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
```

Port Commands

The Port command has several forms, as listed in Table 5.3.

Table 5.3: 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 CCM session on a specified port.
Port Set	Changes CCM 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 CCM Appliance Using SNMP* on page 28.

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

Syntax

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

Table 5.4: Port Alert Add Command Parameters

Parameter	Description
<*port*>	Port number in the range 1-48.
<*string*>	3-32 character string. If the string contains embedded spaces, it must be enclosed in quotation marks.

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 CCM Appliance Using SNMP* on page 28.

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

Syntax

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

Table 5.5: Port Alert Copy Command Parameters

Parameter	Description
<*to_port*>	Port number where alert strings will be copied, in the range 1-48.
<*from_port*>	Port number from which alert strings will be copied, in the range 1-48.

Example

The following command copies the alert strings defined on port 1 to port 17, replacing any previously defined alert strings on port 17.

```
port 17 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 CCM Appliance Using SNMP* on page 28.

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

Syntax

PORT <*port*> ALERT DELETE

Table 5.6: Port Alert Delete Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-48.

Example

The following command deletes defined alert strings from port 26.

```
> PORT 26 ALERT DELETE
Alert-strings assigned to port 26:
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 a 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* on page 26.

Access right: none needed
Access level: all

Syntax

PORT HISTORY

When you are in port history mode, you may issue the commands listed in Table 3.5 on page 26.

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 CCM appliance session on a specified port.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> LOGOUT

Table 5.7: Port Logout Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-48.

Port Set command

The Port Set command changes serial port settings in the CCM configuration database. At least one keyword parameter and value must be specified. Some changes become effective upon the next connection to the port.

For more information, see *Configuring Serial Port Settings* on page 11.

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*>]

Table 5.8: Port Set Command Parameters

Parameter	Description
<*port*>	A port number in the range 1-48, a range of port numbers separated by a dash, multiple port numbers separated by commas or CON. Default = port to which you are attached
ALL	Indicates that the port settings that follow should be applied to all ports except the console port.
TD=<*device*>	Target device type. Valid values are Console and SPC. The SPC value is reserved for future functionality. Default = Console
NAME=<*name*>	Port name, up to 32 characters. If the name contains spaces, enclose the name in double quotes. To return a port name to its default value (last three octets of the MAC address plus the port number), specify Name="". Default = last 3 octets of MAC address plus the port number
BAUD=<*baud*>	Baud rate. Valid values are: 75, 110, 134, 150, 200. 300, 600, 1200, 2400, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 57600 and 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 0-90. 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. The new value does not affect an active session; it takes effect in subsequent sessions. This value overrides the time-out value set with a Server CLI command. Default = use value set with Server CLI command

Table 5.8: 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 in subsequent sessions. When SSH is enabled, the CCM appliance 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 0x41-0x5F and 0x61-0x7A.) 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 CCM appliance 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
```

Quit Command

The Quit command terminates the current CCM appliance session and terminates your Telnet connection to the unit.

Access right: none needed
Access level: all

Syntax

QUIT

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

Server Commands

The Server command has several forms, as listed in Table 5.9.

Table 5.9: Server Command Summary

Command	Description
Server CLI	Specifies the console port type, CLI access character, modem initialization string, port history mode operations and port time-out value. It also enables/disables device connection from the console port.
Server FLASH	Updates the unit's FLASH.
Server PPP	Enables/disables PPP connections to the console port.
Server RADIUS	Specifies RADIUS server parameters.
Server Reboot	Reboots the unit.
Server Security	Specifies user authentication method, enables/disables security lock-out and enables/disables connection methods.
Server Set	Changes the CCM appliance network configuration.
Server SNMP	Enables/disables UDP port 161 SNMP processing.
Server SNMP Community	Defines read, write and trap SNMP community strings.
Server SNMP Manager	Defines/deletes SNMP management entities.

Table 5.9: Server Command Summary (Continued)

Command	Description
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 CCM appliance and specifies the SSH authentication method.

