



Avocent.

Cyclades[®] CS Console Server

Installation, Administration and User Guide



FCC Warning Statement

The Cyclades CS console server has been tested and found to comply with the limits for Class A digital devices, 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 Cyclades CS Console Server Installation, Administration and User Guide, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the problem at his or her own expense.

Notice about FCC Compliance for All Cyclades CS Console Server Models

To comply with FCC standards, the Cyclades CS console server requires the use of a shielded CAT 5 cable for the Ethernet interface. Notice that this cable is not supplied with either of the products and must be provided by the customer.

Canadian DOC Notice

The Cyclades CS console server 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.

L'Avocent Cyclades CS console server 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.



Cyclades[®] CS Console Server

Installation, Administration and User Guide

Avocent, the Avocent logo and The Power of Being There and Cyclades are registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2007 Avocent Corporation. All rights reserved. 590-752-501A



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.

TABLE OF CONTENTS

Chapter 1: Installation	1
<i>Overview</i>	<i>1</i>
<i>Product Models and Configurations</i>	<i>1</i>
<i>Accessing the Cyclades CS Console Server and Connected Devices.....</i>	<i>1</i>
<i>Web Manager.....</i>	<i>2</i>
<i>Prerequisites for Using the Web Manager.....</i>	<i>2</i>
<i>Types of Users.....</i>	<i>3</i>
<i>Important Pre-installation Requirements</i>	<i>3</i>
<i>Basic Installation Procedures.....</i>	<i>3</i>
<i>Making an Ethernet connection.....</i>	<i>4</i>
<i>Making a direct connection to configure the network parameters.....</i>	<i>4</i>
<i>Turning on the console server and the connected devices</i>	<i>5</i>
<i>Performing basic network configuration using the wiz command</i>	<i>5</i>
<i>Adding users and configuring ports using the Web Manager.....</i>	<i>7</i>
<i>Other Methods of Accessing the Web Manager.....</i>	<i>8</i>
Chapter 2: Web Manager for Regular Users.....	9
<i>Using the Web Manager</i>	<i>9</i>
<i>Features of Regular User Forms</i>	<i>10</i>
<i>Connect</i>	<i>10</i>
<i>Connect to the console server.....</i>	<i>11</i>
<i>Connect to serial ports</i>	<i>11</i>
<i>Connection protocols for serial ports.....</i>	<i>12</i>
<i>Security</i>	<i>12</i>
Chapter 3: Web Manager for Administrators.....	13
<i>Common Features of Administrator Forms.....</i>	<i>13</i>
<i>Logging Into the Web Manager.....</i>	<i>14</i>
<i>Overview of Administrative Modes.....</i>	<i>15</i>
<i>Wizard mode</i>	<i>15</i>
<i>Expert mode</i>	<i>16</i>
Chapter 4: Configuring the Cyclades CS Console Server in Wizard Mode.....	17

<i>After Logging In</i>	17
<i>Step 1: Network Settings</i>	17
<i>Step 2: Port Profile</i>	19
<i>Step 3: Access</i>	21
<i>Step 4: Data Buffering</i>	23
<i>Step 5: System Log</i>	26
Chapter 5: Applications	27
<i>Configuring the Console Server in Expert Mode</i>	27
<i>Overview of menus and forms</i>	27
<i>Mapping the expert mode menus and forms</i>	28
<i>Applications Menu and Forms</i>	29
<i>Connect</i>	29
<i>Terminal Profile menu</i>	30
Chapter 6: Network Menu and Forms	33
<i>Host Settings</i>	34
<i>Syslog</i>	36
<i>SNMP</i>	37
<i>Firewall Configuration</i>	41
<i>Host Table</i>	49
<i>Static Routes</i>	49
Chapter 7: Security Menu and Forms	53
<i>Users and Groups</i>	53
<i>Active Ports Sessions</i>	56
<i>Authentication</i>	57
<i>Configuring authentication for console server logins</i>	57
<i>Configuring authentication servers for logins to the console server and connected devices</i> ..	58
<i>Security certificates</i>	61
Chapter 8: Ports Menu and Forms	63
<i>Physical Ports</i>	63
<i>Virtual Ports</i>	77
<i>Ports Status</i>	80
<i>Ports Statistics</i>	81

Chapter 9: Administration Menu and Forms	83
<i>System Information</i>	<i>83</i>
<i>Notifications.....</i>	<i>84</i>
<i>Time/Date.....</i>	<i>87</i>
<i>Boot Configuration</i>	<i>89</i>
<i>Backup Configuration.....</i>	<i>90</i>
<i>Upgrade Firmware</i>	<i>92</i>
<i>Reboot.....</i>	<i>93</i>
<i>Online Help.....</i>	<i>93</i>
Appendices.....	97
<i>Appendix A: Technical Specifications</i>	<i>97</i>
<i>Appendix B: Safety, Regulatory and Compliance Information.....</i>	<i>98</i>
<i>Appendix C: Technical Support.....</i>	<i>104</i>
Index.....	105

LIST OF FIGURES

<i>Figure 1.1: Placement of Mounting Brackets (Forward Mounting Configuration Shown)</i>	3
<i>Figure 1.2: Configuration Wizard Screen</i>	6
<i>Figure 2.1: Regular User Form</i>	10
<i>Figure 3.1: Administrator - Web Manager Buttons</i>	13
<i>Figure 3.2: Example of Web Manager Form in Wizard Mode</i>	15
<i>Figure 3.3: Example of Web Manager Form in Expert Mode</i>	16
<i>Figure 4.1: Wizard - Step 1: Network Settings - DHCP Disabled</i>	17
<i>Figure 4.2: Wizard - Step 1: Network Settings - DHCP Enabled</i>	18
<i>Figure 4.3: Wizard - Step 2: Port Profile</i>	19
<i>Figure 4.4: Wizard - Step 3: Access</i>	21
<i>Figure 4.5: Wizard - Step 3: Access Add User Dialog Box</i>	21
<i>Figure 4.6: Wizard - Step 3: Change Password Dialog Box</i>	22
<i>Figure 4.7: Wizard - Step4: Data Buffering [Local]</i>	24
<i>Figure 4.8: Wizard - Step 4: Data Buffering [Remote]</i>	24
<i>Figure 4.9: Wizard - Step 5: System Log</i>	26
<i>Figure 5.1: Expert Mode Forms Elements</i>	27
<i>Figure 5.2: Expert - SSH session Java Applet</i>	29
<i>Figure 5.3: Expert - Applications - Empty Terminal Profile Menu</i>	30
<i>Figure 5.4: Expert - Terminal Profile Menu Example</i>	31
<i>Figure 6.1: Expert - Network - Host Settings [DHCP Enabled]</i>	34
<i>Figure 6.2: Expert - Network - Host Settings [DHCP disabled]</i>	34
<i>Figure 6.3: Expert - Network - Syslog</i>	36
<i>Figure 6.4: Expert - Network - SNMP</i>	38
<i>Figure 6.5: Expert - New/Mod SNMP v1 v2 Configuration Dialog Box</i>	39
<i>Figure 6.6: Expert - New/Mod SNMP v3 Configuration Dialog Box</i>	40
<i>Figure 6.7: Expert - Network - Firewall Configuration</i>	41
<i>Figure 6.8: Expert - Firewall Configuration Edit Chain Dialog Box</i>	42
<i>Figure 6.9: Expert - Firewall Configuration Add Chain Dialog Box</i>	42
<i>Figure 6.10: Firewall Configuration Edit Rules for chain_name Form</i>	43
<i>Figure 6.11: Firewall Configuration Edit Rules for chain_name Buttons</i>	43
<i>Figure 6.12: Expert - Firewall Configuration Add Rule and Edit Rule Dialog Boxes</i>	43
<i>Figure 6.13: Firewall Configuration TCP Protocol Fields and Menu Options</i>	44
<i>Figure 6.14: Firewall Configuration Add Rule and Edit Rule UDP Protocol Fields</i>	45

<i>Figure 6.15: Input/Output Interface Fields and Fragments Menu Options</i>	46
<i>Figure 6.16: Firewall Configuration Add Rule and Edit Rule LOG Target Fields</i>	46
<i>Figure 6.17: Firewall Configuration Add Rule and Edit Rule REJECT Target Menu Options</i>	47
<i>Figure 6.18: Edit Chain Dialog Box</i>	48
<i>Figure 6.19: Expert - Network - Host Tables</i>	49
<i>Figure 6.20: Expert - Network - Static Routes</i>	50
<i>Figure 6.21: Expert - Static Routes Add and Edit Dialog Boxes - Default Route</i>	50
<i>Figure 6.22: Expert - Static Routes Add and Edit Dialog Boxes - Network Route</i>	50
<i>Figure 6.23: Expert - Static Routes Add and Edit Dialog Boxes - Host Route</i>	51
<i>Figure 7.1: Expert - Security - Users and Groups Form</i>	53
<i>Figure 7.2: Expert - Security - Active Ports Sessions</i>	56
<i>Figure 7.3: Expert - Security - Authentication</i>	57
<i>Figure 7.4: Expert - Security - Authentication - LDAP</i>	60
<i>Figure 7.5: Expert - Physical Ports Default Factory Settings</i>	61
<i>Figure 8.2: Ports - Physical Ports - General Form</i>	65
<i>Figure 8.3: Ports - Physical Ports - Data Buffering Enabled</i>	72
<i>Figure 8.4: Ports - Virtual Ports</i>	77
<i>Figure 8.5: Ports - Virtual Ports - New/Modify Port Dialog Box</i>	78
<i>Figure 8.6: Ports - Virtual Ports - New/Modify Port Dialog Box</i>	79
<i>Figure 8.7: Ports - Virtual Ports - New/Modify - Port Names Dialog box</i>	80
<i>Figure 8.8: Ports - Ports Status (Read-Only)</i>	80
<i>Figure 8.9: Ports - Port Statistics (Read-Only)</i>	81
<i>Figure 9.1: Expert - Administration - Time/Date</i>	87
<i>Figure 9.2: Expert - Administration - Time and Date - NTP Enable</i>	88
<i>Figure 9.3: Expert - Administration - Time/Date - Edit Custom</i>	88
<i>Figure 9.4: Expert - Administration - Online Help</i>	93

LIST OF TABLES

<i>Table 1.1: Cyclades CS Console Server Models</i>	<i>1</i>
<i>Table 1.2: Cyclades CS Console Server Serial Port Pinout.....</i>	<i>5</i>
<i>Table 2.1: Common Form Information.....</i>	<i>10</i>
<i>Table 2.2: Java Applet Buttons for Connecting to the Console Server.....</i>	<i>11</i>
<i>Table 2.3: Available Serial Port Protocols</i>	<i>12</i>
<i>Table 3.1: Description of Administrator Web Manager Buttons.....</i>	<i>13</i>
<i>Table 3.2: Administrator - Logout Button and Other Information in the Upper Right Corner</i>	<i>14</i>
<i>Table 4.1: Port Profile Setup Options</i>	<i>19</i>
<i>Table 4.2: Wizard - Data Buffering Field Names and Definitions.....</i>	<i>25</i>
<i>Table 5.1: Expert Mode Forms Elements Information.....</i>	<i>28</i>
<i>Table 5.2: Expert Mode Menu and Forms, Applications, Network and Security.....</i>	<i>28</i>
<i>Table 5.3: Expert Mode Menu and Forms, Ports and Administration.....</i>	<i>28</i>
<i>Table 6.1: Expert - Network Menu Descriptions.....</i>	<i>33</i>
<i>Table 6.2: Expert - Fields and Menu Options for SNMP Configuration</i>	<i>39</i>
<i>Table 6.3: Expert - TCP Options Fields.....</i>	<i>45</i>
<i>Table 6.4: Expert - Firewall Configuration Input/Output Interface and Fragments Fields</i>	<i>46</i>
<i>Table 7.1: Expert - Active Ports Sessions Information.....</i>	<i>56</i>
<i>Table 8.1: List of Procedures for Serial Port Configuration</i>	<i>64</i>
<i>Table 8.2: Connections Protocols When Serial Port is Connected to Device Console Port</i>	<i>66</i>
<i>Table 8.3: Available Connection Protocols When Terminal is Connected to a Serial Port</i>	<i>66</i>
<i>Table 8.4: Connection Protocols for Modems.....</i>	<i>67</i>
<i>Table 8.5: Access Form Menu and Fields</i>	<i>70</i>
<i>Table 8.6: Expert - Authentication Methods and Fallback Mechanisms</i>	<i>70</i>
<i>Table 8.7: Available Options from the Allow Multiple Sessions Pull-down</i>	<i>73</i>
<i>Table 8.8: Other Form Fields.....</i>	<i>74</i>
<i>Table 8.9: Expert - Port Status Read-Only Form.....</i>	<i>81</i>
<i>Table 8.10: Expert - Ports - Port Status Read-Only Form.....</i>	<i>81</i>
<i>Table 9.1: System Information Form.....</i>	<i>83</i>
<i>Table 9.2: Boot Configuration Form Fields.....</i>	<i>89</i>
<i>Table 9.3: Backup Configuration Settings if Using FTP Server</i>	<i>91</i>
<i>Table 9.4: Backup Configuration if Using Storage Device.....</i>	<i>91</i>
<i>Table A.1: Technical Specifications for the Cyclades® CS console server Hardware.....</i>	<i>97</i>

Overview

The Cyclades® CS console server is a 1U device that serves as a single access point for using and administering servers and other devices.

Product Models and Configurations

There are four models of the Cyclades CS console server based on the number of serial ports.

Table 1.1: Cyclades CS Console Server Models

Product Model Name	Number of Serial Ports
Cyclades CS4001	1
Cyclades CS4004	4
Cyclades CS4008	8
Cyclades CS4016	16

Accessing the Cyclades CS Console Server and Connected Devices

You can access the console server and the connected servers or devices locally or remotely using any of the following methods.

- Using the Web Manager through LAN/WAN IP networks.
- Using a modem, ISDN, GSM or CDMA.
- Using the Web Manager you can login and launch a console session such as Telnet or SSH to connect to the console of devices that are connected to the console server's serial ports.
- By connecting a computer running a terminal emulation program, a console server administrator can log into the console server and enter commands in the console server shell or use the Command Line Interface (CLI) tool.

NOTE: Only one user logged in as "root" or "admin" can have an active CLI or Web Manager session. A second user who connects through the CLI or the Web Manager as the "root" or "admin" has a choice to abort the session or close the other user's session.

Web Manager

Cyclades CS console server administrators perform most tasks through the Web Manager either locally or from a remote location. The Web Manager runs in a browser and provides a real-time view of all the equipment that is connected to the console server.

The console server administrator can use the Web Manager to configure users and ports. An authorized user can access connected devices through the Web Manager to troubleshoot, maintain, recycle power, and reboot connected devices.

Access to the Web Manager is through one of the following ways:

- Through the IP network.
- Through a dial-in connection with an optional external modem connected to one of the serial ports.

Prerequisites for Using the Web Manager

The prerequisites described in this section must be completed before anyone can access the Web Manager. If you have questions about any of the following prerequisites, contact your system or network administrator.

- Basic network parameters must be defined on the console server so the Web Manager can be launched over the network.
- The IP address of the console server must be known.
- When DHCP is enabled, a leased IP address is assigned to console server. The leased IP address may change every time console server reboots. Therefore, an additional step needs to be taken to find out the dynamically-assigned IP address before the Web Manager can be accessed through the browser. Following are three ways to find out the dynamically-assigned IP address:
 - Make an inquiry to the DHCP server on the subnet that the console server resides, using the MAC address (The MAC address is labeled at the bottom of the console server).
 - Connect to console server remotely using Telnet or SSH and use the `ifconfig` command.
 - Connect directly to the console server and use the `ifconfig` command through a terminal emulator application.
- A user account must be defined on the Web Manager.
- By default, the administrator has an account on the Web Manager. An administrator can add regular user accounts with permissions to access to the connected servers or devices using the Web Manager.

Types of Users

The Cyclades CS console server supports the following user account types:

- The root user who can manage the console server and its connected devices. The root user performs the initial network configuration. Access privileges are full read/write and management.

NOTE: It is recommended to change the default password **avocent** to another password before setting up the console server for secure access to the connected servers or devices.

- Users who can be part of an “Admin” group with administrative privileges. This may be a regular user who can perform the same tasks as an administrator.
- Regular users who can access the connected devices through the serial ports they are authorized for. Regular users have limited access to the Web Manager features.

Important Pre-installation Requirements

Before installing and configuring the console server, ensure that you have the following:

- Root Access on your local UNIX machine to use the serial ports
- An appropriate terminal application for your operating system
- IP address, DNS, Network Mask and Gateway addresses of your server or terminal, the console server and the machine to which the console server is connected
- A web browser that supports the console server Web Manager, such as Netscape, Internet Explorer, Firefox or Mozilla
- Java 2 Runtime Environment (JRE) version 1.4.2 or later. If a more recent version is available, go to <http://java.com> to locate and download the latest version of J2RE

Basic Installation Procedures

Mounting the console server

You can mount the Cyclades® CS console server on a wall, rack or cabinet or place it on a desktop or other flat surface. Two brackets are supplied with six hex screws for attaching the brackets to the console server for mounting.

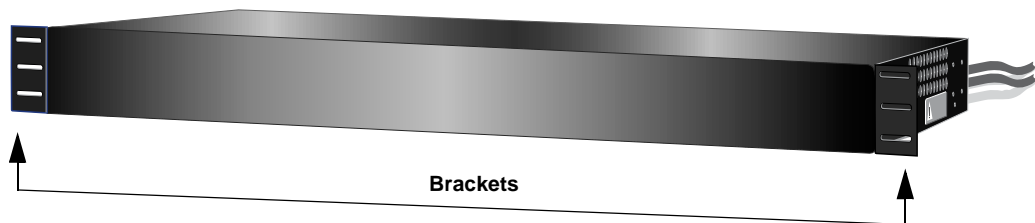


Figure 1.1: Placement of Mounting Brackets (Forward Mounting Configuration Shown)

To rack mount the console server:

1. Install the brackets on to the front or back edges of the console server using a hex screw driver and the screws provided.
2. Mount the console server unit in a secure position.

Making an Ethernet connection

Connect a CAT 5 patch cable from the console server port labeled 10/100BaseT to an Ethernet hub or switch.

To connect devices to serial ports:

Using patch cables with RJ-45 connectors and DB-9 console adaptors assemble crossover cables to connect the console server serial ports to the device's console port.

Making a direct connection to configure the network parameters.

Ensure that a suitable terminal emulation program is installed on your Windows workstation. On servers running a UNIX-based operating system such as Solaris or Linux, make sure that a compatible terminal emulator such as Kermit or Minicom is installed.

To connect to the console port:

You can use a CAT 5 straight-through cable with RJ-45 connectors and the appropriate adaptor provided with the product box to assemble a console cable. All adaptors have an RJ-45 connector on one end and either a DB25 or DB9 male or female connector on the other end.

1. Connect the RJ-45 end of the cable to the Console port on the console server.
2. Connect the adaptor end of the cable to the Console port of your server or device.
3. Open your terminal emulation program, start a connection session, select an available COM port and enter the following console parameters.
 - Bits per second: 9600 bps
 - Data bits: 8
 - Parity: None
 - Stop bit: 1
 - Flow control: None

Console server serial port pinout information

Table 1.2: Cyclades CS Console Server Serial Port Pinout

Pin No.	Signal Name	Input/Output
1	RTS	OUT
2	DTR	OUT
3	TxD	OUT
4	GND	
5	CTS	IN
6	RxD	IN
7	DCD	IN
8	DSR	IN

Turning on the console server and the connected devices

Perform the following procedures in the order shown to ensure proper operation of connected devices.

To turn on the console server:

1. Make sure the console server's power switch is off.
2. Plug in the power cable.
3. Turn the console server's power switch(es) on.

To turn on connected devices:

Turn on the power switches of the connected devices only after you have completed the physical connection to the console server.

Performing basic network configuration using the wiz command

The following procedure assumes that a hardware connection is made between the console server's Console port and the COM port of a server.

To log into the console server through the console:

From your terminal emulation application, log into the console port as **root**.

```
console server login: root
Password: avocent
```

WARNING:For security reasons, it is recommended that you change the default password **avocent** as soon as possible. To change the default password, enter the `passwd` command at the prompt and enter a new password when prompted.

NOTE: The Security Advisory appears the first time console server is accessed or after a reset to factory default parameters. If you are upgrading the firmware on the console server, the previously configured security parameters are retained in the Flash memory.

To use the `wiz` command to configure network parameters:

1. Launch the Configuration Wizard by entering the **wiz** command .

```
[root@CAS root]# wiz
```

As shown in the sample screen below, the system displays the configuration wizard banner and begins running the wizard.

```
*****
***** CONFIGURATION WIZARD *****
*****
Current configuration:

Hostname : CAS
DHCP : disabled
System IP : 192.168.48.11
Domain name : avocent.com
Primary DNS Server : 192.168.44.21
Gateway IP : 192.168.48.1
Network Mask : 255.255.252.0

Set to defaults? (y/n) [n] : _
```

Figure 1.2: Configuration Wizard Screen

2. At the prompt, enter **n** to change the defaults.

```
Set to defaults (y/n) [n] : n
```

3. Press **Enter** to accept the default hostname, otherwise enter your own hostname.

```
Hostname [CAS]: fremont_branch_console server
```

4. Press **Enter** to keep DHCP enabled or enter n to specify a static IP address for the console server. By default, the console server uses the IP address provided by the DHCP server. If your network does not use DHCP, then console server will default to 192.168.160.10.

```
Do you want to use DHCP to automatically assign an IP for your system?  
(y/n) [y] :
```

5. To change the default static IP address, enter a valid IP address at the prompt.

```
System IP[192.168.160.10]: <console_server_IP_address>
```

6. Enter the domain name.

```
Domain name[avocent.com]: <domain_name>
```

7. Enter the IP address for the Primary DNS (domain name) server.

```
Primary DNS Server[192.168.44.21] : <DNS_server_IP_address>
```

8. Enter the IP address for the gateway.

```
Gateway IP[eth0] : <gateway_IP_address>
```

9. Enter the netmask for the subnetwork.

```
Network Mask[#] : <netmask>
```

The network configuration parameters appear.

10. Enter **y** after the prompts shown in the following screen example.

```
Are all these parameters correct? (y/n) [n]: y
```

```
Do you want to activate your configurations now? (y/n) [y]: y
```

```
Do you want to save your configuration to Flash? (y/n) [n]: y
```

11. To confirm the configuration, enter the ifconfig command.

Adding users and configuring ports using the Web Manager

NOTE: From the factory, the console server is configured with all serial ports disabled.

The administrator can add users, enable or disable the serial ports and select and assign specific users to individual ports. For more information on managing users and ports, see *Security Menu and Forms* on page 53 and *Ports Menu and Forms* on page 63.

Other Methods of Accessing the Web Manager

You can access the Web Manager using either DHCP or the default IP address.

NOTE: Accessing the Web Manager using either DHCP or the default IP address requires additional setup and configuration specific to your site's network configuration.

To use a dynamic IP address to access the Web Manager:

This procedure assumes that DHCP is enabled and that you are able to obtain the dynamic IP address currently assigned to the console server.

1. Mount the console server.
2. Connect servers and other devices to be managed through the console server.
3. Power up the console server and connected devices.
4. Enter the console server's IP address in the browser's address field.
5. Log in to the console server and finish configuring users and other settings using the Web Manager.

To use the default IP address to access the Web Manager:

The default IP address for the console server is 192.168.160.10. This procedure assumes that you are able to temporarily change the IP address of a server located on the same subnet as the Cyclades CS console server.

1. On a server that resides on the same subnet as the console server, change the network portion of the IP address of that server to 192.168.160. For the host portion of the IP address, you can use any number except 10, 0 or 255.
2. Open a browser on the server with the changed address. Enter the console server's default IP address, <https://192.168.160.10>, to bring up the Web Manager and log in.

Web Manager for Regular Users

Using the Web Manager

Cyclades® CS console server users perform most tasks through the Web Manager. The Web Manager runs in a browser providing a real-time view of all other equipment connected to the console server.

The console server administrator can use the Web Manager to configure users and ports. An authorized user can access connected devices through the Web Manager to troubleshoot and maintain connected devices.

To log into the Web Manager:

1. Connect your web browser to the console server by typing in the console server's IP address (*e.g.*, `https://10.10.10.10`) in your browser's address field.
2. Press **Enter**. The system displays the console server Web Manager Login form.
3. Type in your username and password.

Features of Regular User Forms

The following figure shows features of the Web Manager when regular users log in.

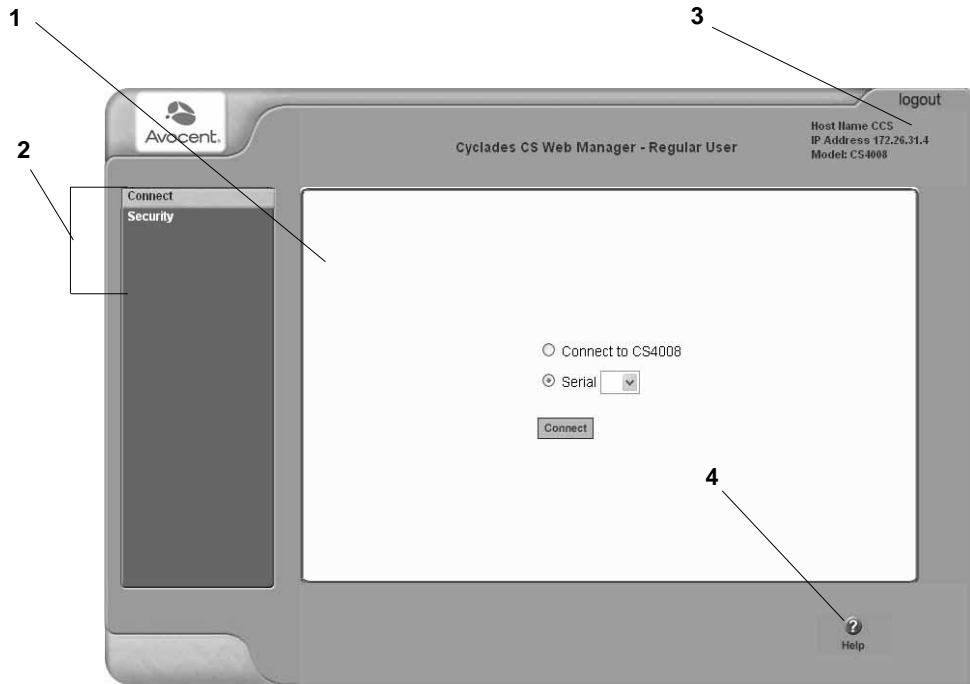


Figure 2.1: Regular User Form

NOTE: The form in the middle changes according to which menu option is selected.

Table 2.1: Common Form Information

Number	Description	Number	Description
1	Web interface main form area	3	logout button and system information
2	Secondary (Left) navigation menu	4	? Help (for online help)

Connect


When you select the *Connect* option, the form displayed will allow you to connect to the console server or to serial ports.

Permission to access a port is granted by the administrator when your user account is created.

Connect to the console server

When you click the *Connect to CS400X* radio button on the Connect form, a Java applet viewer appears running an SSH session on the console server. The IP address of the console server is followed by the session type.

Table 2.2: Java Applet Buttons for Connecting to the Console Server

Button	Purpose
SendBreak	To send a break to the terminal.
Disconnect	To disconnect from the Java applet.
	Select the left icon to reconnect to the server or device; or select the right icon to end the session and disconnect from the Java applet.

Connect to serial ports

The list of serial ports includes the port names or administrator-defined aliases only for ports you have permission to access.

Port access requirements

When you connect to a serial port to access a server or another device, access rights to the specific serial port on the console server is required.

NOTE: If an authentication server is set up in your network, an authentication method and the related parameters should be set up to allow access to the connected devices.

When you select a port from the Serial pull-down list and click the *Connect* button, a Java applet viewer appears. The Connected to message at the top of the screen shows the IP address of the console server followed by the TCP port number.

Connection protocols for serial ports

You can access a server or a device connected to a serial port by using the connection protocol specified for the port.

Table 2.3: Available Serial Port Protocols

Connection Type	Protocol
Console Access Server (CAS)	Telnet, ssh, Telnet&ssh, Raw
Terminal Server (TS)	Telnet, sshv1, sshv2, Local Terminal, Raw Socket
Dial-up	PPP-No Auth., PPP, SLIP, CSLIP

TCP port numbers for serial ports

The TCP port numbers by default start at 7001 for serial port 1 and increment up to the number of serial ports on your console server. The console server administrator may change the default port numbers if needed.

To use Telnet to connect to a device through a serial port:

For this procedure you need the hostname of the console server or its IP address and the TCP port number for the serial port to which the device is connected.

- To use Telnet in a shell, enter the following command:

```
telnet hostname | IP_address TCP_port_number
```

To close a Telnet session:

Enter the Telnet hotkey defined for the client. The default is **Ctrl]** and **q** to quit.

Security

Use the following procedure to set or change your password.

To change your password:

1. Select the *Security* option from the menu panel. The Security form appears.
2. Enter your current password in the Current Password field.
3. Enter the new password in the New Password and the Repeat New Password fields.
4. Click *OK*.
5. Log out and log in using your new password to verify your password change.

Web Manager for Administrators

This chapter is for system administrators who use the Web Manager to configure the Cyclades® CS console server and its users. For information on how to configure the console server using vi or Command Line Interface (CLI), please consult the Cyclades CS console server Command Reference Guide.

The console server's Web Manager for Administrators describes two modes of operation, Wizard and Expert.

Common Features of Administrator Forms

The following figure and table shows and describes the control buttons displayed at the bottom of the form when logged into the Web Manager as administrator.



Figure 3.1: Administrator - Web Manager Buttons

Table 3.1: Description of Administrator Web Manager Buttons

Button name	Use and Results
back	Only appears in Wizard mode. Returns the previous form.
try changes	For testing the changes entered on the current form without saving them by updating the associated configuration files. Changes are preserved if you log in and log out or restart the system. Changes stay in effect unless the cancel changes button is clicked. Changes can be restored at any time until the apply changes button is clicked.
cancel changes	Cancels all unsaved changes by restoring the configuration files from the backup created the last time changes were applied.
apply changes	Applies and saves all unsaved changes. If try changes has not been previously clicked, updates the appropriate configuration files. Overwrites the backed up copy of the configuration files.

Table 3.1: Description of Administrator Web Manager Buttons (Continued)

Button name	Use and Results
reload page	Reloads the page.
Help	Displays the online help.
next	Only appears in Wizard mode. Goes to the next form.
unsaved changes	The unsaved changes button appears on the lower right hand corner of the Web Manager and a graphical LED blinks red whenever the current user has made any changes and has not yet saved the changes.
no unsaved changes	The no unsaved changes button appears and a graphical LED appears in green when no changes have been made that need to be saved.

The following table illustrates the information that displays in the upper right corner of all Web Manager forms.

Table 3.2: Administrator - Logout Button and Other Information in the Upper Right Corner

Form Area Button and Information	Purpose
logout	Click this button to log out.
Host Name: Avocent IP Address: 192.168.48.11 Model: CS4008	Displays the hostname, IP address assigned during initial configuration and the model number of the Cyclades CS console server.

Logging Into the Web Manager

The following procedure describes the login process to the Web Manager and what should be expected the first time you login to the console server.

To log into the Web Manager:

1. To display the Web Manager, enter the IP address of the console server in the address field of your browser.

NOTE: The Cyclades CS console server is usually assigned a static IP address. If DHCP is enabled, you must find out the dynamically-assigned IP address each time you need to run the Web Manager. If necessary, use the default static IP address 192.168.160.10 pre-configured in the console server.

- a. If DHCP is disabled, use the static IP address assigned by the administrator.
 - b. If DHCP is enabled, enter the dynamically-assigned IP address. The Login page displays.
2. Log in as **root** and type in the root password. The default password is **avocent**.

CAUTION: It is important to change the root password as soon as possible to avoid security breaches.

If another administrator is already logged in, a dialog box will prompt you to log off the other administrator before logging in.

3. Select *Yes* or *No* and then click *Apply*.

Overview of Administrative Modes

The console server Web Manager operates in one of two modes, Wizard or Expert.

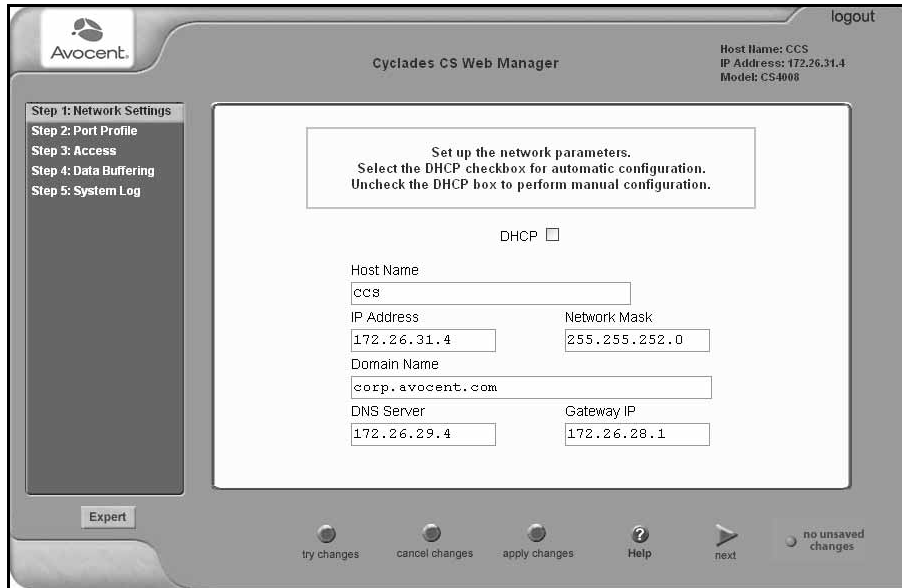
NOTE: The Wizard / Expert button at the lower left of the Web Manager screen indicates the destination mode. If you are in Expert mode, the button reads Wizard, and if you are in Wizard mode, the button reads Expert.

Wizard mode

The Wizard mode is designed to simplify the setup and configuration process by guiding the administrator through six configuration steps.

When you log in to the console server as an administrator or as a user with administrative privileges, the system displays the Expert Mode-Ports-Ports Status form by default.

The following is a typical form of the console server web interface in Wizard Mode. The user entry form varies depending on the selected menu item.



The screenshot displays the Avocent Cyclades CS Web Manager interface in Wizard Mode. The top left corner features the Avocent logo. The top center reads "Cyclades CS Web Manager". The top right corner shows "logout" and system information: "Host Name: CCS", "IP Address: 172.26.31.4", and "Model: CS4008".

A vertical sidebar on the left lists five steps: "Step 1: Network Settings" (highlighted), "Step 2: Port Profile", "Step 3: Access", "Step 4: Data Buffering", and "Step 5: System Log".

The main content area contains a text box with instructions: "Set up the network parameters. Select the DHCP checkbox for automatic configuration. Uncheck the DHCP box to perform manual configuration." Below this is a "DHCP" checkbox, which is currently unchecked.

Below the checkbox are several input fields for network configuration:

- Host Name:
- IP Address: Network Mask:
- Domain Name:
- DNS Server: Gateway IP:

At the bottom of the interface, there is an "Expert" button and a row of navigation controls: "try changes", "cancel changes", "apply changes", "Help", "next", and "no unsaved changes".

Figure 3.2: Example of Web Manager Form in Wizard Mode

Expert mode

Expert is the default mode when logging in to the Cyclades CS console server. The following is a typical console server screen in Expert mode. The main difference in the interface when you switch between the two modes is the addition of a top menu bar in the Expert mode to support more detailed and customized configuration.

In Expert mode the top menu bar contains the primary commands and the left menu panel contains the secondary commands. Based on what you select from the top menu bar, the left menu selections will change accordingly.

The screenshot displays the Avocent Web Manager interface in Expert Mode. The top navigation bar includes the Avocent logo, a menu with 'Applications | Network | Security | Ports | Administration', and a 'logout' button. The right side of the top bar shows host information: 'Host Name: CCS', 'IP Address: 172.26.31.4', and 'Model: CS4008'. On the left, a sidebar menu lists 'Host Settings', 'Syslog', 'SNMP', 'Firewall Configuration', 'Host Tables', and 'Static Routes'. The main content area is titled 'Host Settings' and contains several configuration sections: 'DHCP' (unchecked), 'Host Name' (input field with 'CCS'), 'Console Banner' (input field with 'Cyclades CS'), 'Ethernet Port' section with 'Primary IP' (172.26.31.4), 'Network Mask' (255.255.252.0), 'Secondary IP' (empty), and 'Secondary Network Mask' (empty); 'MTU' (1500); and 'DNS Service' section with 'Primary DNS Server' (172.26.29.4) and 'Secondary DNS Server' (empty). At the bottom, there is a 'Wizard' button and a row of controls: 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and a 'no unsaved changes' indicator.

Figure 3.3: Example of Web Manager Form in Expert Mode

Configuring the Cyclades CS Console Server in Wizard Mode

After Logging In

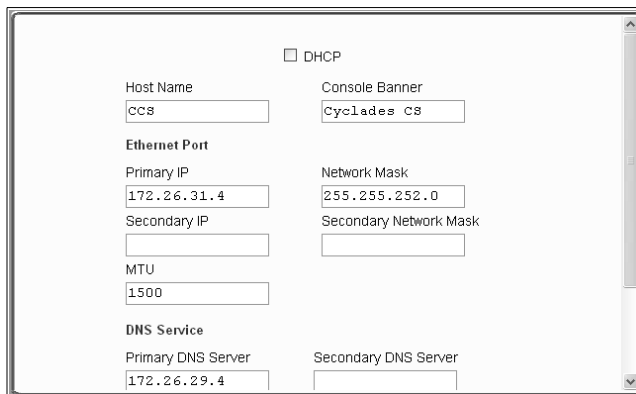
When you first log into the Cyclades CS console server, the Web Manager will open the Ports Status form in Expert mode. To begin using Web Manager Wizard to configure the console server, click the Wizard button at the lower left corner of the window.

Step 1: Network Settings

Selecting *Step 1: Network Settings* displays a form for reconfiguring existing network settings. During initial setup of the console server, the basic network settings required to enable logins were configured through the Web Manager. Skip this step if the displayed settings are correct.

In Expert mode, under Network menu, you can specify additional networking-related information and perform other advanced configuration tasks.

If DHCP is disabled, the form appears as shown in the following figure.



The screenshot shows a web-based configuration form for network settings. At the top, there is a checkbox labeled "DHCP" which is unchecked. Below this, the form is organized into several sections:

- Host Name:** A text input field containing "CCS".
- Console Banner:** A text input field containing "Cyclades CS".
- Ethernet Port:** A section containing:
 - Primary IP:** A text input field containing "172.26.31.4".
 - Network Mask:** A text input field containing "255.255.252.0".
 - Secondary IP:** An empty text input field.
 - Secondary Network Mask:** An empty text input field.
- MTU:** A text input field containing "1500".
- DNS Service:** A section containing:
 - Primary DNS Server:** A text input field containing "172.26.29.4".
 - Secondary DNS Server:** An empty text input field.

Figure 4.1: Wizard - Step 1: Network Settings - DHCP Disabled

If the DHCP is enabled, the following form appears.

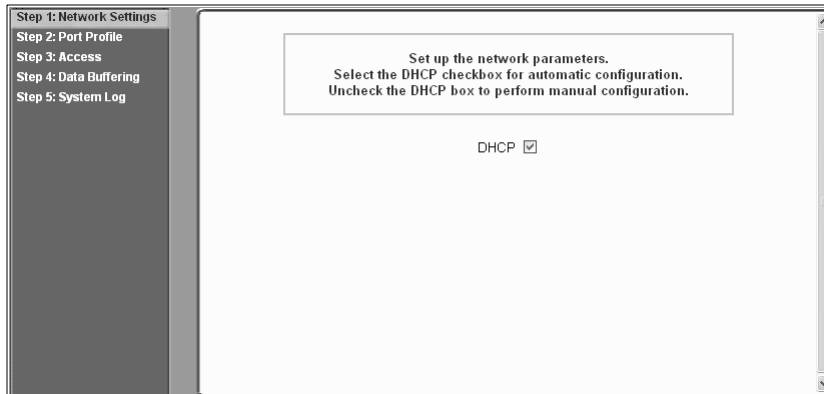


Figure 4.2: Wizard - Step 1: Network Settings - DHCP Enabled

To configure the network settings:

1. Select *Step 1: Network Settings*. The DHCP form is displayed. By default, DHCP is active.

NOTE: If DHCP is enabled, a local DHCP server assigns the console server a dynamic IP address that can change. The administrator chooses whether or not to use DHCP during initial setup.