Server CLI command

The Server CLI command:

- Specifies the console port type
- Specifies the CLI access character
- Enables or disables device connection from the console 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 [TYPE=<*type*>] [CHAR=^<*char*>] [CONNECT=ON|OFF] [HISTORY=HOLD|AUTO,CLEAR|KEEP] [MODEMINIT="<*string*>"] [TIMEOUT=<*time-out*>]

Table 5.10: Server CLI Command Parameters

Parameter	Description
TYPE=<*type*>	Terminal type to be used on the console port. The entire name of the type must be specified; abbreviations are not permitted. Valid types are: ASCII, VT52, VT100, VT102, VT220 and VT320. Default: ASCII
CHAR=^<*char*>	CLI access character in the range A through _ (underscore). (The allowable ASCII range is 0x41-0x5F and 0x61-0x7A.) 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

Table 5.10: Server CLI Command Parameters (Continued)

Parameter	Description
CONNECT=ON|OFF	Enables or disables the ability to use the Connect command from the console port. When enabled, a console port user may use the Connect command to establish a connection to the serial device attached to another CCM appliance serial port. When disabled, you cannot use the Connect command from the console 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): Hold Upon connection you are informed of how much data is in the history buffer, but the data is not displayed. Auto Upon connection you are informed of how much data is in the history buffer, and it is then displayed. Clear The history buffer's content is cleared when a session ends. Keep 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 S0=1. Default = "" (no modem is attached to the console port)
TIMEOUT=<*time-out*>	Number of time-out minutes in the range 0-90. 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 CCM 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

Server FLASH command

The Server FLASH command updates the CCM appliance 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.

There are two program images that you may update in the CCM appliance FLASH. The boot image file (ccm50bt.img) contains the CCM appliance startup and self-test logic. The application image (ccm50app.img) contains the program that provides CCM appliance functionality.

You will need a TFTP server. Download the latest FLASH image from the Equinox web site, www.equinox.com, and save the image file to the appropriate directory on the TFTP server.

NOTE: Powering down a system in the middle of a boot FLASH update may render the unit inoperable. To update the bootstrap, it is recommended that the unit be placed on a UPS under controlled conditions to avoid interruption of the boot FLASH update process.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

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

Table 5.11: Server FLASH Command Parameters

Parameter	Description
BOOT|APP	Indicates either the boot image should be updated or 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 boot image program using the image file name c:\winnt\system32\drivers\ccm50bt.img, which is located on the TFTP server host located at 192.168.1.16.

```
> ser fla app hostip=192.168.1.16
c:\winnt\system32\drivers\ima=ccm50bt.img
```

Server PPP command

The Server PPP command enables or disables the PPP server on the console port. For more information and requirements, see *Connecting to devices using PPP* on page 15 and *Configuring and using dial-in connections* on page 14.

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 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*>]

Table 5.12: Server PPP Command Parameters

Parameter	Description
DISABLE|ENABLE	Disables or enables the PPP server.
LOCALIP=<*local_ip*>	IP address to be used to connect the CCM appliance over the PPP connection. Must be on same subnet as REMOTEIP address.

Table 5.12: Server PPP Command Parameters (Continued)

Parameter	Description
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*>	Subnet mask 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 CCM RADIUS client. For more information, see *RADIUS authentication* on page 23.

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

Table 5.13: Server RADIUS Command Parameters

Parameter	Description
PRIMARY| SECONDARY	Indicates either the primary RADIUS server or 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.

Table 5.13: Server RADIUS Command Parameters (Continued)

Parameter	Description
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=ThePrimaryRadSecret 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 CCM appliance. During a reboot, any active Telnet sessions, including your own, are terminated, and all users are informed accordingly. Any 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 the authentication method, enables/disables access methods and enables/disables security lock-out. For more information, see *Using Authentication Methods* on page 23, *Enabling plain text Telnet and SSH connections* on page 18 and *Using security lock-out* on page 25.