2. If you are using DHCP, proceed to Step 2: Port Profile, if not, click on the checkbox to deselect DHCP and enter your network settings manually.
3. Enter the required network information.
4. Select *apply changes* to save configuration to Flash.
5. Select the *Next* button or proceed to Step 2: Port Profile.

Step 2: Port Profile

Selecting *Step 2: Port Profile* displays a form for configuring the Console Access Profile (CAS). The protocol used to access the serial ports can be configured in this form.

Figure 4.3: Wizard - Step 2: Port Profile

In Wizard mode, the system assumes that all devices will be connected to the serial ports with the same parameter values. If you need to assign different parameters to the serial ports that each server or device is connected to, use the Expert mode, Ports - Physical Ports to assign individual port parameters.

Table 4.1: Port Profile Setup Options

Parameter	Options	Description
Connection Protocol	Console (Telnet) [Default] Console (ssh) Console (Telnetssh) Console (Raw)	Sets the protocol to be used to connect to devices that are connected to serial ports. Console (ssh) encrypts data and authentication information. Console (Telnetssh) allows users to connect using either protocol. Console (Raw) is for unnegotiated plain socket connections. Use Expert mode if you wish to specify any of several other connection protocols that are listed under Ports-Physical Ports-Modify-General.
Flow Control	None [Default] Hardware Software	Must match the flow control method of the devices connected to all serial ports.
Parity	None [Default] Odd Even	Must match the parity used by the devices connected to all serial ports.

Table 4.1: Port Profile Setup Options (Continued)

Parameter	Options	Description
Baud Rate (Kbps)	9600 [Default] Options range from 2400–921600 Kbps	Must match the baud rates of the devices connected to all serial ports.
Data Size	8 [Default] Options range from 5–8	Must match the number of data bits used by the devices connected to all ports.
Stop Bits	1 [Default] Options are either 1 or 2	Must match the number of stop bits used by the devices connected to all ports.
Authentication Required	Check for enabled. Unchecked for disabled. [Default]	If the Authentication Required is enabled, user authentication is enforced using the local passwd database. To specify other authentication methods such as RADIUS, TACACS+ or LDAP go to Expert mode and select <i>Security-Authentication</i> .

Expert mode provides additional options for custom configuration of serial ports, such as assigning an alias to a serial port, specifying individual parameters to the serial ports (or groups of serial ports) or using any of several other connection protocols.

To set parameters for all serial ports:

This step configures all serial ports with the same values. Use this form if all the devices connected to the serial ports on the console server can run using the same connection protocol with the same speed. Also, make sure the values you specify here are the same as those in effect on the connected devices.

1. Change network parameters as needed.
2. To change whether authentication is required, check the *Authentication Required* checkbox to enable or leave it unchecked to disable.
3. Select *apply changes* to save configuration to Flash.
4. Select the *Next* button or proceed to the next section, Step 3: Access.

Step 3: Access

Selecting *Step 3: Access* displays the form shown in the following figure that enables you to add or delete user accounts and set or change existing passwords.

In addition, administrative privileges can be granted to added users by adding the user accounts to an admin group, enabling them to administer the connected devices without the ability to change the configuration of the console server. By default any user can access any port as long as a valid user ID and password are used.

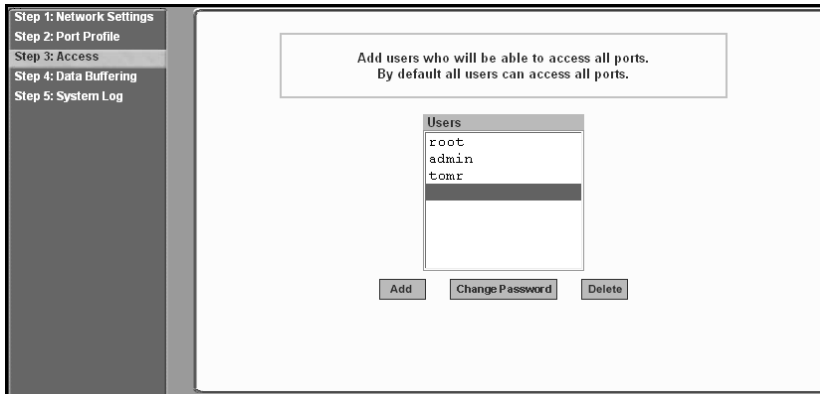


Figure 4.4: Wizard - Step 3: Access

The Access form lists the currently defined users and features *Add*, *Change Password* and *Delete* buttons.

In the Users list by default, there is a root account that cannot be deleted. The root has access privileges to all the Web Manager's functionality as well as access to all the serial ports on the console server.

Click the *Add* button. The following form is displayed.

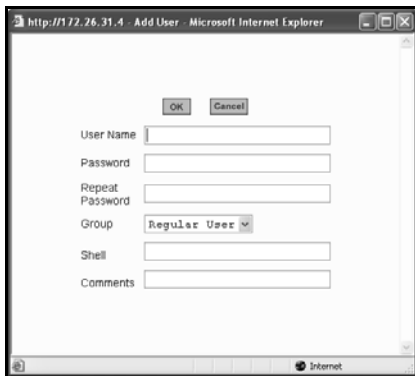


Figure 4.5: Wizard - Step 3: Access Add User Dialog Box

If you click the *Change Password* button, the following dialog box appears.

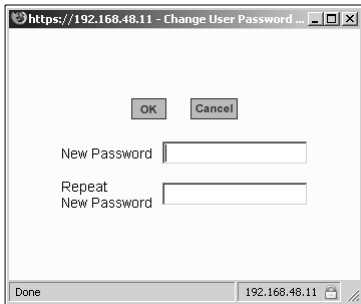


Figure 4.6: Wizard - Step 3: Change Password Dialog Box

To add a user:

1. Select *Step 3: Access*. The Access form displays.
2. Click *Add*. The Add User dialog box appears.
3. Enter the user name and password in the User Name and Password fields and enter the password again in the Repeat Password field.
4. Select from the Group menu options.
 - a. To create a regular user account without administrator privileges, select *Regular User [Default]* from the Group pull-down menu.
 - b. To create an account with administrator privileges, select *Admin* from the Group pull-down menus.

NOTE: To define a new group, switch to Expert mode and select Security - Users and Groups.

5. Enter the default shell in the Shell field (optional).
6. Enter comments to identify the user's role or configuration in the Comments field (optional).
7. Click *OK*.
8. Click the *apply changes* button.

To delete a user:

1. Select *Step 3: Access*. The Access form displays.
2. Select the *user name* to delete.
3. Click *Delete*.
4. Click *apply changes*.

To change a password:

CAUTION: Leaving the default root password unchanged leaves the console server and connected devices open to anyone who knows the default password and the console server's IP address. For security reasons, change the root password from the default **avocent** as soon as possible.

1. Select *Step 3: Access*. The Access form displays.
2. Select the name of the user whose password you wish to change.
3. Click *Change Password*. The Change User Password dialog box displays.
4. Enter the new password in both fields and click *OK*.
5. Click *apply changes*.

Step 4: Data Buffering

Selecting *Step 4: Data Buffering* displays a form to allow logging the console data to a data buffer file either locally in the console server or remotely to an external storage source such as an NFS server or Syslog server. Once *Enable Data Buffering* is selected, the form displays a number of fields. The displayed fields depends on whether selected Destination is Local or Remote.

The values set in this form apply to all serial ports. Data buffering allows a site to save a record of all communication during a serial port connection session. You can set up data buffer files to be stored either in local files on the console server's Flash memory or on the hard disk of an external server, such as an NFS or Syslog server.

The following figure shows the form when *Enable Data Buffering* is checked and the Destination is set to *Local*.

The screenshot shows a wizard interface with a sidebar on the left containing five steps: Step 1: Network Settings, Step 2: Port Profile, Step 3: Access, Step 4: Data Buffering (highlighted), and Step 5: System Log. The main content area has a title box that reads: "Set up data buffering to the output from the consoles in a console log file. The previous port-specific parameters will be discarded." Below this, the "Enable Data Buffering" checkbox is checked. The "Destination" dropdown menu is set to "Local". The "Mode" dropdown menu is set to "Circular", and the "File Size (Bytes)" text input field contains the value "0". The "Record the timestamp in the data buffering file" checkbox is unchecked. The "Show Menu" dropdown menu is set to "show all options".

Figure 4.7: Wizard - Step4: Data Buffering [Local]

The following figure shows the form when *Enable Data Buffering* is checked and the Destination is set to *Remote*.

The screenshot shows the same wizard interface as Figure 4.7, but with the "Destination" dropdown menu set to "Remote". The "NFS File Path" text input field is now visible and empty. The "Enable Data Buffering" checkbox is checked, and the "Record the timestamp in the data buffering file" checkbox is unchecked. The "Show Menu" dropdown menu is set to "show all options".

Figure 4.8: Wizard - Step 4: Data Buffering [Remote]

The difference between Local and Remote data buffering is as follows:

- For local files, set a file size greater than zero. Make sure the file size does not exceed the space available on the console server's Flash memory.
- With the remote server, data is stored in files sequentially. The NFS server must be configured with the mount point shared (exported). In linear mode, data is written into a continuous sequence of files and the file spaces is not reused. The administrator needs to allow enough space for the expected amount of data and take measures such as moving unneeded data files off line, to ensure data does not outgrow the available space.

The following table provides description for each field whether local or remote destination is selected.

Table 4.2: Wizard - Data Buffering Field Names and Definitions

Field name	Definition
Destination	Where the buffer files should be stored. Local, for example, Flash or Remote on a server.
Mode	For Local Destination - Select Linear for sequential files or Circular for non-sequential format. Local data buffering stores data in circular or linear mode. In circular mode, data is written into the specified local data file until the upper limit on the file size is reached; then the data is overwritten starting from the top of the file as additional data comes in. Circular buffering requires the administrator to set up processes to examine the data during the timeframe before the data is overwritten by new data.
File Size (Bytes)	For Local Destination - Sets the value for this field to be greater than zero.
Record the timestamp	If enabled, the system inserts a timestamp in the buffer.
NFS File Path	For Remote Destination - Includes the path where the data buffer file should be stored.
Show Menu	Defines the options you wish to show in the menu of the buffer file.

To configure data buffering:

1. Select *Step 4: Data Buffering*.
2. Click the *Enable Data Buffering* checkbox. The Destination pull-down menu appears.
3. Select a location for the data files from the Destination pull-down menu (either *Local* or *Remote*). Additional pull-down menus and fields appear, depending on which destination is selected.
4. When the destination is local, perform the following steps.
 - a. From the Mode pull-down menu, select *Circular* or *Linear* data buffering.
 - b. Type a file size in bytes into the File Size (Bytes) field. The file size should be greater than zero.
5. When the destination is *Remote*, perform the following steps.
 - a. In the NFS File Path field, enter the pathname for the mount point of the directory where data buffer file is to be stored. For example, if the mount point directory's pathname is `/var/adm/ccslogs`, enter **`/var/adm/ccslogs`** in the field.

NOTE: The NFS server must already be configured with the mount point shared (exported) and the shared directory from the NFS server must be mounted on the console server.

- b. To cause a timestamp to be saved with the data in the data buffer file, enable the Record the timestamp in the data buffering file.

- c. Select an option from the Show Menu pull-down menu. The choices are: *show all options*, *No*, *Show data buffering file only* and *Show* without the erase options.
6. Click *apply changes*.

Step 5: System Log

Selecting *Step 5: System Log* displays a form for identifying one or more syslog servers to receive syslog messages generated by the console server's serial ports.

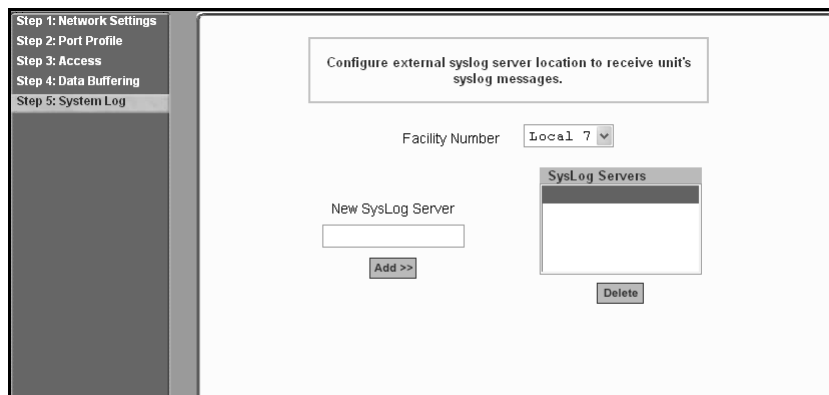


Figure 4.9: Wizard - Step 5: System Log

NOTE: To configure syslog with data buffering features for specific ports, switch to the Expert mode, then select *Ports - Physical Ports - Modify Selected Ports - Data Buffering*.

Before setting up syslogging, make sure a pre-configured syslog server is available on the same network as the console server. From the syslog server administrator, obtain the the IP address of the syslog server and the facility number for messages coming from the syslog server.

To add a syslog server:

1. Select *Step 5: System Log*. The System Log form displays.
2. From the *Facility Number* pull-down menu, select the facility number.
3. In the *New Syslog Server* field, enter the IP address of a syslog server and then click the *Add* button. Repeat this step until all syslog servers are listed.
4. The new server(s) appears in the Syslog Servers list.
5. Click *apply changes*.

To delete a syslog server:

1. From the Syslog Server list, select the syslog server that you wish to delete from the current facility location and then click *Delete*.
2. Click *apply changes*.

Configuring the Console Server in Expert Mode

Most applications require that you set the Web Manager to Expert mode. If you are in Wizard mode and need to perform advanced configuration, click the Expert button at the bottom of the left menu panel to switch to Expert mode. If the Wizard button displays at the lower left of the screen, you are in Expert mode.

Overview of menus and forms

Figure 5.1 shows a typical Expert mode screen. The top menu bar contains the primary commands and the left menu panel contains the secondary commands. Based on what you select from the top menu bar, the left menu panel selections change accordingly and the form area may include tabs for other options as shown.

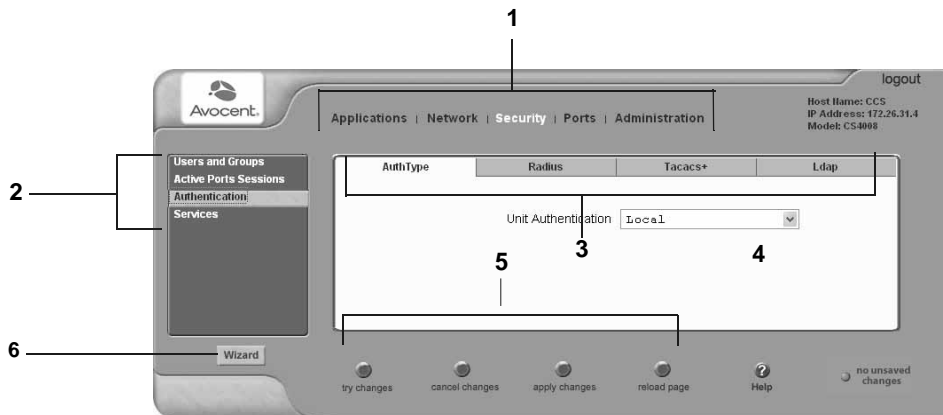


Figure 5.1: Expert Mode Forms Elements

Table 5.1: Expert Mode Forms Elements Information

Number	Description	Number	Description
1	Top menu	4	Main form area
2	Secondary (Left) navigation menu	5	Command buttons
3	Form tabs (not available on all forms)	6	Wizard/Expert selection button

Mapping the expert mode menus and forms

The following tables illustrate mapping of the menus and forms available in Expert mode.

Table 5.2: Expert Mode Menu and Forms, Applications, Network and Security

Applications	Network	Security
<ul style="list-style-type: none"> • <i>Connect</i> • <i>Terminal Profile menu</i> 	<ul style="list-style-type: none"> • <i>Host Settings</i> • <i>Syslog</i> • <i>SNMP</i> • <i>Firewall Configuration</i> • <i>Host Tables</i> • <i>Static Routes</i> 	<ul style="list-style-type: none"> • <i>Users and Groups</i> • <i>Active Ports Sessions</i> • <i>Authentication</i> <ul style="list-style-type: none"> • <i>Auth Type</i> • <i>Radius</i> • <i>Tacacs+</i> • <i>Ldap</i> • <i>Serial port settings</i>

Table 5.3: Expert Mode Menu and Forms, Ports and Administration

Ports	Administration
<ul style="list-style-type: none"> • <i>Physical Ports</i> • <i>Virtual Ports</i> • <i>Ports Status</i> • <i>Ports Statistics</i> 	<ul style="list-style-type: none"> • <i>System Information</i> • <i>Notifications</i> • <i>Time/Date</i> • <i>Boot Configuration</i> • <i>Backup Configuration</i> • <i>Upgrade Firmware</i> • <i>Reboot</i> • <i>Online Help</i>

Applications Menu and Forms

The following provides a description of the left menu panel and links to the detailed information and associated procedure.

Connect

Using the Connect form, you can connect directly to the console server or to devices connected to the serial ports. Always connect to the console server shell using a secure SSH session or connect directly to the serial ports.

Connecting to the console server

Clicking the *Connect to CS400X* radio button and then clicking on the the *Connect* displays a Java applet running an SSH session similar to the following figure.

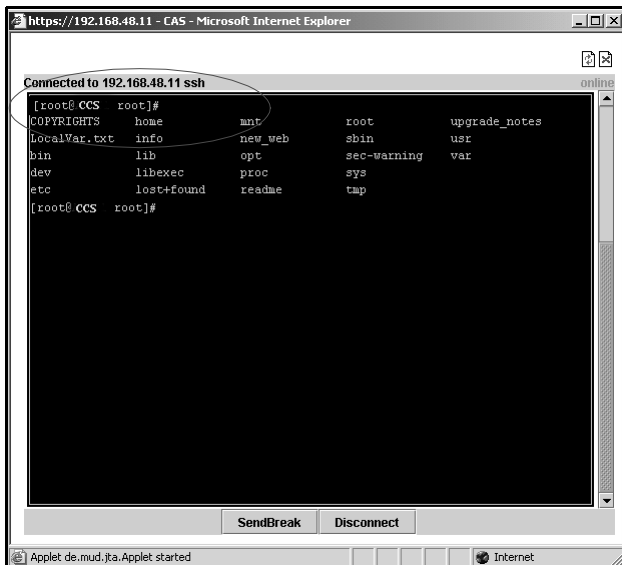


Figure 5.2: Expert - SSH session Java Applet

Connecting to devices connected to the serial ports

The Serial pull-down menu lists all the serial port numbers or the administrator-assigned aliases that a user is authorized to access. Selecting a port number or alias and clicking *Connect* displays a Java applet with a connection protocol for which the serial port is configured.

If authentication is in effect for the port, you need to supply a user name and password to log into the device.

To connect to the console server:

This procedure logs you into the console server as a Regular User in an SSH session.

1. Go to *Applications - Connect* in Expert mode.
2. Click the *Connect to CS400X* radio button.
3. Click the *Connect* button. A Java applet viewer appears.

NOTE: You cannot authenticate unless you enable *allow root access*.

To connect to a device through a serial port:

1. Go to *Applications - Connect* in Expert mode.
2. Click the *Serial* radio button.
3. Select a port number or alias from the *Serial* pull-down menu.
4. Click *Connect*. A Java applet viewer appears. If authentication is specified for the selected port, you are prompted to log in. If not, you are logged in automatically.

Terminal Profile menu

On the Terminal Profile Menu under Applications, you can define a terminal command menu. This menu is used if a terminal is connected to one of the serial ports and is configured as a local terminal. A server terminal configured as a local terminal launches a session directly on the console server with access to the Linux commands on the console server unless you configure a menu here.