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*>] [ENCRYPT=<*conns*>] [LOCKOUT=<*hours*>]

Table 5.14: Server Security Command Parameters

Parameter	Description
AUTHENTICATION=<*auth*>	Authentication method. You may specify multiple values (other than None), separated by commas. Valid values are: LOCAL Use the local CCM user database to authenticate users. RADIUS Use the previously defined RADIUS server(s) to authenticate users. NONE Do not authenticate users. This method cannot be used when SSH access is enabled, and it cannot be combined with other authentication methods. 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 zero value. Default = 0 (disabled)

Server Set command

The Server Set command changes CCM appliance address settings. You may specify one, two or all three parameters. A reboot is required if you change the IP address.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

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

Table 5.15: Server Set Command Parameters

Parameter	Description
IP=<*ip_address*>	IP address.
MASK=<*subnet*>	Subnet mask for the subnet on which the CCM appliance 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 CCM Appliance Using SNMP* on page 28.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP ENABLE|DISABLE

Table 5.16: 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.

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.

For more information, see *Managing the CCM Appliance Using SNMP* on page 28.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

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

Table 5.17: 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 CCM appliance may be accessed using SNMP from any IP address.

For more information, see *Managing the CCM Appliance Using SNMP* on page 28.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP MANAGER ADD|DELETE <*ip_address*>

Table 5.18: 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 CCM appliance displays a numbered list of all currently disabled traps. When you issue this command with the Disable parameter, a numbered list of all currently enabled traps is displayed.

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 CCM Appliance Using SNMP* on page 28 and *Supported Traps* on page 78.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP [ENABLE|DISABLE] [ALL]

Table 5.19: 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 CCM appliance 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 CCM Appliance Using SNMP* on page 28.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

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

Table 5.20: 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 CCM appliance and specifies the SSH authentication method. When you enable SSH, all CCM sessions will be

terminated if a CCM SSH server key must be generated. You must also have previously specified an authentication method other than None with the Server Security command.

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* on page 15.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

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

Table 5.21: Server SSH Command Parameters

Parameter	Description
ENABLE|DISABLE	Enables or disables SSH session access to the CCM appliance.
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

Show Commands

The Show command has several forms, as listed in Table 5.22.

Table 5.22: 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 CCM configuration information and statistics.
Show Server CLI	Displays CCM CLI settings.
Show Server PPP	Displays CCM PPP settings.
Show Server RADIUS	Displays CCM RADIUS settings.
Show Server Security	Displays CCM authentication, connection and security lock-out settings.

Table 5.22: Show Command Summary (Continued)

Command	Description
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]

The SHOW PORT NAMES command display includes the 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.

Table 5.23: Show Port Command Parameter

Parameter	Description
<*port*>	Either a port number in the range 1-48 or CON. Default = your port
ALL	Displays information about all ports.
NAMES	Displays port numbers and associated logical names.

Table 5.24 lists the display fields for a Show Port command that specifies one or all ports.

Table 5.24: Show Port Command Display Fields

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 (from Port Set command). 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.

Table 5.24: Show Port Command Display Fields (Continued)

Field	Content
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 **	Port name assigned with the Port Set command or the default name (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 Access commands).
Access *	User's access rights (from User Add and User Set Access commands).
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 being accessed.

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

Table 5.25: Show Port Alert Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-48.

Show Server command

The Show Server command displays CCM appliance configuration information and statistics.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER

Table 5.26: Show Server Command Display Fields

Field	Content
Server	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).
Up Time	Days, hours, minutes and seconds since unit was rebooted.
MAC	Ethernet MAC address.
S/N	Serial number.
Port	Port number.
Username	Username (from User Add command).
Duration	Duration of session.
Socket	Telnet 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 serial CLI settings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER CLI

Table 5.27: Show Server CLI Command Display Fields

Field	Contents
CLI Port	Console port terminal type.
Access Character	Control character used to access the CLI.