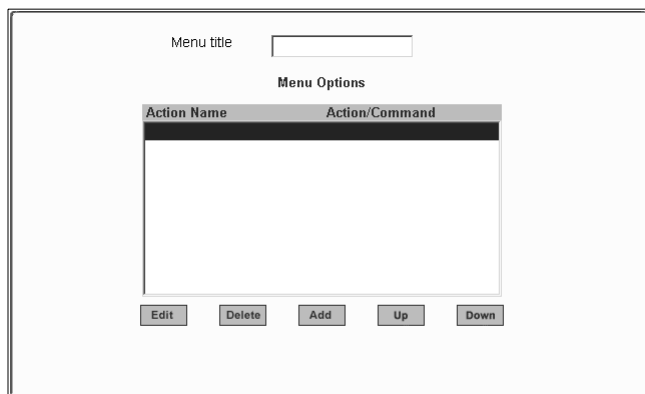


Figure 5.3: Expert - Applications - Empty Terminal Profile Menu

The menu can contain any command recognized by the Linux operating system on the console server. The most common use of this feature is to create multiple menu options for launching SSH sessions on remote hosts.

When you click *Add*, the Add Option dialog box appears.

For example, you can create a menu called SSH to Servers with options that launch SSH connections to several servers, as shown in the following example.

Menu title:

Menu Options

Action Name	Action/Command
SSH-SunRay	ssh 192.168.48.11
SSH-MyLinux	ssh 192.168.48.15
SSH-W2K3	ssh 192.168.48.12

Buttons: Edit, Delete, Add, Up, Down

Figure 5.4: Expert - Terminal Profile Menu Example

The command menu appears when the terminal is powered on.

To create a menu for a local server terminal:

1. Go to *Applications - Terminal Profile Menu*. The Terminal Profile menu displays.
2. Enter a title for the menu in the Menu title field.
3. To edit an existing menu option, select the Action Name from the table and then click *Edit*.
4. To add a new menu option, click *Add*. The Add Option dialog box displays.
 - a. Enter a title for the menu option in the Title field.
 - b. Enter an action or command to be executed when the user clicks the menu option in the Action/Command field.
5. Click *OK*.
6. Click *apply changes*.

Network Menu and Forms

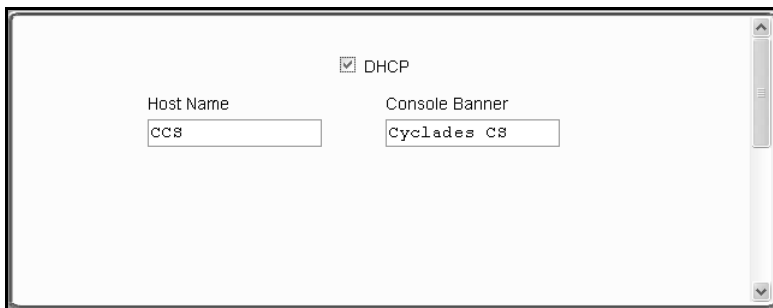
This chapter describes the Network menu and related forms. The following table provides a description of the left menu panel.

Table 6.1: Expert - Network Menu Descriptions

Menu Selection	Use This Menu to:
<i>Host Settings</i> on page 34	Configure the network parameters such as Host Name, IP addresses, DNS services and Gateway.
<i>Syslog</i> on page 36	Configure how the console server will handle its syslog messages. The console server generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit and control purposes.
<i>SNMP</i> on page 37	Configure SNMP with community names, OID and user names. This section and the dialog boxes guide you to configure the required parameters.
<i>Firewall Configuration</i> on page 41	Configure static IP tables and how packets should be filtered.
<i>Host Table</i> on page 49	View information about the local network environment. View table of hosts; create, edit and delete hosts.
<i>Static Routes</i> on page 49	Manually add routes. Static routes are a very quick and effective way to route data from one subnet to different subnets.

Host Settings

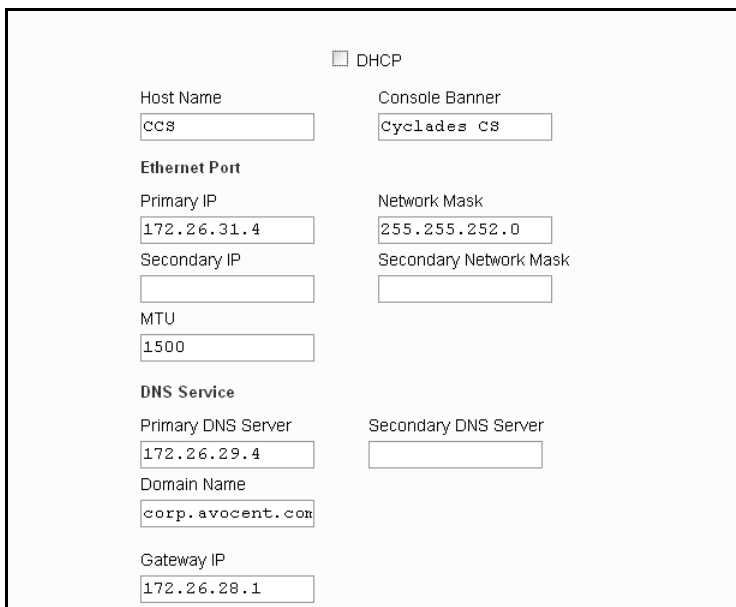
When you select *Network - Host Settings* the following form appears.



The screenshot shows a web form titled "Host Settings" with a checked checkbox for "DHCP". The form contains two input fields: "Host Name" with the value "CCS" and "Console Banner" with the value "Cyclades CS".

Figure 6.1: Expert - Network - Host Settings [DHCP Enabled]

If the DHCP is not enabled, other options appear on the form as shown in the following figure.



The screenshot shows the same "Host Settings" form but with the "DHCP" checkbox unchecked. Additional fields are visible, including "Ethernet Port", "Primary IP" (172.26.31.4), "Network Mask" (255.255.252.0), "Secondary IP", "Secondary Network Mask", "MTU" (1500), "DNS Service" (Primary DNS Server: 172.26.29.4, Secondary DNS Server: empty), "Domain Name" (corp.avocent.com), and "Gateway IP" (172.26.28.1).

Figure 6.2: Expert - Network - Host Settings [DHCP disabled]

To configure host settings [Expert]:

1. Go to *Network - Host Settings*. The Host Settings form appears. By default, the DHCP is enabled. To disable DHCP, click the checkbox to remove the check mark. Additional fields appear.

2. Enter the name assigned to the IP address of the console server in the Host Name field, which is the fully qualified domain name identifying the specific host server on the network.
3. Enter a console banner in the Console Banner field. The console banner appears on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection.
4. Under Ethernet Port, complete or edit the following fields, as necessary.
 - a. Enter the IP address of the console server in the Primary IP field.
 - b. Enter the netmask in the Network Mask field.
 - c. Specify the network mask of the secondary IP in the Secondary Network Mask field.
 - d. Specify the desired maximum transmission unit in the Maximum Transmission Unit field.
5. Under DNS Service specify or change the following information, if desired.
 - a. Enter the address of the domain name server in the Primary DNS Server field.
 - b. If there is a backup DNS server, enter the address of the secondary DNS in the Primary DNS Server field.
 - c. Enter the domain in the Domain Name field.
 - d. Enter the IP address of the gateway in the Gateway IP field.
6. Click *apply changes*.

Syslog

When *Network - Syslog* is selected, the form shown in the following figure appears.

CAS Ports Facility

Syslog Destination

Console Root User Server

New Syslog Server

Syslog Servers	

Filter CAS log messages by level

Emergency Alert Critical Error

Warning Notice Info Debug

Filter Data Buffering log messages by level

Emergency Alert Critical Error

Warning Notice Info Debug

Filter Web log messages by level

Emergency Alert Critical Error

Warning Notice Info Debug

Filter System log messages by level

Emergency Alert Critical Error

Warning Notice Info Debug

Figure 6.3: Expert - Network - Syslog

You can use the Syslog form to configure how the console server handles system logged messages. The Syslog form allows you to perform the following:

- Specify one or more syslog servers to receive syslog messages related to ports.
- Specify rules for filtering messages.

The top field on the form CAS Ports Facility is used to tell the console server where to send syslog messages.

You can specify a facility number for the messages from serial ports.

You can send the syslog messages:

- To the console port for logging the messages even if no user is logged in
- To all sessions where the root user is logged in
- To one or more syslog servers

You can add or remove syslog servers.

The bottom part of the form has filtering rules for specifying which types of messages are forwarded based on the following criteria:

- Severity level: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.
- Category CAS log; Data Buffering log; Web log or System log.

To configure syslogging for serial ports and specify message filtering:

1. Go to *Network - Syslog* in Expert mode. The Syslog form appears.
2. Select a facility number for messages generated by serial ports by selecting the number from the CAS Ports Facility pull-down menu.
3. Select a destination for the syslog messages by clicking the checkbox next to one or all of the options: Console, Root User or Server.
4. Add a syslog server to the Syslog Servers list, by entering its IP address in the New Syslog Server field and clicking the Add-- button.
5. Configure the message filtering as per your requirements.
6. Click *apply changes*.

SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. SNMP works by sending messages called protocol data units (PDUs) to different parts of a network. SNMP-compliant devices (agents), store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The console server SNMP agent supports SNMPv1/v2 and v3. To use SNMP v1 or v2, you need to specify a community name, a source IP address or a range of IP addresses, an object ID (OID) and permission (read-write or read-only). SNMP v3 requires: user name, password, OID and permission.

Selecting *Network - SNMP* displays the form shown in the following figure.

To activate the snmpd services, you should go to the Security > Services section.

System Information Settings

SysContact

SysLocation

Access Control

SNMPv1/SNMPv2 Configuration

Community	Source	OID	Permissi
-----------	--------	-----	----------

SNMPv3 Configuration

User name	Permission	OID
-----------	------------	-----

Figure 6.4: Expert - Network - SNMP

You can use this form to enable notifications about significant events or traps from the console server to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

The following table explains the required parameters to complete the SNMP form and the associated dialog boxes.

Table 6.2: Expert - Fields and Menu Options for SNMP Configuration

Field or Menu Option	Description
SysContact	The email address of the console server's administrator, for example, ccs_admin@avocent.com.
SysLocation	The physical location of the console server.
Community	SNMP v1 and v2 only. A Community defines an access environment. The type of access is classified under Permission: either read only or read write. The most common community is public. NOTE: Take caution in using a public community name as it is commonly known. By default, the public community cannot access SNMP information on the console server.
Source	SNMP v1 and v2 only. Valid entries are default or a subnet address, for example, 193.168.44.0/24 .
OID	Object Identifier. Each managed object has a unique identifier.
Permission	Read Only access to the entire MIB except for SNMP configuration objects. Read/Write access to the entire MIB except for SNMP configuration objects.
User Name and Password	SNMP v3 only.

Clicking the *Add* or *Edit* buttons under SNMPv1/SNMPv2 Configuration displays the New/Mod SNMP v1 v2 Configuration dialog box, as shown in the following figure.

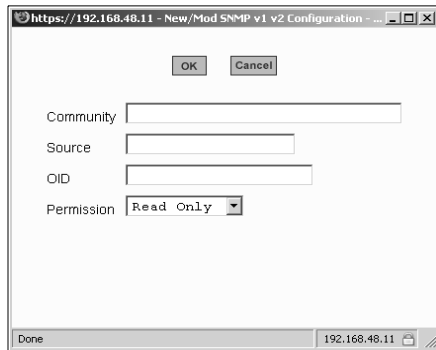


Figure 6.5: Expert - New/Mod SNMP v1 v2 Configuration Dialog Box

Clicking the *Add* or *Edit* buttons under SNMPv3 Configuration displays the New/Mod SNMP v3 Configuration dialog box, as shown in the following figure.

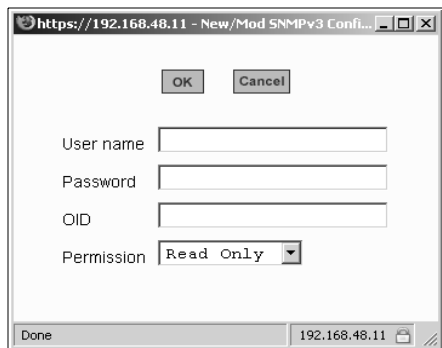


Figure 6.6: Expert - New/Mod SNMP v3 Configuration Dialog Box

To configure SNMP:

1. Go to *Networks - SNMP*. The SNMP form appears.
2. To enable any version of SNMP, perform the following:
 - a. To add an SNMPv1/SNMPv2 entry, press the *Add* button under the SNMPv1/SNMPv2 Configuration table.
 - b. To add an SNMPv3 entry, press the *Add* button at the bottom of the SNMPv3 Configuration table. The New/Modify SNMP Daemon Configuration dialog box appears.
3. For SNMP v1 or v2 configuration, enter or change the following information:
 - a. Enter the community name in the Community field.
 - b. Enter the source IP address or range of IP addresses in the Source field.
4. For SNMP v3 configuration, enter or change the following information:
 - a. Enter the user name in the User name field.
 - b. Enter the password in the Password field.

NOTE: The SNMPv3 password must be fewer than 31 characters.

5. For any version of SNMP, perform the following:
 - a. Enter the unique object identifier for the object in the OID field.
 - b. Choose Read Only or Read/Write from the Permission field.
6. Click *OK*.
7. Click *apply changes*.

NOTE: In addition to SNMP configuration described in this section, you need to make sure SNMP service is enabled and configured for one or more serial ports in order to send SNMP traps.

Firewall Configuration

Firewall configuration, also known as IP filtering, refers to the selective blocking of the passage of IP packets between global and local networks. The filtering is based on rules that describe the characteristics of the packet. For example, the contents of the IP header, the input/output interface or the protocol.

This feature is used mainly in firewall applications to filter the packets that could potentially harm the network system or generate unnecessary traffic in the network.

Selecting *Network - Firewall Configuration* displays the form shown in the following figure.

Name	Policy	Packets	Bytes
INPUT	ACCEPT	51412	4984K
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	6280	2160K

Below the table are four buttons: Edit, Delete, Add, and Edit Rules.

Figure 6.7: Expert - Network - Firewall Configuration

You can use the Firewall Configuration form to enable a firewall on the console server. You can define rules to allow or disallow packets and configure filtering of packets that are sent and received through the console server.

Each entry in the list on the Firewall Configuration form represents a chain with a set of rules.

By default the list has three built-in chains, as shown in the previous figure. The chains accept all INPUT, FORWARD and OUTPUT packets. You can use the *Edit*, *Delete*, *Add* and *Edit Rules* buttons on the form to perform the following to configure packet filtering:

- Edit default chains
- Delete user-added chains
- Add new chains
- Edit rules for chains

Edit button

Selecting one of the default chains and pressing the *Edit* button, the Edit Chain dialog box shown in the following figure appears.



Figure 6.8: Expert - Firewall Configuration Edit Chain Dialog Box

Only the policy can be edited for a default chain. The options are ACCEPT and DROP.

NOTE: User-defined chains cannot be edited. If a user-defined chain is selected for editing, an error message is displayed. If this message appears, click *OK* to continue.

Delete button

If one of the user-defined chains is selected and the *Delete* button is pressed, the chain is deleted.

NOTE: Default chains cannot be deleted. If one of the default chains is selected and the *Delete* button is pressed, an error message is displayed. If this message appears, click *OK* to continue.

Add button

If the *Add* button is pressed, the Add Chain dialog box shown in the following figure appears.

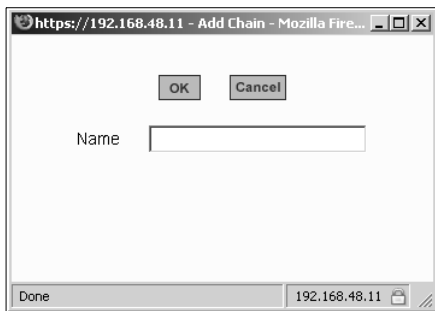


Figure 6.9: Expert - Firewall Configuration Add Chain Dialog Box

Adding a chain only creates a named entry for the chain. Rules must be configured for the chain after it is added to the list of chains.

Edit Rules button

If the *Edit Rules* button is pressed, a form appears with a list of headings like the one shown in the following figure. The example shows the OUTPUT chain selected for editing.

Edit Rules for Chain [OUTPUT]					
Packets	Bytes	Target	Source	Destination	Protocol

Figure 6.10: Firewall Configuration Edit Rules for chain_name Form

The buttons shown in the following figure appear at the bottom of the form.

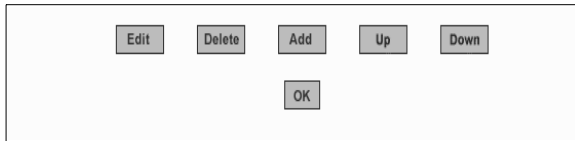


Figure 6.11: Firewall Configuration Edit Rules for chain_name Buttons

- Pressing the *Add* button opens the Add Rule dialog box.
- Selecting a rule and pressing the *Edit* button opens the Edit Rule dialog box.
- Selecting a rule and pressing the *Up* or *Down* button moves the rule up and down the list.

Options on the Add Rule and Edit Rule dialog boxes

The *Add Rule* and *Edit Rule* dialog boxes have the fields and options shown in the following figure.

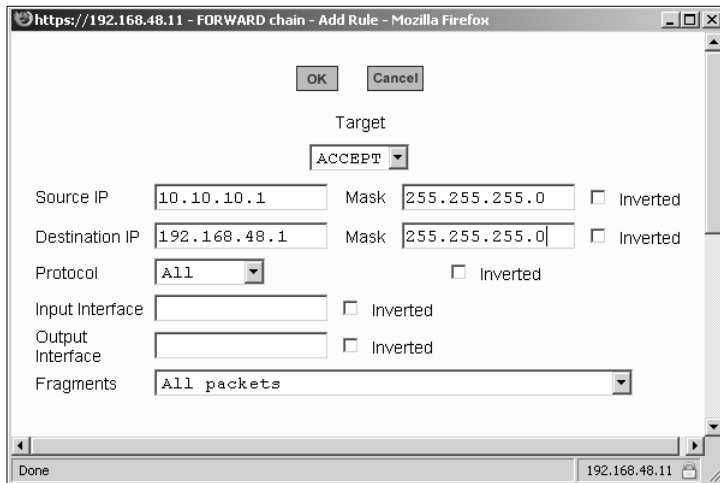


Figure 6.12: Expert - Firewall Configuration Add Rule and Edit Rule Dialog Boxes

Inverted checkboxes

If the *Inverted* checkbox is enabled for the corresponding option, the target action is performed on packets that do not match any of the criteria specified in that line.

For example, if you select *DROP* as the target action from the Target pull-down list, check *Inverted* on the line with the Source IP and do not specify any other criteria in the rule, any packets arriving from any other source IP address than the one specified are dropped.

Target pull-down menu options

The Target pull-down menu shows the action to be performed on an IP packet that matches all the criteria specified in a rule. The kernel can be configured to *ACCEPT*, *DROP*, *RETURN*, *LOG* or *REJECT* the packet by sending a message, translating the source or the destination IP address or sending the packet to another user-defined chain.

Source or destination IP and mask

If you add a value in the Source IP field, incoming packets are filtered for the specified IP address and if you add a value in the Destination IP field, outgoing packets are filtered for the specified IP address. A value in the Mask field means incoming or outgoing packets are filtered for IP addresses from the network in the specified subnet.

Protocol

You can select a protocol for filtering. Fields that appear for each protocol are explained in the following sections.

Numeric protocol fields

If *Numeric* is selected as the protocol when specifying a rule, a text field appears to the right of the menu for the desired number.

TCP protocol fields

If TCP is selected as the protocol when specifying a rule, the additional fields shown in the following figure appear on the bottom of the form.

TCP Options Section

Source Port to Inverted

Destination Port to Inverted

TCP Flags

SYN <input type="text" value="Any"/>	ACK <input type="text" value="Any"/>	FIN <input type="text" value="Any"/>
RST <input type="text" value="Any"/>	URG <input type="text" value="Any"/>	PSH <input type="text" value="Any"/>

Inverted

Figure 6.13: Firewall Configuration TCP Protocol Fields and Menu Options

Table 6.3: Expert - TCP Options Fields

Field/Menu Option	Definition
Source Port - OR - Destination Port -AND- to	A port number for filtering in the Source Port or Destination Port field. A range of IP address can be specified by adding a second port number in the to field. TCP packets are filtered for for the range of specified IP addresses.
TCP Flags	The TCP flags cause packets to be filtered for the specified flag and the selected condition. The flags are: SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), URG (urgent) or PSH (push) and the conditions are either Any, Set or Unset.
Inverted	By checking this box, the TCP options are Inverted. Inverting an item negates the selected rules. Rules will apply to everything except the selected options.

UDP protocol fields

If UDP is selected as a protocol when specifying a rule, the additional fields shown in the following figure appear at the bottom of the form.

UDP Options Section

Source Port to Inverted

Destination Port to Inverted

Figure 6.14: Firewall Configuration Add Rule and Edit Rule UDP Protocol Fields

ICMP protocol fields

If *ICMP* is selected as a protocol, the ICMP Type pull-down menu is displayed in the ICMP Options Section at the bottom of the Firewall Configuration form. Select the ICMP type needed from the list.

Input interface, output interface and fragments

If an interface (such as eth0 or eth1) is entered in the Input Interface field, incoming packets are filtered for the specified interface. If an interface is entered in the Output Interface field, outgoing packets are filtered for the specified interface. The input and output interface fields are shown in the following figure along with the options on the Fragments pull-down menu.

The screenshot shows three fields: 'Input Interface' and 'Output Interface', each with an empty text box and an 'Inverted' checkbox. Below them is a 'Fragments' dropdown menu with three options: 'All packets' (selected), '2nd, 3rd... fragmented packets', and 'Non-fragmented and 1st fragmented packets'.

Figure 6.15: Input/Output Interface Fields and Fragments Menu Options.

Table 6.4: Expert - Firewall Configuration Input/Output Interface and Fragments Fields

Field	Definition
Input Interface	The input interface (ethN) for the packet.
Output Interface	The output interface (ethN) for the packet.
Inverted	Inverting an item negates the selected rules. Rules will apply to everything except the selected options.
Fragments	The types of packets to be filtered: <ul style="list-style-type: none"> • All packets • 2nd, 3rd... fragmented packets • Non-fragmented and 1st fragmented packets

LOG target

If you select *LOG* from the Target field, the fields and menus shown in the following figure appear in the LOG Options Section at the bottom of the form.

The screenshot shows the 'LOG Options Section' with a 'Log Level' dropdown menu set to 'emerg', a 'Log Prefix' text box, and three checkboxes: 'TCP sequence', 'TCP options', and 'IP options', all of which are currently unchecked.

Figure 6.16: Firewall Configuration Add Rule and Edit Rule LOG Target Fields

REJECT target

If *REJECT* is selected from the Target pull-down menu, the following pull-down menu appears.

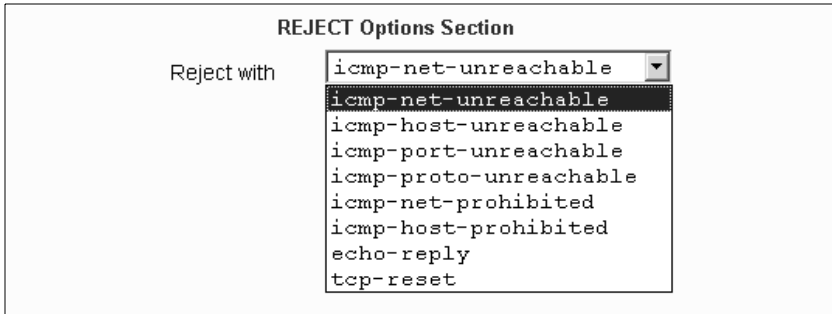


Figure 6.17: Firewall Configuration Add Rule and Edit Rule REJECT Target Menu Options

Any *Reject with* option causes the input packet to be dropped and a reply packet of the specified type to be sent

NOTE: The packets are matched (using tcp flags and appropriate reject type) with the REJECT target.

Firewall configuration procedures

The following sections describe the procedures for defining packet filtering:

To add a chain:

1. Go to *Network - Firewall Configuration*.
2. Click *Add*. The Add Chain dialog box appears.
3. Enter the name of the chain to be added in the Name field.
4. Click *OK*. The name of the new chain appears in the list.

NOTE: Spaces are not allowed in the chain name.

5. Add one or more rules to finish, as described in *To add a rule:* on page 48.

To edit a chain:

Perform this procedure if you wish to change the policy for a default chain.

NOTE: User-defined chains cannot be edited. If you wish to rename a chain you added, delete it and create a new one.

1. Go to *Network - Firewall Configuration*.
2. Select one of the default chains from Chain list and then click the *Edit* button.

NOTE: User-defined chains cannot be edited.

If you select one of the default chains, the Edit Chain dialog box appears.



Figure 6.18: Edit Chain Dialog Box

3. Select the desired policy from the Policy pull-down menu
4. Click *OK*.
5. Click *apply changes*.

To add a rule:

1. Go to *Network - Firewall Configuration*.
2. Select the chain to which you wish to add a rule from Chain list and then click the *Edit Rules* button.
3. Click the *Add Rule* button. The Add Rule dialog box appears.
4. Configure the rule as desired. For definitions of the fields in this form see *Firewall Configuration* on page 41.
5. Click *OK*.
6. Click *apply changes*.

To edit a rule:

1. Go to *Network - Firewall Configuration*
2. Select the chain that you wish to edit from the list and click the *Edit Rules* button. The Edit Rules form appears.
3. Select the rule to be edited from the Rules list and then click the *Edit* button. The Edit Rule dialog box appears.
4. Modify the rule as desired. For definitions of the fields in this form see *Firewall Configuration* on page 41.
5. Click *OK*.
6. Click *apply changes*.

Host Table

The Host Table form enables you to keep a table of host names and IP addresses that compose your local network and provides information on your environment.

Selecting *Network - Host Tables* displays the form shown in the following figure.

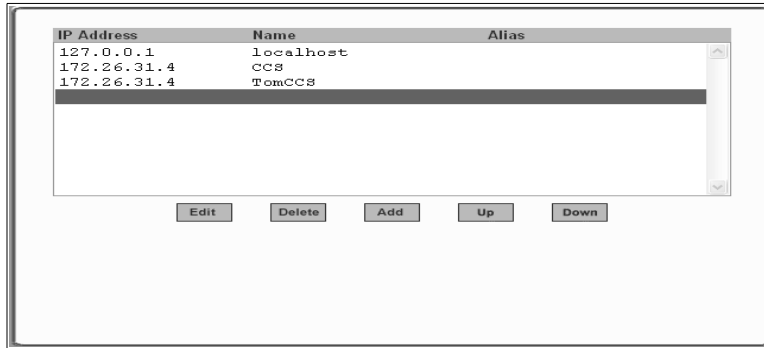


Figure 6.19: Expert - Network - Host Tables

To define the console server's IP address and hostname

1. Go to *Network - Host Tables*. The Host Tables form appears.
2. To edit a host, select the host IP address from the list and click the *Edit* button.
3. To add a host, click the *Add* button. The host table dialog box appears.
4. Enter the new or modified host address in the IP Address field and the host name in the Name field.
5. Click *OK*.
6. To delete a host, select the host you wish to delete and click *Delete*.
7. Click *apply changes*.

Static Routes

The Static Routes form allows you to add routes manually. The Routing Table defines which interface should transmit an IP packet based on destination IP information. Static routes are a quick and effective way to route data from one subnet to another.

Selecting *Network - Static Routes* displays the form shown in the following figure.

Destination IP	Destination Mask	Gateway	Interface	Metric
default		172.26.28.1		

Figure 6.20: Expert - Network - Static Routes

Clicking the *Edit* or *Add* buttons displays the form shown in the following figure.

Apply Cancel

Route Default

Go to Gateway

Metric

Done 192.168.48.11

Figure 6.21: Expert - Static Routes Add and Edit Dialog Boxes - Default Route

The example shows the fields and menus that appear when the Default route type is selected from the Route pull-down menu.

Apply Cancel

Route Network

Network IP

Network Mask

Go to Gateway

Metric

Done 192.168.48.11

Figure 6.22: Expert - Static Routes Add and Edit Dialog Boxes - Network Route

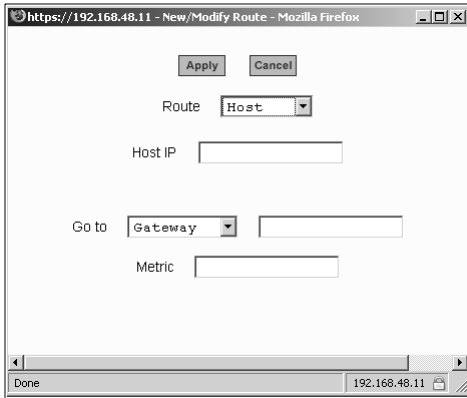


Figure 6.23: Expert - Static Routes Add and Edit Dialog Boxes - Host Route

To configure static routes [Expert]:

1. Go to *Network - Static Routes*. The Static Routes form displays.
 - To edit a static route, select a route from the Static Routes list and then select the *Edit* button.
 - To add a static route, select the *Add* button from the form. The system invokes the *New/Modify Route* dialog box.
2. Choose *Default*, *Network* or *Host* from the Route pull-down menu.
3. If you selected *Network*, perform the following steps.
 - a. Enter the IP address of the destination network in the Network IP field.
 - b. Enter the netmask of the destination network in the Network Mask field.
4. If you selected *Host*, type the IP address of the destination host in the Host IP field.
5. Select *Gateway* or *Interface* from the Go to pull-down menu and enter the address of the gateway or the name of the interface in the adjacent field.
6. Click *apply changes*.

Security Menu and Forms

Users and Groups

The Users and Groups form allows you to perform the following tasks:

- Set up user access to the console server Web Manager
- Assign users to specific groups that share common access rights
- Assign or change passwords
- Create new groups and add to the group list

The two groups to which you can assign a user are:

- Admin - Read/Write Access
- Regular User - Limited Read/Write Access

CAUTION: There is only one root user for the initial setup of the console server by the administrator. The user name is root and the default password is avocent. For security purposes make sure you change this default password as soon as possible.

Selecting *Security - Users and Groups* in Expert mode displays the form shown in the following figure.



Figure 7.1: Expert - Security - Users and Groups Form

You can use the Users and Groups form to perform the following:

- Add or delete users
- Assign or change user passwords
- Add or delete groups
- Add users to a group
- Delete users from a group

Adding a User

If you click the *Add* button on the Security - Users and Groups form under the Users List, the Add User dialog box appears. The following table describes the fields in the Add User dialog box.

Adding a Group

If you click the *Add* button on the Security - Users and Groups form under the Group List, the Add Group dialog box appears. Add a new group by entering a group name and add individual users separated by commas.

To add a user:

1. Go to *Security - Users and Groups*. The Users and Groups form displays.
2. Click *Add*. The Add User dialog box displays.
3. Enter the name of the user to be added in the User Name field.
4. Enter the password associated with the user name in the Password and Repeat Password fields.
5. Assign a group from the Group pull-down menu.

NOTE: To configure a user to be able to perform all administrative functions, select the Admin group.

6. Optional: Select a shell from the Shell pull-down menu. The default shell is `/bin/sh` when the user makes a SSH or Telnet connection.
7. Optional: Enter information, as desired, about the user's role or responsibilities.
8. Click *OK*.
9. Click *apply changes*.

To delete a user or group:

1. Go to *Security - Users and Groups*. The Users and Groups form displays.
2. Select the name of a user or group to delete.
3. Click *Delete*.
4. Click *apply changes*.

To change a user's password:

1. Go to *Security - Users and Groups*. The Users and Groups form displays.
2. Select the name of the user whose password you wish to change.

3. Click *Change Password*. The Change User Password dialog box displays.
4. Enter the new password in the New Password field and enter it again in the Repeat New Password field.
5. Click *OK*.
6. Click *apply changes*.

To add a group:

1. Go to *Security - Users and Groups*. The Users and Groups form displays.
2. Under the list of groups, click *Add*. The Add Group dialog box displays.
3. Enter the name for the new group in the Group Name field.
4. Enter one user name or multiple comma-separated user names in the Users field.
5. Click *OK*.
6. Click *apply changes*.

To modify a group:

1. Go to *Security - Users and Groups*. The Users and Groups form displays.
2. Select the name of a group to modify.
3. Click *Edit*. The Edit Group form displays.
4. Add or delete users from the group as desired.
5. Click *OK*.
6. Click *apply changes*.

Active Ports Sessions

Selecting *Security - Active Ports Sessions* displays the form shown in the following figure.

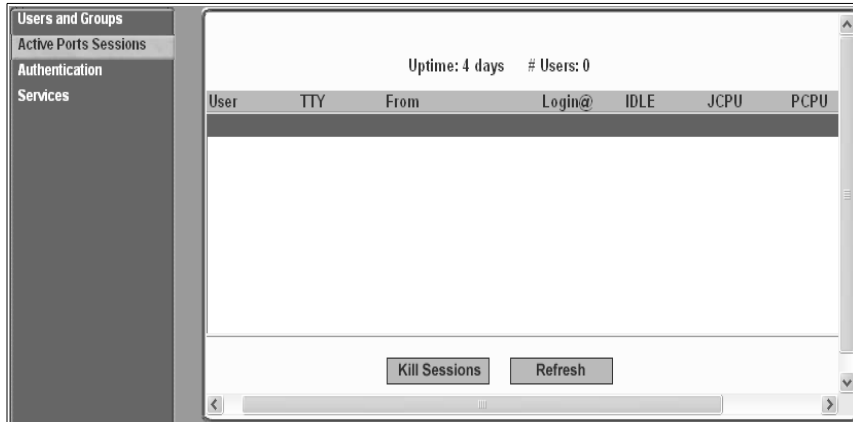


Figure 7.2: Expert - Security - Active Ports Sessions

The Active Ports Sessions form provides status and usage information related to all active serial ports sessions. You can use the form to view who is logged into each port and the processes they are running. Open sessions are displayed with their identification and statistical data, the related data such as CPU usage for a specific client, JCPU processes and PCPU processing time.

The Kill Sessions and Refresh buttons either end or refresh the selected session.

The following table defines the active ports sessions form fields.

Table 7.1: Expert - Active Ports Sessions Information

Field Name	Definition
User	First eight characters of the user name.
TTY	Connection method.
From	Where the network connection is from.
Login	Login time in hours and minutes. If login was not on the same day, the date of login also appears.
Idle	How long since last activity.
JCPU	The amount of CPU time consumed by all active processes including currently running background jobs.
PCPU	The amount of CPU time consumed by the current process.
What	Name of the current process.

To view, kill or refresh active user sessions:

1. Go to *Security - Active Ports Sessions*. The Active Ports Sessions form appears.
2. To refresh the display, click the *Refresh* button.
3. To kill a session, select the desired session and click the *Kill Sessions* button.

Authentication

Selecting *Security - Authentication* displays the form shown in the following figure, which includes AuthType, Radius, Tacacs+ and Ldap tabs.

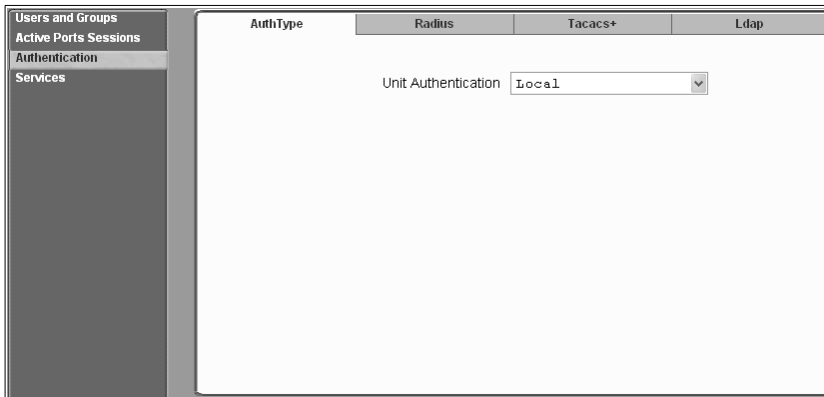


Figure 7.3: Expert - Security - Authentication

You can use the Authentication forms to select a method for authenticating logins to the console server or to identify authentication servers that are configured for logins either to the console server or to the serial ports.

Configuring authentication for console server logins

The default authentication method for the console server is Local. You can either accept the default or select another authentication method from the Unit Authentication pull-down menu on the AuthType form.

Any authentication method selected for the console server is used for authentication of any user attempting to log into the console server through Telnet, SSH or the Web Manager.

To configure the console server login authentication method:

1. Go to *Security - Authentication*. The AuthType form is displayed.
2. To specify an authentication method for login to the console server, select a method from the Unit Authentication pull-down menu.

NOTE: Make sure an authentication server is specified for the selected authentication type.

3. Click *apply changes*.

Configuring authentication servers for logins to the console server and connected devices

If you are configuring any authentication method other than Local, make sure an authentication server is set up for that method.

The following is a summary of the things you need to know about setting up authentication servers.

- The Cyclades CS console server must be on the same subnet as the authentication server.
- Each authentication server must be configured and operational.
- The console server administrator should obtain the necessary information from each authentication server administrator, in order set up and identify those servers on the Cyclades CS console server.

For example, if LDAP authentication were to be used for logins to the console server for logins to serial ports, then the console server needs to have network access to an LDAP authentication server. The administrator needs to perform setup on the console server for both types of authentication servers.

The administrator completes the appropriate form through the Web Manager Expert - Security - Authentication to setup an authentication server for every authentication method to be used by the console server and its ports.

To configure a RADIUS authentication server:

Perform the following procedure to configure a RADIUS authentication server when the console server or any of its ports are configured to use RADIUS authentication method or any of its variations (Local/RADIUS, RADIUS/Local or RADIUS/DownLocal).

1. Go to *Security - Authentication - RADIUS* in Expert mode.
2. Fill in the form according to your local RADIUS server configuration.
3. Click *apply changes*.

To configure a TACACS+ authentication server:

Perform the following procedure to configure a TACACS+ authentication server when the console server or any of its ports are configured to use TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local or TACACS+/DownLocal).

1. Go to *Security - Authentication - TACACS+* in Expert mode. The TACACS+ form displays.
2. Fill in the form according to your local TACACS+ server configuration.
3. To apply Authorization in addition to authentication to the box and ports, select the *Enable Raccess Authorization* checkbox.

By default, Raccess Authorization is disabled and no additional authorization is implemented. When Raccess Authorization is enabled, the authorization level of users trying to access the console server or its ports using TACACS+ authentication is checked. Users with

administrator privileges have administrative access and users with regular user privileges have regular user access.

4. To specify a time-out period in seconds for each authentication attempt, type a number in the Timeout field.

If the authentication server does not respond to the client's login attempt before the specified time period, the login attempt is cancelled. The user may retry depending on the number specified in the Retries field on this form.

5. To specify a number of times the user can request authentication verification from the server before sending an authentication failure message to the user, enter a number in the Retries field.
6. Click *apply changes*.

The LDAP authentication server

Perform the following procedure to configure an LDAP authentication server when the console server or any of its ports are configured to use the LDAP authentication method or any of its variations (LDAP, LDAP/Local or LDAPDownLocal).

You can enter information in the LDAP User Name, LDAP Password and LDAP Login Attribute fields, but an entry is not required.

Work with the LDAP server administrator to ensure that the following types of accounts are set up on the LDAP server and that the administrators of the console server and the connected devices know the passwords assigned to the accounts:

- An account for admin.
- If LDAP authentication is specified for the console server, accounts for all users who need to log into the console server to administer connected devices.
- If LDAP authentication is specified for serial ports, accounts for users who need administrative access to the connected devices.

To configure an LDAP authentication server:

1. Go to *Security - Authentication - LDAP* in Expert mode. The LDAP form displays with LDAP Server and LDAP Base fields filled in from with the current values in the `/etc/ldap.conf` file.

AuthType	Radius	Tacacs+	Ldap
			Ldap Server: 127.0.0.1
			Ldap Base: dc=padl, dc=com
			<input type="checkbox"/> Secure Ldap
			Ldap User Name: []
			Ldap Password: []
			Ldap Login Attribute: []

Figure 7.4: Expert - Security - Authentication - LDAP

2. Supply the IP address of the LDAP server in the LDAP Server field.
3. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the LDAP Base field, change the definition.

The default distinguished name is dc, as in dc=value,dc=value. If the distinguished name on the LDAP server is **o**, then replace dc in the base field with **o**, as in **o=value,o=value**.

4. Replace the default base name with the name of your LDAP domain.

For example, for the LDAP domain name avocent.com, the correct entry is:

dc=avocent,dc=com.

5. Enable Secure LDAP, if required.
6. Enter optional information in LDAP User Name, LDAP Password and LDAP Login Attribute fields.
7. Click *apply changes*. The changes are stored in /etc/ldap.conf on the console server.