Table 5.27: Show Server CLI Command Display Fields (Continued)

Field	Contents
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.
Connect	Indicates whether a valid user on the console port may use the Connect command.
Modeminit string	String used to initiate modem connections on the console 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 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 CCM 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 authentication, connection and lock-out settings that were configured with the Server Security and Server SSH commands.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER SECURITY

Table 5.28: 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.
Fingerprint (BB)	SSH key bubble babble.

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]

Table 5.29: 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 Table 5.30.

Table 5.30: 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 or PCON 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 socket number.
From Socket	Telnet client IP address and socket number.

A Show User All command display includes the information in Table 5.31.

Table 5.31: 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 or PCON but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User's access rights.

SPC Command

The SPC command is reserved for future functionality.

User Commands

The User command has several forms, as listed in Table 5.32.

Table 5.32: User Command Summary

Command	Description
User Add	Adds a new user to the user database.
User Delete	Deletes a user from the user database.
User Logout	Terminates a user's active 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 CCM user database. The user database holds a maximum of 64 user definitions. For more information, see *Managing User Accounts* on page 20 and *Access rights and levels* on page 21.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

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

Table 5.33: User Add Command

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 may 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.

Table 5.33: User Add Command (Continued)

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 Can 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 CCM appliance commands.

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

User Delete command

The User Delete command removes a username entry from the CCM user database. The username may no longer be used to authenticate a session with the CCM appliance. 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*>

Table 5.34: 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 CCM appliance. 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: ADMIN (may log out all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER LOGOUT <*username*>

Table 5.35: 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 user database. For more information, see *Managing User Accounts* on page 20 and *Access rights and levels* on page 21.

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*>]

Table 5.36: 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 may be received is 4K bytes.
FTPIP=<*ftpadd*>	FTP server's IP address.

Table 5.36: User Set Command Parameters (Continued)

Parameter	Description
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 Can 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 configuration 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: ADMIN (may unlock all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER UNLOCK <*username*>

Table 5.37: User Logout Command Parameter

Parameter	Description
<username>	Username to be unlocked.

APPENDICES

Appendix A: Technical Specifications

Table A.1: CCM4850 Appliance Technical Specifications

Item	Value
Device Ports	
Number	48
Type	Serial ports
Connectors	Serial port RJ-45
Console Port	
Number	1
Connector	Serial port RJ-45
Network Connection	
Number	1
Type	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT Gigabit Ethernet: IEEE 802ab, 1000Base T
Connector	RJ-45
Dimensions	
H x W x D	4.45 x 25.40 x 44.45 cm 1U form factor (1.75 x 10.00 x 17.50 in)
Weight	5 lbs (2.27 kg) without cables
Heat Dissipation	205 BTU/hr
Airflow	14 cfm
Power Consumption	60 W measured
AC-input power	90 W maximum
AC-input maximum	100 to 240 VAC
AC-input current rating	1 A maximum

Table A.1: CCM4850 Appliance Technical Specifications (Continued)

Item	Value
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	0^{o} to 55^{o} Celsius (32^{o} to 131^{o} Fahrenheit) operating -40^{o} to $+70^{o}$ Celsius (-40^{o} to $+158^{o}$ Fahrenheit) nonoperating
Humidity	10% to 90% noncondensing
Safety and EMC Standards	UL 60950-1, CSA C22.2 No. 60950-00-CAN/CSA (UL cUL Listed), IEC 60950 (1999-04) 3rd Edition, CENELEC EN 60950
Regulatory Compliance	FCC P. 15 Class A, ICES-003, EN 55022: 1998 Class A, EN 61000-3-2, EN 61000-3-3, AS/NZS 3548: 1995, CNS 13438 - Issued: 1997/01/01, VCCI V-3/01/04 Class A, EN 55024-1998. The products herewith comply with the requirements of the Low Voltage Directive, 73/23/EEC and the EMC Directive 89/336/EEC, including amendments by the CE-marking Directive 93/68/EEC.