Serial port settings

All serial ports on Cyclades CS console servers shipped from the factory are disabled by default. The administrator can enable ports individually or collectively and assign specific users to individual ports.

Port	Disable	Alias	Connection Protocol	Serial Config
1	Yes		Console (Telnet)	9600 8N1
2	Yes		Console (Telnet)	9600 8N1
3	Yes		Console (Telnet)	9600 8N1
4	Yes		Console (Telnet)	9600 8N1
5	Yes		Console (Telnet)	9600 8N1
6	Yes		Console (Telnet)	9600 8N1
7	Yes		Console (Telnet)	9600 8N1
8	Yes		Console (Telnet)	9600 8N1
9	Yes		Console (Telnet)	9600 8N1
10	Yes		Console (Telnet)	9600 8N1

Figure 7.5: Expert - Physical Ports Default Factory Settings

Security certificates

The Cyclades CS console server generates its own self-signed SSL certificate for HTTPS using OpenSSL.

ICertificate for HTTP security

A certificate for HTTP security is created by a Certificate Authority. Certificates are most commonly obtained through generating public and private keys using a public key algorithm like RSA or X.509. The keys can be generated by using a key generator software. The procedure to obtain a Signed Digital Certificate is documented in the *Cyclades CS Console Server Command Reference Guide*.

User configured digital certificate

You can generate a self-signed digital certificate. It is highly recommended that you use the openssl tool to generate a self-signed certificate and replace the console server generated certificate. The procedure to configure a self-signed digital certificate is documented in the *Cyclades CS Console Server Command Reference Guide*.

X.509 certificate on ssh

The OpenSSH software included with the console server has support for X.509 certificates. The administrator must activate and configure the SSH to use X.509. In order to implement authentication of SSH sessions through exchange of X.509 certificates please refer to the configuration procedures described in the *Cyclades CS Console Server Command Reference Guide*.

Ports Menu and Forms

Physical Ports

When Physical Ports is selected under Ports - Physical Ports in Expert mode, the following form appears.

Port	Disable	Alias	Connection Protocol	Serial Config
1		Console01	Console (Telnet)	9600 8N1
2		IPDU_01	Power Management	9600 8N1
3		WS_01	Console (SSH)	9600 8N1
4		WS_02	Console (SSH)	9600 8N1
5		WS_03	Console (SSH)	9600 8N1
6	Yes	WS_Stby	Console (SSH)	9600 8N1
7		IPDU_02	Power Management	9600 8N1
8		DE_F02	Console (TelnetSSH)	9600 8N1
9		DE_F03	Console (TelnetSSH)	9600 8N1
10		DE_F04	Console (TelnetSSH)	9600 8N1

Figure 8.1: Ports - Physical Ports

Using this form, you can enable or disable ports and configure parameters for individual or a group of serial ports.

You can select contiguous serial ports on the form by using the **Shift** key or non-contiguous ports by using the **Ctrl** key on your keyboard. You can select *Enable Selected Ports* or *Disable Selected Ports* by pressing the corresponding button.

You can select the *Modify All Ports* button to specify the same parameters for all the serial ports or you can select the *Modify Selected Ports* button and set values for an individual or a group of ports.

To select one or more serial ports:

1. Go to *Ports - Physical Ports* in Expert mode The Physical Ports form appears.
2. To select a port or ports, perform one of the following steps.
 - a. To select a single port, click the port.

- b. To select multiple ports in a range, click the first port in the list and then hold down the **Shift** key while selecting the last port or ports in the range.
 - c. To select multiple ports that are not in a range, click the first desired port in the list and then hold down the **Ctrl** key while selecting another port or ports.
3. Go to the desired procedure from the following list.

Table 8.1: List of Procedures for Serial Port Configuration

To enable or disable serial ports: on page 64

To configure a serial port connection protocol for a console connection: on page 67

To configure user access to serial ports: on page 70

To configure data buffering for serial ports: on page 72

To configure multiple sessions and port sniffing for one or more serial ports: on page 74

To configure TCP port number, STTY options, break interval and the login banner for a serial port connected to a console: on page 75

To enable or disable serial ports:

1. Go to *Ports - Physical Ports* and select a port or ports to modify.
 2. To enable selected ports, click the *Enable Selected Ports* button.
 3. To disable selected ports, click the *Disable Selected Ports* button.
-

NOTE: By default, all Serial Ports are disabled from the factory. The Administrator can activate and assign specific users to individual physical ports.

4. Click *apply changes*.

General form

Under *Ports - Physical Ports*, if you select one or more ports from the ports list and click the *Modify* button, the General form appears as shown in the following form.

The screenshot shows a configuration window with the following settings:

- Connection Protocol: Console (Telnet)
- Baud Rate (Kbps): 9600
- Flow Control: None
- Parity: None
- DCD State: Disregard
- Data: 8
- Stop Bits: 1

Selected ports #: 1,2 Done

Figure 8.2: Ports - Physical Ports - General Form

The General form allows you to define general port settings and select the connection type to a serial port (SSH, Telnet or both).

The number of the selected port or ports displays next to the Done button at the bottom of the form in the format: Selected ports #:N, where N stands for the port number.

Connection profiles

The following sections describe the available connection protocols for each connection to the serial ports.

Console Access Server (CAS) profile connection protocols

When a serial port is connected to the console port on a device, a CAS profile must be defined for the serial port.

Selecting the appropriate connection protocol on the Ports - Physical Ports - General is part of defining the CAS profile.

The CAS connection protocols apply in the following cases:

- When a user accesses the serial port through the Web Manager, the session automatically uses the specified protocol to connect to the console of the connected device.
- When a user logs in remotely to the serial port, access is allowed only for the selected protocol. If another protocol is used then access is denied. For example, if you specify the Console (SSH) protocol, the user can use SSH but cannot use Telnet to access the serial port.

Table 8.2: Connections Protocols When Serial Port is Connected to Device Console Port

Protocol Name	Result
Console (Telnet)	Authorized users can use Telnet to connect to the console of the connected device.
Console (SSH)	Authorized users can use SSH to connect to the console of the connected device.
Console (TelnetSSH)	Authorized users can use Telnet and/or SSH to connect to the console of the connected device simultaneously. When the multiple sessions feature is configured, simultaneous Telnet and/or SSH sessions are allowed through the serial port.
Console (Raw)	Authorized users can make a Raw Socket connection to the console of the connected device.

Terminal Server (TS) profile connection protocols

When a server terminal is connected to the console port on a device, a TS profile must be defined for the serial port.

Selecting the appropriate connection protocol on the Ports - Physical Ports - General form is part of defining the TS profile.

When configuring serial ports to support server terminals, you can:

- Dedicate a terminal to access a single remote server by means of either Telnet, SSHv1, SSHv2 or Raw Socket connections.
- Enable a terminal to access multiple servers through the console server.

The TS profile must specify the TCP port number, the terminal type and the IP address for the remote host on the Ports - Physical Ports - Other form.

Table 8.3: Available Connection Protocols When Terminal is Connected to a Serial Port

Protocol Name	Result
Telnet	Dedicates a server terminal connected to a serial port to access a server using the Telnet protocol. When the attached terminal is powered on, the console server opens a Telnet session on the server. The server's IP address should be specified on the Other form, Ports - Physical Ports - Other.
SSHv1	Dedicates a server terminal connected to the selected serial port to access a server using the SSHv1 protocol. When the attached terminal is powered on, the console server opens an SSHv1 session on the server. The server's IP address should be specified on the Other form, Ports - Physical Ports - Other.

Table 8.3: Available Connection Protocols When Terminal is Connected to a Serial Port (Continued)

Protocol Name	Result
SSHv2	Dedicates a server terminal connected to the selected serial port to access a server using the SSHv2 protocol. When the attached terminal is powered on, the console server opens a SSHv2 session on the server. The server's IP address should be specified on the Other form, Ports - Physical Ports - Other.
Local Terminal	Dedicates a server terminal connected to the selected serial port for connecting to the console server. When the attached terminal is powered on, the console server opens a Telnet session on itself. The user then can use any of the console server's Linux commands. You can also create a terminal profile menu, Applications - Terminal Profile Menu that enables the user to quickly launch sessions on any number of remote hosts.
Raw Socket	Dedicates a server terminal connected to the selected serial port to access a specific remote host using the Raw Socket protocol. When the attached terminal is powered on, the console server opens a Raw Socket session on the host using an IP address and TCP port number specified on the Other form, Ports - Physical Ports - Other.

Modem connection protocols

Table 8.4: Connection Protocols for Modems

Protocol Name	Result
PPP-No Auth	Starts a PPP session without interactive authentication required. Assumes the specified console server serial port is connected to an external modem.
PPP	Starts a PPP session with authentication required. Assumes the specified console server serial port is connected to an external modem.
SLIP	Starts a SLIP session. Assumes the specified console server serial port is connected to an external modem.
CSLIP	Starts a CSLIP session. Assumes the specified console server serial port is connected to an external modem.

To configure a serial port connection protocol for a console connection:

This procedure assumes that the selected serial port is physically connected to a console port on a device.

1. Go to *Ports - Physical Ports* in Expert mode, select a port or ports to modify, click the appropriate Modify Ports button. The General form appears.
2. Click the *General* tab. The General form appears with the number(s) of the selected port(s) next to the Done button at the bottom of the form. All active tabs are yellow.
3. To change the connection protocol, select one of the options from the Connection Protocol pull-down menu: Console (Telnet), Console (SSH), Console (Telnet & SSH) or Console (Raw). The default is Console (Telnet).

If you wish to change any of the other current settings, see *To configure serial port settings to match the connected devices:* on page 69.

To further configure the serial port's connection protocol:

- For user access and authentication methods see *Access* on page 70.
- For TCP Port number and other port configuration options see *Other* on page 74.

To configure a serial port connection protocol for a terminal server:

This procedure assumes that the selected serial port is physically connected to a terminal. For more information on Terminal Server connection protocols see *Terminal Server (TS) profile connection protocols* on page 66.

1. Go to *Ports - Physical Ports* in Expert mode, select a port or ports to modify, click the appropriate *Modify Ports* button. The General form appears.
2. Click the *General* tab. The General form appears with the number(s) of the selected port(s) next to the Done button at the bottom of the form and the active tabs in yellow.
3. To change the connection protocol, select a Terminal Server connection from the Connection Protocol pull-down menu, Telnet, SSHv1, SSHv2, Local Terminal or Raw Socket.
4. To configure a terminal to automatically connect to the console server, perform the following steps:
 - a. Select *Local Terminal* from the Connection Protocol pull-down menu.
 - b. Define a terminal profile menu. The Terminal Profile Menu form is found under the Expert - Applications - Terminal Profile Menu.
5. To configure a terminal to automatically connect to a server, perform the following steps:
 - a. Select *Telnet, SSHv1, SSHv2* or *Raw Socket* from the Connection Protocol pull-down menu.
 - b. Specify authorized users/groups and the authentication method in the Access form.
 - c. Specify the TCP Port number, the IP address of the remote host and the terminal type using the Other form. The Other form is located at Ports - Physical Ports - Modify Selected Ports - Other.
6. If you are finished, click *Done*.
7. Click *apply changes*.

To configure a serial port connection protocol for an external modem:

This procedure assumes that the selected serial port is physically connected to an external modem.

1. Go to *Ports - Physical Ports* in Expert mode, select a port or ports to modify, click the appropriate *Modify Ports* button. The General form appears.
2. Click the *General* tab. The General form appears with the number(s) of the selected port(s) next to the Done button at the bottom of the form and the active tabs are in yellow.

3. To change the connection protocol, select one of the options from the Connection Protocol pull-down menu: PPP-No Auth., PPP, SLIP or CSLIP.
4. If you wish to change any of the other current settings, see *To configure serial port settings to match the connected devices:*, following.
5. To further configure the serial port's connection protocol:
 - For user access and authentication methods, see *Access* on page 70.
 - To specify the TCP Port number and configure modem initialization and PPP options see information on the tab labeled *Other* on page 74.
6. If you are finished, click *Done*.
7. Click *apply changes*.

To associate an alias to a serial port:

An alias can be associated to a port when it is individually selected for modification. To associate an alias to a port perform the following steps.

1. Go to *Ports - Physical Ports* in Expert mode, select a port to modify and click the Modify Ports button.
2. Enter the desired string in the Alias field.
3. Click *Done*.
4. Click *apply changes*.

NOTE: The Alias field cannot be set if you select the Modify All Ports.

To configure serial port settings to match the connected devices:

The settings for a serial port must match the connection settings on the connected device.

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify. The General form appears.
2. Select from the following pull-down menus:

• Baud Rate: Range 2400 to 921600 Kbps	Default: 9600.
• Flow Control: None/Hardware/Software	Default: None
• Parity: None/Odd/Even	Default: None
• Data Size: Range 5 - 8	Default: 8
• Stop Bits: 1 or 2	Default: 1
3. To change whether the DCD (Data Carrier Detect) State is disregarded or not, select either Disregard or Regard.
4. Click *Done*.
5. Click *apply changes*.

Access

Under *Ports - Physical Ports* in Expert Mode, select one or more serial ports and click the Modify Port(s), select the *Access* form from the tabbed menu. The Access form appears.

Table 8.5: Access Form Menu and Fields

Field	Description
Authorized Users/Groups	Restrict or deny access to a serial port by specifying one or more users or groups. You can deny access to one or more users or groups by entering an exclamation point (!) before the user or group name. For example, to explicitly deny access to a user called noadmin and enable access only to a single user called johnd you would enter the following: Inoadmin,johnd . Successive names are separated by a comma.
Type	Select an authentication type for the serial port from the pull-down list. The default is no authentication (Type=None).

To configure user access to serial ports:

Use this procedure if you wish to specify a list of authorized users or groups.

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify.
2. Click the *Access* tab. The Access form appears.
3. To restrict access to one or more users or to a group of users, enter previously defined user or group names in the Authorized Users/Groups field, with names separated by commas.
4. To deny access to one or more users or groups, preface the user or group names with an exclamation point (!).
5. Click *Done*.
6. Click *apply changes*.

Authentication methods and fallback mechanism

The following table provides a brief description of the authentication methods. When an authentication method is configured to be performed by an authentication server such as LDAP, RADIUS or TACACS+, the user can get access denial if either the authentication server is down or it does not authenticate. An authentication fallback mechanism can be defined in case the first authentication level fails.

Table 8.6: Expert - Authentication Methods and Fallback Mechanisms

Authentication Type	Definition
None	No authentication.
LDAP	Authentication is performed against an LDAP database using an LDAP server.
LDAP/Local	LDAP authentication is tried first, switching to Local if unsuccessful.

Table 8.6: Expert - Authentication Methods and Fallback Mechanisms (Continued)

Authentication Type	Definition
LDAPDownLocal	Local authentication is performed only when the LDAP server is down.
Local	Authentication is performed locally. For example, using the <code>/etc/passwd</code> file.
Local/Radius	Authentication is performed locally first, switching to Radius if unsuccessful.
Local/TACACS+	Authentication is performed locally first, switching to TACACS+ if unsuccessful.
Radius	Authentication is performed using a Radius authentication server.
Radius/Local	Radius authentication is tried first, switching to Local if unsuccessful.
RadiusDownLocal	Local authentication is performed only when the Radius server is down.
TACACS+	Authentication is performed using a TACACS+ authentication server.
TACACS+/Local	TACACS+ authentication is tried first, switching to Local if unsuccessful.
TACACS+DownLocal	Local authentication is tried only when the TACACS+ server is down.

To configure a serial port login authentication method:

This procedure configures an authentication method that applies to logins to devices connected to serial ports. You can select different methods for individual ports or for groups of ports.

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify.
2. Click the *Access* tab.
3. To select an authentication method, select one of the options in the *Type* menu.
4. Click *Done*.
5. Click *apply changes*. The changes are stored in the `/etc/portSlave/pSlave.conf` file on the console server.
6. Make sure that an authentication server is specified for the selected authentication type.

Data Buffering

Under *Ports - Physical Ports* in Expert Mode, after you select one or more serial ports and click the *Modify Port(s)*, you can select the *Data Buffering* form from the tabbed menu. The Data Buffering form appears.

There are different fields on this form depending on whether one or both options are enabled. The form displays *Enable Data Buffering* and *Buffer to Syslog* options.

If *Enable Data Buffering* is active, the form displays different fields depending on whether *Local* or *Remote* are selected from the *Destination* menu.

Figure 8.3: Ports - Physical Ports - Data Buffering Enabled

If Buffer to Syslog is checked, data buffer files are sent to the syslog server.

NOTE: Go to *Wizard - Step 5: System Log or Expert - Network - Syslog* to set up a syslog server.'

To configure data buffering for serial ports:

Perform this procedure if you wish to configure data buffering. Obtain the facility number for the console server from the system administrator of the syslog server. Options range from Local0 to Local7.

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify.
2. Select the Data Buffering tab. The Data Buffering form displays.
3. Select Enable Data Buffering.
4. From the Destination pull-down menu, choose Local or Remote to specify whether the data buffer files are stored locally or remotely on a file server.
5. If you chose Local from the Destination pull-down menu, perform the following:
 - a. Choose Circular or Linear from the Mode pull-down menu. Will be either circular or linear. In circular mode, data is written into the specified local data file until the upper limit on the file size is reached; then the data is overwritten starting from the top of the file as additional data comes in.
 - b. Enter a size larger than 0 in the File Size (Bytes) field.
6. If you chose Remote from the Destination pull-down menu, enter the NFS mount point for the directory where data buffer file is to be stored in the NFS File Path field.

NOTE: If you are configuring data buffer files to be stored remotely, make sure that a system administrator has already configured an NFS server and shared the mount point.

7. Click the checkbox next to Record the timestamp in the data buffering file to specify whether to include a timestamp with the data.

8. From the Show Menu pull-down menu, choose Show all options, No, Show data buffering file only or Show without the erase options.
9. If you checked Buffer to Syslog, enter the IP address of the syslog server in the Syslog Server field.
10. Choose an option from the Facility Number pull-down menu.
11. Enter the maximum size of the buffer in the Syslog Buffer Size field.
12. Click the radio button next to one of the following options:
 - a. Buffer Syslog at all times
 - b. Buffer only when nobody is connected to the port
13. Click *Done*.
14. Click *apply changes*.

To configure alarm notifications to be sent based on the type of buffered data, use the Notifications form, Expert - Administration - Notifications.

Multi User

Under *Ports - Physical Ports* in Expert Mode, after you select one or more serial ports and click the Modify Port(s), you can select the Multi User form from the tabbed menu. The Multi User form appears.

The Multi User form enables you to open more than one session from the same serial port. Multiple users can connect simultaneously to a serial port. To connect to a port or start a shared session, the user must have permission to access the port. If you allow multiple sessions through the Allow Multiple Sessions pull-down menu, the Privilege Users field should be populated with the user names who have access rights.

Table 8.7: Available Options from the Allow Multiple Sessions Pull-down

Menu Option	Description
No	Do not allow multiple sessions. Only two users can connect to the same port simultaneously. One shared session and one normal session are allowed.
Yes (show menu)	More than two simultaneous users can connect to the same serial port. A sniffer menu is presented to the user and they can choose to: <ul style="list-style-type: none"> • Open a sniff session. • Open a read/write session. • Cancel a connection. • Send a message to other users connected to the same serial port.
Read/Write (do not show menu)	Read/write sessions are opened and the sniffer menu won't be presented.
ReadOnly (do not show menu)	Read only sessions are opened and the sniffer menu won't be presented.

To configure multiple sessions and port sniffing for one or more serial ports:

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify.
2. Click the *Multi User* tab.
3. To allow or to prevent multiple sessions, select an option from the Allow Multiple Sessions pull-down menu. The options are: No, Yes (show menu), Read/Write (do not show menu), ReadOnly.
4. To configure the type of data that displays on the monitor in a port-sharing session, select an option from the Sniff Mode pull-down menu.
5. If you have allowed multiple sessions, complete the following fields.
 - a. Add user names to the Privilege Users field.
 - b. Enter a hotkey in the Menu Hotkey field to display the sniffer menu on the monitor. The default shown is **^z**. The caret stands for the **Ctrl** key.
 - c. Enable the Notify Users field, if desired.
6. Click *Done*.
7. Click *apply changes*.

Other

Under *Ports - Physical Ports* in Expert Mode, after you select one or more serial ports and click *Modify Port(s)*, you can select the *Other* form from the tabbed menu to configure other options. The *Other* form appears.