Appendix B: Device Cabling

Each CCM appliance serial port has an RJ-45 connector for attaching a serial device. Table B.1 lists the pin assignments.

Table B.1: Port Pin Assignments

Pin Number	RS-232 Signal	Direction	Description
1	RTS	Output	Request to Send
2	DSR	Input	Data Set Ready
3	DCD	Input	Data Carrier Detect
4	RD	Input	Receive Data
5	TD	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			

Modular adaptors are available from Equinox to convert RJ-45 modular jacks to standard pinout configurations. Adaptors are available for use with:

- CAT 5 and CAT 6 cable.
- Serial reversing cable. Reversing adaptors and cables are recommended for distances greater than 100 feet.

Adaptors for use with CAT 5 and CAT 6 cable

Table B.2 lists the adaptors available from Equinox for use with CAT 5 and CAT 6 cable.

Table B.2: Adaptors for Use with CAT 5 and CAT 6 Cable

Part Number	Description
210122	RJ-45 to DB-9M (DTE) Adaptor
210120	RJ-45 to DB-9F (DCE) Adaptor
210124	RJ-45 to DB-25M (DTE) Adaptor
210123	RJ-45 to DB-25M (DCE) Adaptor
210125	RJ-45 to DB-25F (DTE) Adaptor
210121	RJ-45 to DB-25F (DCE) Adaptor

Table B.2: Adaptors for Use with CAT 5 and CAT 6 Cable (Continued)

Part Number	Description
210127	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
750238	CAT 5 Serial Starter Kit - includes all the above adaptors

Figure B.1 shows the pin assignments for the adaptors listed in Table B.2.

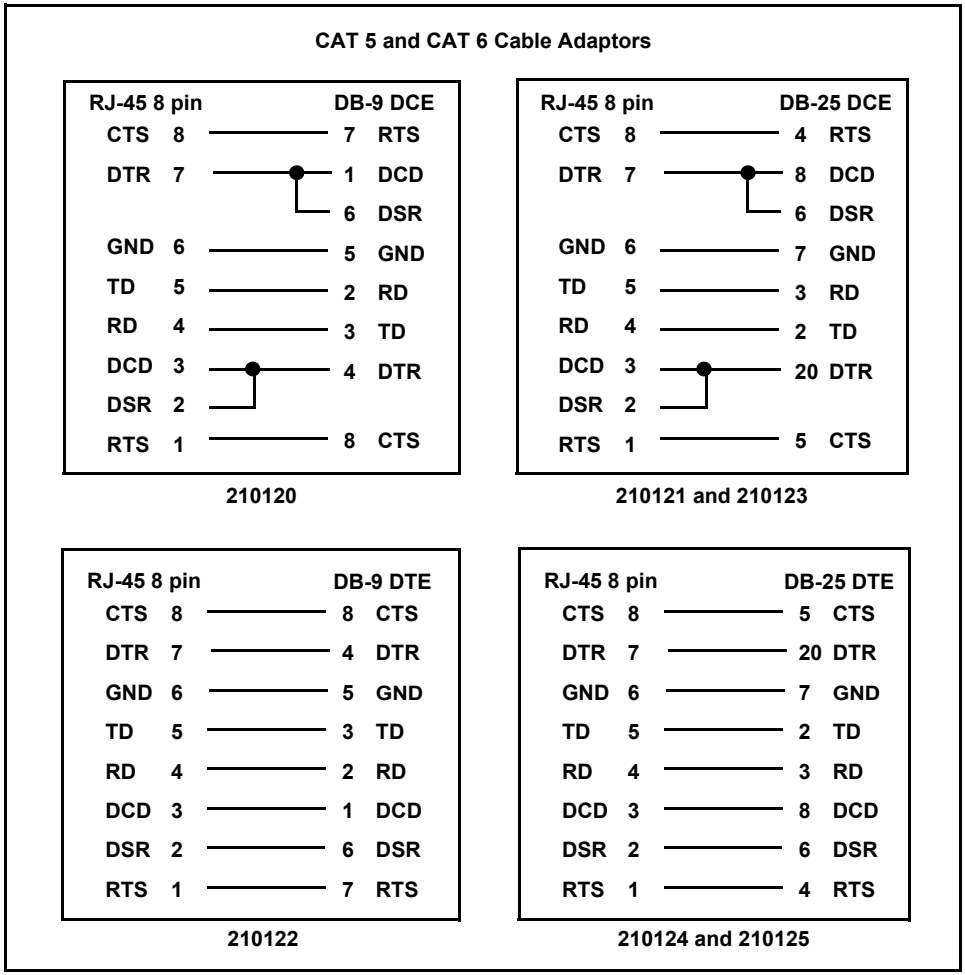

Figure B.1: CAT 5 and CAT 6 Cable Adaptor Pin Assignments

Reversing adaptors and cables

Table B.3 lists the reversing adaptors and reversing cables available from Equinox.

Table B.3: Reversing Adaptors and Cables

Part Number	Description
210094	RJ-45 to DB-9M (DTE) Adaptor
210095	RJ-45 to DB-9F (DCE) Adaptor
210090	RJ-45 to DB-25M (DTE) Adaptor
210092	RJ-45 to DB-25M (DCE) Adaptor
210091	RJ-45 to DB-25F (DTE) Adaptor
210093	RJ-45 to DB-25F (DCE) Adaptor
210105	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
690226	10 foot 8-wire Reversing Modular Cable
690227	25 foot 8-wire Reversing Modular Cable
690228	75 foot 8-wire Reversing Modular Cable
750122	Wiring Starter Kit (8-wire) - includes all the above adaptors and one 690226 cable

Figure B.2 shows the pin assignments for the adaptors listed in Table B.3.