You can use this form to configure other settings. The options on this form may be less common settings. The following table describes the available fields in the *Other* form.

Table 8.8: Other Form Fields

Field Name	Definition
TCP Port	The TCP Port number for a serial port. The TCP port numbers by default start from 7001 and increment by +1 up to the number of serial ports that the console server unit has. For example, a console server unit with 8 serial ports have TCP port numbers 7001 through 7008.
Port IP Alias	A name (alias) for the IP of the selected port. A port IP alias field appears when a console (CAS) profile is selected from the Connection Protocol pull-down menu on the General form.
TCP Keep-alive Interval	Specifies the time interval between the periodic polling by the system to check client processes and connectivity.
Idle Timeout	The maximum time (in seconds) that a session can be idle before the user is logged off.
STTY Options	Set terminal options.

Table 8.8: Other Form Fields (Continued)

Field Name	Definition
Break Interval	Usually 250 to 500 milliseconds. It's a logical zero on the TXD or RXD lines to reset the communications line.
Break Sequence	Usually a character sequence ~break (Ctrl-b) .
Login Banner	Enter the text you wish to appear as a login banner when logging into a terminal.
Host to Connect	This field should be populated with the IP address of the device to which you are connecting. The field is displayed when a terminal server (TS) profile is selected from the Connection Protocol pull-down menu on the General form.
Terminal Type	This field should be populated with the terminal type when connecting to a host system. The field is displayed when a terminal server (TS) profile is selected from the Connection Protocol pull-down menu on the General form.

To configure TCP port number, STTY options, break interval and the login banner for a serial port connected to a console:

1. Go to *Ports - Physical Ports* in Expert mode and select a port or ports to modify.
2. Select the *Other* tab.
3. To change the port number for the serial port, enter another number in the TCP Port field.
4. To assign a name to the port's IP address, enter an alias in the Port IP Alias field (console connection protocol only).
5. To change the keep-alive interval, enter another number in the TCP Keep-alive Interval field.
6. To change the idle timeout interval, enter another value in the Idle Timeout field.
7. Specify stty options, if desired, in the STTY Options field.
8. To change the break interval, enter a new number in the Break Interval field.
9. To change the break sequence, enter a new sequence in the Break Sequence field.
10. To change the content of the login banner, enter new content in the Login Banner field.
11. Click *Done*.
12. Click *apply changes*.

To configure terminal server connection options:

Perform this procedure if you have connected a server terminal to a serial port.

1. Select the port and choose a TS profile from the Connection Protocol pull-down menu on General form.
2. Click the *Other* tab. The Other form displays.

3. To change the port number used to access the serial port, enter another number in the TCP Port field.
4. To change the keep-alive interval, enter another number in the TCP Keep-alive Interval field.
5. To change the idle timeout interval, enter another value in the Idle Timeout field.
6. Specify stty options, if desired, in the STTY Options field.
7. To change the break interval, enter a new number in the Break Interval field.
8. To change the break sequence, enter a new sequence in the Break Sequence field.
9. To change the content of the login banner, enter new text in the Login Banner field.
10. For a dedicated terminal, enter the IP address of the desired host in the Host to Connect field.
11. Enter the type of terminal in the Terminal Type field.
12. Click *Done*.
13. Click *apply changes*.

Virtual Ports

When *Virtual Ports* is selected, the following form appears.

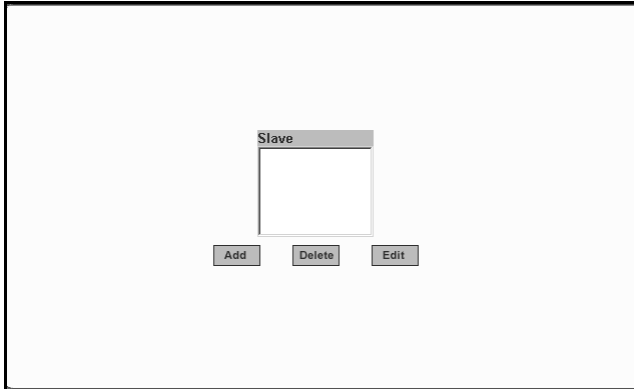


Figure 8.4: Ports - Virtual Ports

The virtual ports form allows you to perform clustering of the console server units. The console server clustering is designed to allow a large number of serial ports (up to 1024) to be configured and virtually accessed through one IP address.

NOTE: Clustering only works for ports that are configured as CAS profile.

You can use one console server as the master to control other console servers as slaves. The ports on the slave unit(s) appear as if they are part of the master.

This section shows you how to define and configure the slaves. When you click the *Add* or *Edit* button on the Ports - Virtual Ports form, the following dialog box appears.

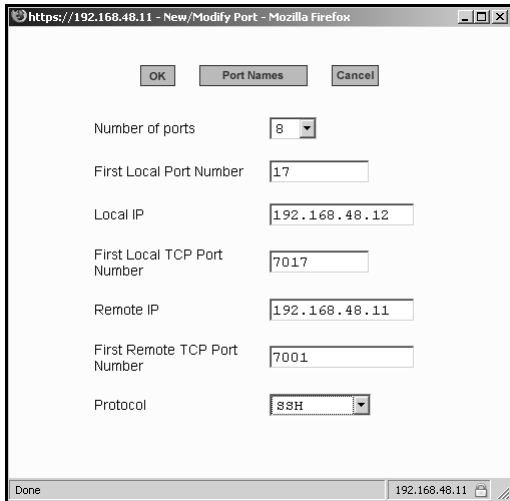


Figure 8.5: Ports - Virtual Ports - New/Modify Port Dialog Box

The following table describes the fields available in the Virtual Ports New/Modify Port dialog box.

Once you have configured the slave console server and defined the cluster parameters, the slave serial ports and the connected devices are accessible from the master console server under Applications - Connect - Serial pull-down menu.

To cluster console servers or modify cluster configuration:

Use this procedure if you wish to cluster console servers and add or modify ports.

NOTE: The console servers should be connected individually to an IP network. The units should not be cascaded.

1. Go to *Ports - Virtual Ports* in Expert mode and click the *Add* button to add new slave ports or click the *Edit* button to edit a slave port. The New/Modify Port dialog box appears.

https://192.168.48.11 - New/Modify Port - Mozilla Firefox

OK Port Names Cancel

Number of ports 8

First Local Port Number 17

Local IP 192.168.48.12

First Local TCP Port Number 7017

Remote IP 192.168.48.11

First Remote TCP Port Number 7001

Protocol SSH

Done 192.168.48.11

Figure 8.6: Ports - Virtual Ports - New/Modify Port Dialog Box

2. From the pull-down menu select the number of ports that you wish to assign as slaves. Choices are 1, 4, 8 and 16.
3. Enter the First Local Port Number. This is the first port number on the master.
4. Enter the Local IP address. This is the IP address of the master.
5. Enter the First Local TCP Port Number. This is the first TCP port number on the master.
6. Enter the Remote IP address. This is the IP address of the slave.
7. Enter the First Remote TCP Port Number. This is the first TCP port number of the slave. The default is 7001.
8. Select the communication protocol between the master and the slave from the Protocol pull-down menu. The options are Telnet or SSH.

To assign names to slave ports in the cluster

Selecting the *Port Names* button on the New/Modify Port dialog box, displays the form shown in the following figure.

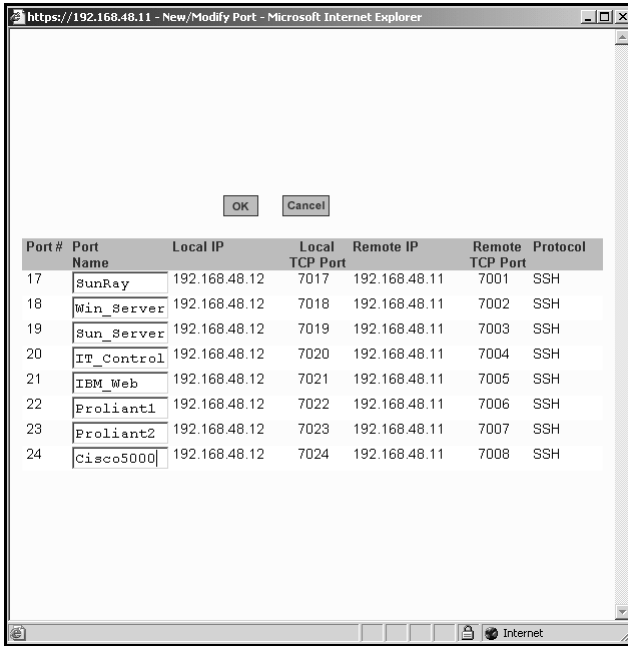


Figure 8.7: Ports - Virtual Ports - New/Modify - Port Names Dialog box

Use this form to assign a name or alias to the slave ports in the cluster. Use a naming convention for effective management of the console server and the connected devices on your network.

Ports Status

Selecting *Ports - Port Status* in Expert mode displays the following read-only form, which displays tabular serial port status information.

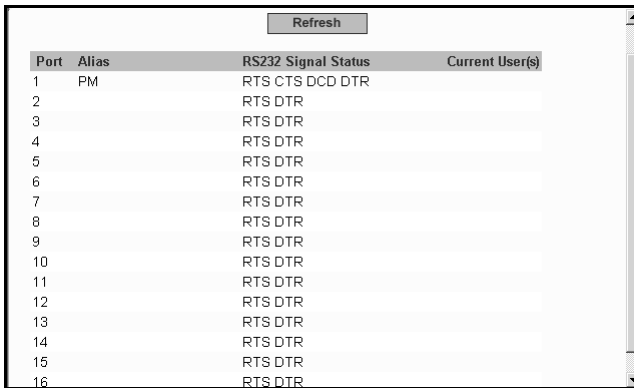


Figure 8.8: Ports - Ports Status (Read-Only)

The information in the following table is available in the Ports Status read-only form. All users have access to this form. The information on this page gets updated when you click the *Refresh* button.

Table 8.9: Expert - Port Status Read-Only Form

Column Name	Description
Port	The serial port number.
Alias	Displays the name (alias) for the serial port if one is assigned by the administrator.
RS232 Signal Status	Serial Communication Signal Status.
Current User(s)	Displays the user(s) connected to each serial port.

Ports Statistics

Selecting *Ports - Port Statistics* in Expert mode, displays the following read-only form.

Port/Alias	Baud Rate	Tx bytes	Rx bytes	Frame	Parity	Break	Overrun
1 PM	9600	1043	7276	0	0	0	0
2 Thinkpad	9600	67282	461	0	0	0	0
3 Telnet	9600	13782	99	0	0	0	0
4	9600	0	0	0	0	0	0
5	9600	0	0	0	0	0	0
6	9600	0	0	0	0	0	0
7	9600	0	0	0	0	0	0
8	9600	0	0	0	0	0	0
9	9600	0	0	0	0	0	0
10	9600	0	0	0	0	0	0
11	9600	0	0	0	0	0	0
12	9600	0	0	0	0	0	0
13	9600	0	0	0	0	0	0
14	9600	0	0	0	0	0	0
15	9600	0	0	0	0	0	0
16	9600	0	0	0	0	0	0

Figure 8.9: Ports - Port Statistics (Read-Only)

The following information is available in the Ports Statistics read-only form. All users have access to this form. The information on this page gets updated when you click the *Refresh* button.

Table 8.10: Expert - Ports - Port Status Read-Only Form

Column Name	Description
Port	The serial port number.
Alias	Displays the name (alias) for the serial port if one is assigned by the administrator.
Baud Rate	The measure of how fast data is moving between devices.
Tx Bytes	Data transmitted.

Table 8.10: Expert - Ports - Port Status Read-Only Form (Continued)

Column Name	Description
Rx Bytes	Data received.
Frame	A formatted packet of data usually associated with the Data-Link layer.
Parity	Error checking bit appended to a data packet. A method of checking the accuracy of transmitted characters. Parity is usually not used, but can be odd or even. A None parity means that data has not exchanged.
Break	An out-of-band signal on an RS-232 serial port that involves making the Tx data line active for more than two whole character times (or about 2ms on a 9600bps line).
Overrun	The amount of time it takes for the new data to overwrite the older unread data.

Administration Menu and Forms

System Information

Selecting *Administration - System* information in Expert mode displays a form containing information about all of the system parameters as shown in the following table.

Table 9.1: System Information Form

Information	Parameters
System Information	<ul style="list-style-type: none"> • Kernel Version • Current Date • Up Time • Power Supply State
CPU Information	<ul style="list-style-type: none"> • CPU Type • Clock Speed • Revision • Bogomips
Memory Information	<ul style="list-style-type: none"> • MemTotal • MemFree • Buffers • Cached • SwapCached • Active • Inactive • HighTotal • HighFree • LowTotal • LowFree • SwapTotal • SwapFree • Dirty • Writeback • Mapped • Slab • CommitLimit • Committed_AS • PageTables • VmallocTotal • VmallocUsed • VmallocChunk
Ram Disk Usage	<ul style="list-style-type: none"> • Filesystem • 1k-blocks • Used • Available • Use% • Mounted

To view system information:

Go to *Administration - System Information* in Expert mode. The System Information form displays. Scrolling down the form allows you to see all of the information.

Notifications

Selecting *Administration - Notifications* in Expert mode displays the Notifications form, allowing you to set up alarm notifications about system issues or other events of interest that occur on the devices connected to the serial ports. You can configure notifications to be sent to users through email, pager or SNMP traps.

Clicking the *Edit* button displays the Notifications Entry dialog box.

The form allows you to define alarm trigger actions and specify how to handle them. Different fields appear on the dialog boxes depending on whether *Email*, *Pager* or *SNMP Trap* notification have been selected from the Notifications form.

To choose a method for sending notifications for serial port data buffering events:

1. Go to *Administration - Notifications* in Expert mode. The Notifications form displays.
2. Enable *Notification Alarm for Data Buffering* by clicking the checkbox.
3. Select *Email*, *Pager* or *SNMP Trap* from the pull-down menu.
4. To create a new entry for an event to trigger an alarm or notification, click the *Add* button.
5. To edit a previously-configured trigger, click the *Edit* button.

Email Notifications Entry

When you select *Email* from the pull-down menu and click either the *Add* or *Edit* button, the Email Notification dialog box is displayed.

To configure a trigger for email notification for serial ports:

1. Go to *Administration - Notifications* in Expert mode and select *Email* from the pull-down menu. If desired, enable *Notification Alarm for Data Buffering* for an alarm to sound when the trigger action occurs; and click either *Add* or *Edit*. The Notifications Entry dialog box displays.
2. Specify the event you wish to trigger a notification in the Alarm Trigger field.
3. If you need to edit an existing notification select it from the pull-down list and proceed.
4. Enter or change the recipient for the notification email in the To field.
5. Enter or change the sender email address in the From field.
6. Enter or change the subject in the Subject field.
7. Enter or edit the text message in the Body field.
8. Enter or change the SMTP server's IP address in the SMTP Server field.
9. Enter or change the SMTP port number in the SMTP Port field.
10. Click *OK*.

11. Click *apply changes*.

Pager notifications entry

When you go to *Administration - Notifications*, select *Pager* from the pull-down menu and click on *Add* or *Edit* button the Pager Notifications Add/Edit dialog box displays.

To configure a trigger for pager notification for serial ports:

1. Go to *Administration - Notifications* in Expert mode and select *Pager* from the pull-down menu. If desired, enable *Notification Alarm for Data Buffering* for an alarm to sound when the trigger action occurs; and click either *Add* or *Edit*. The Notifications Add/Edit dialog box displays.
2. Specify the event you wish to trigger a notification in the Alarm Trigger field.
3. If you need to edit an existing notification, select it from the pull-down list and proceed.
4. Enter or change the pager number in the Pager Number field.
5. Enter or edit the text that describes the event in the Text field.
6. Enter or change the Short Message Services (SMS) username, the SMS server's IP address or name and the SMS port number in the SMS User Name, SMS Server and SMS Port fields respectively.
7. Click *OK*.
8. Click *apply changes*.

SNMP trap notifications entry

When you go to *Administration - Notifications* and select *SNMP Trap* from the pull-down menu and then click on the *Add* or *Edit* button, the Notifications SNMP Add/Edit dialog box displays.

SNMP traps are event notifications sent to a list of responsible parties set up to receive alerts for the managed systems. Any SNMP enabled device generates Fault Reports (Traps) that are defined in the Management Information Base (MIB). SNMPv1 and SNMPv2 define the messaging format for the trap. The following table describes the available fields in the SNMP trap notification entry dialog box.

To configure a trigger for SNMP trap notification for serial ports:

1. Go to *Administration - Notifications* in Expert mode, select *SNMP Trap* from the pull-down menu. If desired, enable *Notification Alarm for Data Buffering* for an alarm to sound when the trigger action occurs and click either *Add* or *Edit*. The Notifications Entry dialog box is displayed.
2. Specify the event you wish to trigger a notification in the Alarm Trigger field.
3. If you need to edit an existing notification select it from the pull-down list and proceed.
4. Enter or change the number in the OID Type Value field.
5. Accept the trap number or select a new one from the Trap Number pull-down menu.
6. Enter a community in the Community field.

7. Enter the IP address of the SMTP Server.
8. Enter a message in the Body text area.
9. Click *OK*.
10. Click *apply changes*.

Serial ports alarm notification

You can configure the notification entry form to monitor the DCD signal so that the system will generate an alarm in any of the following events.

- A serial console cable is removed from the console server
- A device/server attached to the console is powered down

The configuration also enables you to detect if a modem is in use and is still powered on and active.

To configure a trigger for serial port alarm notification:

1. Go to *Administration - Notifications* in Expert mode.
2. Enable the checkbox for *Notification Alarm for Data Buffering*.
3. Select *Email*, *Pager* or *SNMP Trap* from the pull-down menu.
4. Click the *Add* button.
5. Enter **Port** in the Alarm Trigger field.
6. Configure the parameters selected in step 3. See *Notifications* on page 84.
7. Click *OK*.
8. Click *apply changes*.

Time/Date

Selecting *Administration - Time/Date* in Expert mode displays the form shown in the following figure.

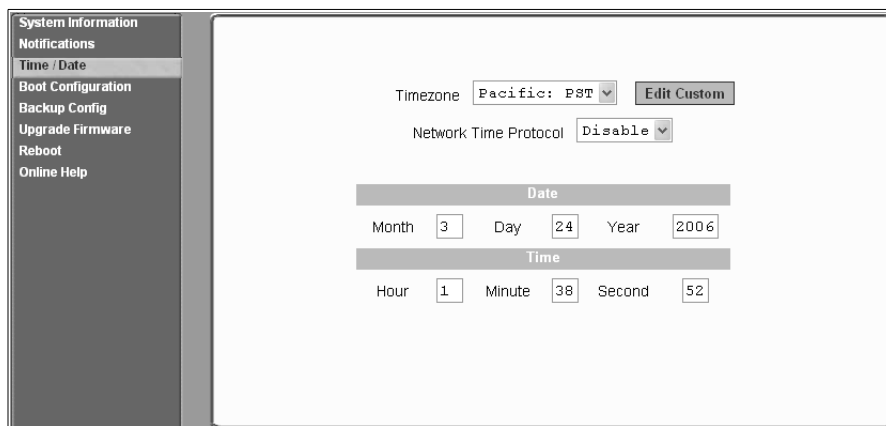
The screenshot shows a web-based configuration interface. On the left is a vertical navigation menu with the following items: System Information, Notifications, Time / Date (highlighted), Boot Configuration, Backup Config, Upgrade Firmware, Reboot, and Online Help. The main content area displays the 'Time/Date' configuration form. At the top, there is a 'Timezone' dropdown menu set to 'Pacific: PST' and an 'Edit Custom' button. Below that is a 'Network Time Protocol' dropdown menu set to 'Disable'. The form is divided into two sections: 'Date' and 'Time'. The 'Date' section has three input fields: 'Month' (3), 'Day' (24), and 'Year' (2006). The 'Time' section has three input fields: 'Hour' (1), 'Minute' (38), and 'Second' (52).

Figure 9.1: Expert - Administration - Time/Date

You can use the Time/Date form in Expert mode to set the console server's time and date by manually entering the time and date information in the form or setting it up to acquire time and date information from the NTP server, which synchronizes the console server's system clock with any of several NTP servers available on the Internet.