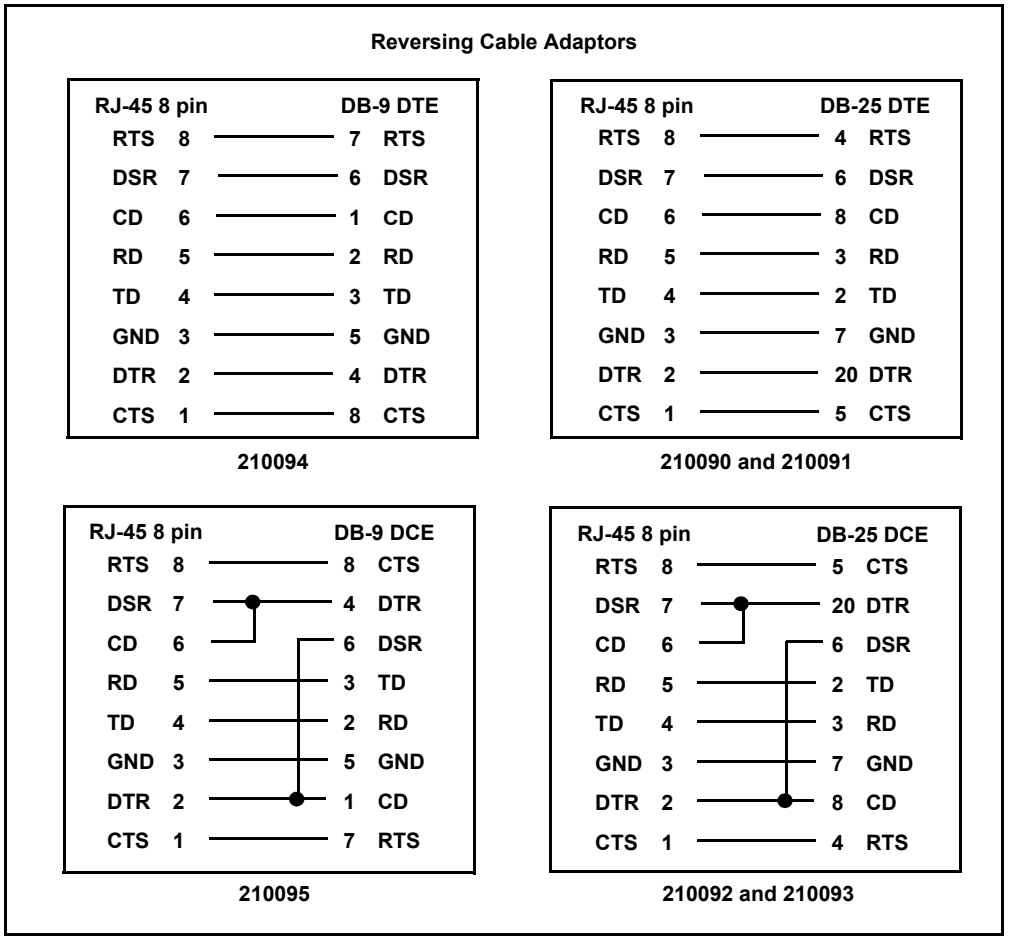

Figure B.2: Reversing Cable Adaptor Pin Assignments

If you choose to use a non-Equinox reversing cable, make sure the cable is reversing, as shown in Figure B.3.

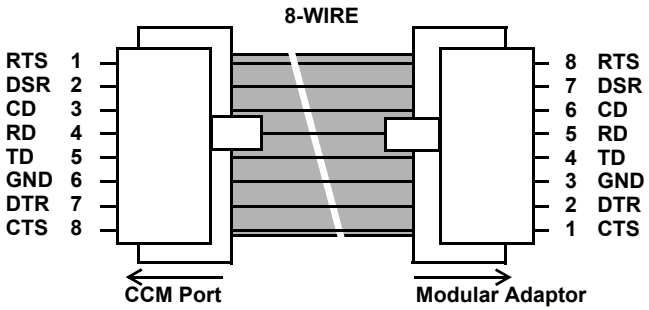

Figure B.3: 8-wire RJ-45 Reversing Cable

Appendix C: Supported Traps

The CCM appliance supports the following MIB2 traps:

- authenticationFailure
- linkUp
- linkDown
- coldStart

Table C.1 lists the supported enterprise traps. The Equinox web site, www.equinox.com, contains the complete trap MIB.

Table C.1: CCM4850 Appliance Enterprise Traps

Trap	Description and Variable(s)
RebootStarted	The CCM appliance is rebooting. Variable: initiating username
UserLogin	A user logged in to the CCM appliance. Variable: username
UserLogout	A user logged out of the CCM appliance. Variable: username
SerialSessionStarted	A serial session has started. Variables: username, server name and port number
SerialSessionStopped	A serial session has stopped. Variables: username, server name and port number
SerialSession Terminated	Another user has terminated a serial session. Variables: initiating username, terminated username, server name and port number
ImageUpgradeStarted	The CCM appliance has started an image upgrade. Variables: initiating username, image type (boot or application), new version number, current version number
ImageUpgradeResults	An image upgrade has ended. Variables: result (successful or error code), initiating username, image type (boot or application), upgrade version number and running version number (if the upgrade was successful, the two version numbers will match)
UserAdded	A new user has been added to the CCM appliance user database. Variables: initiating username and new username
UserDeleted	A user has been deleted from the CCM appliance user database. Variables: initiating username and deleted username
UserModified	A user's definition has been modified in the CCM appliance user database. Variables: initiating username and modified username

Table C.1: CCM4850 Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
UserAuthentication Failure	A user failed to authenticate with the CCM appliance. Variable: username
FactoryDefaultsSet	The CCM appliance has received a command to set itself to factory default values. (The appliance sends this trap after receiving the command, but before actually reverting to factory default values.)
PortAlert	The CCM appliance detected a port alert string on a serial port. Variables: server name, port number and port alert string
ConfigurationFile Loaded	The CCM appliance has loaded a configuration file. This trap applies to AVWorks software. Variables: initiating username and name of loaded file
UserDatabaseFile Loaded	The CCM appliance has loaded a user database file. This trap applies to AVWorks software. Variables: initiating username and name of loaded file
PortPowerOnDetect	The CCM appliance detected that a port's power on/off control signal is in the state indicating power is on. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number
PortPowerOffDetect	The CCM appliance detected that a port's power on/off control signal is in the state indicating power is off. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number
UserLocked	A user account has been locked. Variables: client IP address, locked username and reason
UserUnlocked	A user account has been unlocked. Variables: client IP address, initiating username, unlocked username and reason
AggregatedServer StatusChanged	The status of one or more servers (connections paths) has changed. The appliance always sends this trap upon bootup. Thereafter, it sends the trap when there is a change in connection path status, and will include only those paths whose status has changed. Variable(s): connection path(s)

Appendix D: Ports Used

Table D.1 lists the UDP and TCP port numbers used by the CCM appliance. The values assume a default configuration; some values are configurable.

Table D.1: Ports Used by CCM Appliance

Port Type and Number	Used for
TCP 22	SSH2, if enabled.
TCP 23	Telnet.
UDP 69	TFTP
UDP 161	SNMP, if enabled.
UDP 3211	Secure protocol used by AVWorks software.
TCP 3211	Secure protocol used by AVWorks software.
TCP 3001-3048	Telnet serial sessions with ports 1-48.
TCP 3101-3148	SSH serial sessions with ports 1-48.

Appendix E: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating problems you encounter with your Equinox product. If an issue should develop, follow the steps below for the fastest possible service:

1. Check the pertinent section of the manual to see if the issue may be resolved by following the procedures outlined.
2. Check our web site at www.equinox.com/support to search the knowledge base or use the on-line service request.
3. Call Equinox Technical Support for assistance at (954) 746-9000, ext. 322. Visit the Equinox web site at http://www.equinox.com/support and click on *Support - Getting Support* for current phone support hours.

INDEX

A

B

C

L

M

P

Q

R

S

T

U

LIMITED WARRANTY

Equinox warrants that the Product(s) shall be free from manufacturing defects in materials and workmanship for a period of five (5) years from the date of delivery provided that the Product was properly installed and used. Defects, malfunctions or failures of the warranted Product caused by damage resulting from acts of God (such as floods, fire, etc.), environmental and atmospheric disturbances, other external forces such as power line disturbances, host computer malfunction, plugging the board in under power, or incorrect cabling and damage caused by misuse, abuse and unauthorized alteration or repair are not warranted.

This warranty is limited to the repair and/or replacement, at Equinox' option, of the defective Product during its warranty period. Customer must obtain a Return Material Authorization (RMA) number prior to returning the defective Product to Equinox for service. Customer agrees to insure the Product or assume the risk of loss or damage in transit, to prepay shipping charges and to use the original shipping container or equivalent. Contact Equinox Customer Support at 954-746-9000 for further information. Product repaired or replaced shall be warranted for a period of ninety (90) days or for the duration of the initial Product warranty period, whichever is longer.

THE PROVISIONS OF THE WARRANTY ARE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED, WRITTEN OR ORAL, AND EQUINOX' LIABILITY ARISING OUT OF THE MANUFACTURE, SALE OR SUPPLYING OF THE PRODUCT AND ITS USE, WHETHER BASED ON WARRANTY, CONTRACT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE ORIGINAL COST OF THE PRODUCT. IN NO EVENT SHALL EQUINOX BE LIABLE FOR UNINTENDED OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR USE DAMAGES ARISING OUT OF THE MANUFACTURE, SALE OR SUPPLYING OF THE PRODUCT.

EQUINOX®
an Avocent Company

For Technical Support:

Email: support@equinox.com
www.equinox.com

Equinox Systems
One Equinox Way
Sunrise, Florida
33351 USA
Tel: 954.746.9000

590-373-001B