To set the time and date manually:

1. Go to *Administration - Time/Date* in Expert mode. The Time/Date form displays.
2. Select a time zone from the Timezone pull-down list.
3. If necessary, select *Disable* from the Network Time Protocol pull-down. NTP is disabled by default.
4. Type the date and time in the fields provided.
5. Click *apply changes*.

To configure time and date using an NTP server:

NTP is disabled by default.

1. Go to *Administration - Time/Date* in Expert mode. The Time/Date form displays.
2. Select a time zone from the Timezone pull-down list.
3. Select *Enable* from the Network Time Protocol pull-down menu. When NTP is enabled, the following form is displayed.

Timezone

Network Time Protocol

NTP Server

Figure 9.2: Expert - Administration - Time and Date - NTP Enable

4. Type the IP address of the NTP server in the NTP Server field.
5. Click *OK*.
6. Click *apply changes*.

Setting up a customized time zone configuration

The Edit Custom button next to the Timezone field allows you to set up a customized time zone function, such as for daylight savings time or any other time zone offset anomaly that might occur anywhere in the world. You can create a time zone identifier of your choice, which is added to the Timezone pull-down menu options in the main Time/Date form. When you select the *Edit Custom* button, the following dialog box will appear.

OK Cancel

Timezone Name

Standard Time Acronym GMT off

Enable daylight saving time

Done Internet

Figure 9.3: Expert - Administration - Time/Date - Edit Custom

To create a custom time zone selection:

1. Enter the name of the time zone you would like to appear in the Timezone pulldown menu on the main Time/Date form. (**Pacific** entered here as an example.)
2. Choose a preferred or standard acronym for the time zone (**PST** is shown here for Pacific Standard Time).
3. Enter the offset from GMT for the time zone (west of GMT is entered as a negative number).
4. Click *OK*.
5. Click *apply changes*.

To use the custom option to set daylight savings time:

1. Select the *Enable daylight saving time* checkbox. A Timezone Configuration dialog box appears.
2. Enter the daylight savings time (DST) acronym of your choice in the DST Acronym field.
3. Enter the number of hours and minutes (**HH:MM** format) the clock will be reset at the beginning of the daylight savings time period. (Positive number only.)
4. In the following fields, enter the date (month, day) and time (hours:minutes) for both the beginning and ending dates of daylight time.
5. Click *OK* to update the Time/Date settings and return to the main Time/Date form.
6. Click *apply changes*.

Boot Configuration

Boot configuration defines the location from which the console server loads the operating system. The console server can boot from its internal firmware or from the network. By default, the Cyclades CS console server boots from Flash memory. Selecting *Administration - Boot Configuration* in Expert mode displays the Boot Configuration form.

If you need to boot from the network, make sure the following prerequisites are met:

- A TFTP or BootP server must be available on the network
- An upgraded console server boot image file must be downloaded from Avocent and made available on the TFTP or BootP server
- The Cyclades CS console server must be configured with a fixed IP address
- The boot filename and the IP address of the TFTP or BootP server is known.

Table 9.2: Boot Configuration Form Fields

Field Name	Definition
IP Address assigned to Ethernet	A fixed IP address or a DHCP assigned IP address to the console server.
Watchdog Timer	Whether the Watchdog Timer is active or inactive. If the Watchdog Timer is active, the console server reboots if the software crashes.
Unit boot from	Specify whether to boot the console server from Flash or from the network.
Boot Type	Select to boot from a TFTP server, a BootP server or both.
Boot File Name	Filename of the boot program.
Server's IP Address	The IP address of the TFTP or the BootP server.
Console Speed	An alternative console speed from 4800 to 115200 (9600 is the default).
Flash Test	Select to test boot from the Flash card. You can skip this test or do a full test.

Table 9.2: Boot Configuration Form Fields (Continued)

Field Name	Definition
RAM Test	Select to test boot from RAM. You can skip this test, do a quick test or a full test.
Fast Ethernet	The speed of the Ethernet connection. Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value): <ul style="list-style-type: none"> • 100BaseT Half-Duplex • 100BaseT Full-Duplex • 10BaseT Half-Duplex • 10BaseT Full-Duplex
Fast Ethernet Max. Interrupt Events	The maximum number of packets that the CPU handles before an interrupt (0 is the default).

To configure the console server boot:

1. Go to *Administration - Boot Configuration* in Expert mode. The Boot Configuration form displays.
2. Enter the IP address of the console server in the IP Address assigned to Ethernet field.
3. Accept or change the selected option in the Watchdog Timer field.
4. Select *Flash* or *Network* from the *Unit boot from* menu.
5. Select *TFTP*, *BootP* or *Both* from the Boot Type menu if you have selected *Network* from the *Unit boot from* in step 4.
6. Accept or change the filename of the boot program in the Boot File Name field.
7. If specifying network boot, perform the following steps:
 - a. Enter the IP address of the TFTP or BootP server in the Server's IP Address field.
 - b. Select a console speed from the Console Speed pull-down menu to match the speed of the terminal you are using on the console port of the console server.
 - c. Select *Skip* or *Full* from the Flash Test pull-down menu to bypass or run a test on the Flash memory at boot time.
 - d. Select *Skip*, *Quick* or *Full* from the RAM Test pull-down menu to bypass or run a test on the RAM at boot time.
 - e. Choose an Ethernet speed from the Fast Ethernet pull-down menu.
 - f. Specify the maximum number of packets that the CPU handles before an interrupt in the Fast Ethernet Max. Interrupt Events field.
8. Click *apply changes*.

Backup Configuration

Selecting *Administration - Backup Config* in Expert mode displays the Backup Configuration form.

The Type pull-down menu options on this form are FTP and Storage Device. If *Storage Device* is selected, the storage device can be a CompactFlash drive.

NOTE: Use an FTP server to save and retrieve your console server configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from the console server by pinging the FTP server. Use a storage device such as a CompactFlash drive to save your configuration...

Table 9.3: Backup Configuration Settings if Using FTP Server

Field	Definition
Server IP	IP address of an FTP server on the same subnet as the console server. (Verify accessibility by pinging the FTP server.)
Path and Filename	Path of a directory on the FTP server where you have write access for saving the backup copy of the configuration file. Specify a filename if you wish to save the file under another name. For example, to save the configuration file <code>zvmppccs.0720_qa.ccs-k26</code> in a directory called <code>/upload</code> on the FTP server, you would enter the following in the Path and Filename field: <code>/upload/zvmppccs.0720_qa.ccs-k26</code>
Username and Password	Obtain the user name and password to use from the FTP server's administrator.
Save	Saves the configuration.
Load	Downloads a previously saved copy of the configuration file from the selected device.

Table 9.4: Backup Configuration if Using Storage Device

Field Name	Definition
Default Configuration	The system saves the configuration in the storage device but does not override the internal Flash configuration after reboot.
Replace Configuration	The system saves the configuration in the storage device with a flag REPLACE used by the RESTORECONF utility to override the internal Flash configuration after reboot.

To back up or restore the configuration files using an FTP server:

1. Go to *Administration - Backup Config* in Expert mode.
2. Select *FTP* from the Type pull-down menu.
3. Enter the IP address of the FTP server in the Server IP field.
4. Enter the directory path on the FTP server where you have write permissions in the Path and Filename field. Enter the filename after the directory path. For example, **`/upload/zvmppccs.0720_qa.ccs-k26`**.
5. Enter the user name and password provided by your system administrator for the FTP server.

6. To back up a copy of the current configuration files, press the *Save* button.
7. To download a previously saved copy of the configuration files, press the *Load* button.

To back up or restore the configuration files using a storage device:

1. Go to *Administration - Backup Config* in Expert mode.
2. Select *Storage Device* from the Type pull-down menu.
3. To back up a copy of the current configuration files, select *Default Configuration* and press the *Save* button.
4. To restore a copy of the configuration files saved on the storage device without replacing the internal Flash configuration, select *Default Configuration* and press the *Load* button.
5. Click *apply changes*.
6. Reboot the system. See *Reboot* on page 93 for details.
7. To replace the configuration saved on the storage device previously, select *Replace Configuration* and click the *Save* button.
8. To restore a copy of the configuration files saved on the storage device and replace the internal Flash configuration, select *Replace Configuration* and click the *Load* button.
9. Click *apply changes*.
10. Reboot the system. See *Reboot* on page 93 for details.

Upgrade Firmware

Selecting *Administration - Upgrade Firmware* in Expert mode displays the Upgrade Firmware form. You can use this form to configure an automated upgrade of the console server's firmware, which includes the Kernel, applications and configuration files. The firmware is upgradeable using an FTP server.

NOTE: Check the file name for the upgrade version and read the upgrade instructions carefully. Distinct procedures are required depending on the version you are upgrading from.

To upgrade the console server firmware:

This procedure is for upgrading the latest release of the console server firmware. The upgrade installs the software on the Flash memory.

1. Go to *Administration - Upgrade Firmware*. The Upgrade Firmware form displays.
2. Choose *FTP* from the Type menu. (FTP is the only supported type).
3. Enter the URL of the FTP server in the FTP Site field.
4. Enter the username recognized by the FTP server in the Username field.
5. Enter the password associated with the username on the FTP server in the Password field.
6. Enter the pathname of the file on the FTP server in the Path and Filename field.
7. Click the *Upgrade Now* button.

8. Click *cancel changes* if you need to restore the backed up configuration files.

Reboot

Selecting Administration - Reboot in Expert mode brings up a simple form containing only a Reboot button. Clicking the Reboot button reboots the console server.

To reboot the console server:

1. Go to *Administration - Reboot* in Expert mode.
2. Click the *Reboot* button. A confirmation dialog box displays.
3. Click *OK*.

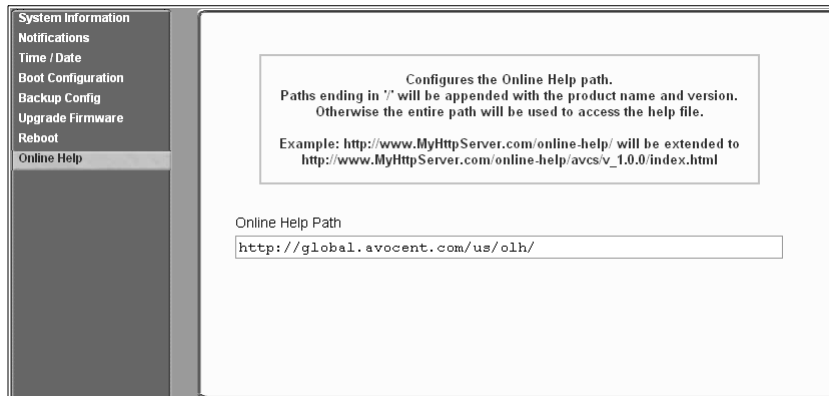
Online Help

When the online help feature is configured for your console server, clicking the *Help* button from any form on the Web Manager opens a new window and redirects its content to the configured path for the online help product documentation.

NOTE: Using the online help feature from the Avocent server is not always possible due to firewall configurations, nor is it recommended. It is generally advisable for you to use the online help system provided with the product or download the online help .zip file and run it from a local server.

Online help for the Cyclades CS console server is shipped with the product and should be loaded on a local server. The system administrator can also download the online help from Avocent. For more information on downloading the online help, contact Technical Support. The procedure for configuring the online help on the local server follows.

Selecting *Administration - Online Help* in Expert mode brings up the form shown in the following figure.



System Information
Notifications
Time / Date
Boot Configuration
Backup Config
Upgrade Firmware
Reboot
Online Help

Configures the Online Help path.
Paths ending in '/' will be appended with the product name and version.
Otherwise the entire path will be used to access the help file.
Example: `http://www.MyHttpServer.com/online-help/` will be extended to
`http://www.MyHttpServer.com/online-help/avcs/v_1.0.0/index.html`

Online Help Path

Figure 9.4: Expert - Administration - Online Help

The console server administrator can either use the supplied online help or download the online help .zip file and reconfigure the path to a local server where the online help can be stored and

accessed by the Web Manager. The console server firmware stores the new link in Flash and accesses the online help files whenever the help button is clicked.

The Online Help Path field is where the path will be entered for the Web Manager to locate the online help files. The Help button on the Web Manager looks for its help files in the location specified here. By default, `http://global.avocent.com/us/olh/` is the location specified in the field. It is recommended that the console server administrator reconfigure this path to use a local server.

The console server administrator can change the URL in the URL Prefix field to point the Help button to the new local server location for the files.

To configure the local online help path:

1. Extract the files using the appropriate unzip utility for your O/S and put them into the desired directory under the web server's root directory. This must be a publicly accessible web server

For example, the following command line would work on a server running UNIX.

```
#cd $WEB_SERVER_ROOT/ccs-help  
#gunzip ccs_online_hlp.zip
```

By default, the online help files are expanded into a console server directory under the directory where the zip file is located.

2. Log into the Web Manager as admin and go to *Administration - Online Help*. The Help configuration screen displays (see *Figure 9.4*).
3. In the URL prefix field, enter the URL of the help files on the server where you installed them.

The following example would work for a web server named remoteadmin.

<http://www.remoteadmin.com/online-help/>

The software adds the name of the ccs directory to the URL prefix and launches the online help.

4. Click *Save*.
5. Click *apply changes*.

APPENDICES

Appendix A: Technical Specifications

Table A.1: Technical Specifications for the Cyclades® CS console server Hardware

CPU	MPC855T (PowerPC Dual-CPU)
Memory	128MB DIMM SDRAM / 16MB CompactFlash
Interfaces	1 Ethernet 10/100BT on RJ45 1 RS232 Console on RJ45 RS232 Serial Ports on RJ45
Power	Internal 100-240VAC, 50/60 Hz†
Operating Temperature	50°F to 112°F (10°C to 44°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 90% non-condensating
Dimensions	console server 1-3: 6.3 x 4.0 x 1.5 in (16 x 10 x 3.8 cm) console server 4-48: 17 x 8.5 x 1.75 in (43.18 x 21.59 x 4.45 cm)
Certification	FCC Part 15, A EN55022, A (CE) EN55024 UL 60950-1, CSA 60950-1-03 Solaris Ready™

Appendix B: Safety, Regulatory and Compliance Information

Safety and environmental guidelines for rack-mounting the console server

NOTE: Each heading and its contents in this section is also provided in German (*Deutsch*) in italics immediately following the English version.

The following considerations should be taken into account when rack-mounting the Cyclades CS console server.

Folgendes sollte beim Rack-Einbau des Cyclades CS berücksichtigt werden.

Temperature

The manufacturer's maximum recommended ambient temperature for the Cyclades CS console server is 122 °F (50 °C).

Temperatur

Die maximal empfohlene Umgebungstemperatur des Cyclades CS beträgt 50 °C (122 °F).

Elevated operating ambient temperature

If the console server is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature. See above.

Erhöhte Umgebungstemperatur im betrieb

Bitte treffen Sie entsprechende Vorkehrungen um die Herstellerangaben zur maximalen Umgebungstemperatur einzuhalten. Bitte beachten Sie, dass bei einer Installation des Cyclades CS console server in einem geschlossenen oder mehrfach bestücktem Rack die Umgebungstemperatur im Betrieb höher sein kann als die Raumtemperatur.

Reduced air flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Luftdurchsatz

Für einen sicheren Betrieb bitte auf ausreichenden Luftdurchsatz im Rack achten.

Mechanical loading

Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Sicherer mechanischer Aufbau

Bitte vermeiden Sie beim Einbau der Geräte ungleichmäßige mechanische Belastung.

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. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Elektrische Überlastung

Bitte beachten Sie beim elektrischen Anschluss der Geräte, dass diese zum Schutz vor Überlastung mit entsprechenden Schutzvorkehrungen ausgestattet sein können. Bitte sorgen Sie gegebenenfalls für Klarheit durch entsprechende Beschriftung:

Reliable earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit, such as power strips or extension cords.

Zuverlässige Erdung

Eine ausreichende Erdung der im Rack montierten Geräte muss sichergestellt sein. Insbesondere sollte indirekten Verbindungen zur Stromversorgung über Powerleisten oder Verlängerungen besondere Aufmerksamkeit gewidmet werden.

Safety precautions for operating the console server

Please read all the following safety guidelines to protect yourself and your Cyclades CS console server.

Sicherheitsvorkehrungen beim Betrieb des Cyclades CS console server

Bitte lesen Sie alle folgenden Sicherheitsrichtlinien um sich und Ihren Cyclades CS console server vor Schäden zu bewahren.

WARNING: Do not operate your Cyclades CS console server with the cover removed.

Vorsicht: Bitte betreiben Sie den Cyclades CS console server nicht mit geöffnetem Gehäuse.

CAUTION: To avoid shorting out your Cyclades CS console server when disconnecting the network cable, first unplug the cable from the Host Server, unplug external power (if applicable) from the equipment and then unplug the cable from the network jack. When reconnecting a network cable to the back of the equipment, first plug the cable into the network jack and then into the Host Server equipment.

Vorsicht: Um Schäden beim Entfernen des Netzkabels zu vermeiden bitte immer zuerst das Kabel vom Host Server entfernen, anschließend die externe Stromzufuhr abklemmen und danach das Kabel aus der Netzbuchse ausstecken. Beim Wiederherstellen der Verbindung immer zuerst das Kabel in die Netzbuchse des Cyclades CS console server zuerst einstecken und danach das Kabel in den Host Server einstecken.

CAUTION: To help prevent electric shock, plug the Cyclades CS console server into a properly grounded power source. The cable is equipped with a three-prong plug to help ensure proper grounding. Do not use adaptor plugs or remove the grounding prong from the cable. If you have to use an extension cable, use a three-wire cable with properly grounded plugs.

Vorsicht: Um Stromschläge zu vermeiden den Cyclades CS console server bitte mit einer ausreichend geerdeten Stromquelle verbinden. Zu diesem Zweck ist das Eingangskabel mit einem dreipoligen Stecker ausgestattet. Bitte keinesfalls dazwischen liegende adaptor einsetzen oder den Erdungsstift entfernen. Falls eine Verlängerung eingesetzt werden muss bitte ausschließlich dreipolige Kabel mit ausreichender Erdung verwenden.

CAUTION: To help protect the Cyclades CS console server from electrical power fluctuations, use a surge suppressor, line conditioner or uninterruptible power supply. Be sure that nothing rests on the cables of the console server and that they are not located where they can be stepped on or tripped over. Do not spill food or liquids on console server.

Vorsicht: Um den Cyclades CS console server vor elektrischen Netzschwankungen zu bewahren bitte Überspannungsfiler, Entstörfiler oder eine UVS einsetzen. Stellen Sie bitte sicher dass sich keine Gegenstände auf den Kabeln des Cyclades CS console server befinden und dass die Kabel tritt- und stolpersicher geführt sind. Bitte keine Lebensmittel oder Flüssigkeiten über den Cyclades CS console server schütten.

CAUTION: Do not push any objects through the openings of the Cyclades CS console server. Doing so can cause fire or electric shock by shorting out interior components.

Vorsicht: Zur Vermeidung von Brandgefahr oder elektrischen Schlägen bitte keine Gegenstände durch die Öffnungen des Cyclades CS console server stecken.

CAUTION: Keep your Cyclades CS console server away from heat sources and do not block host's cooling vents.

Vorsicht: Der Cyclades CS console server muss vor Hitzequellen geschützt werden und die Lüfterausgänge dürfen nicht blockiert sein.

Working inside the console server

Do not attempt to service the console server yourself, except when following instructions from Avocent Technical Support personnel. In the latter case, first take the following precautions:

1. Turn the console server off.
2. Ground yourself by touching an unpainted metal surface on the back of the equipment before touching anything inside the unit.

Electrostatic Discharge (ESD) Precautions

When handling any electronic component or assembly, you must observe the following antistatic precautions to prevent damage.

- Always wear a grounded wrist strap when working around printed circuit boards
- Treat all assemblies, components and interface connections as static-sensitive

- Avoid working in carpeted areas
- Keep body movement to a minimum while removing or installing boards to minimize the buildup of static charge

Arbeiten am Cyclades CS console server

Bitte versuchen Sie nicht den Cyclades CS console server selbst zu warten mit Ausnahme unter Befolgung der Anweisungen von Avocent technischem Personal. In diesem Fall bitte folgenden Vorsichtsmaßnahmen einhalten:

1. Schalten Sie den Cyclades CS console server aus.
2. Erden Sie sich bitte selbst durch Berühren einer blanken Metalloberfläche auf der Rückseite des Gerätes bevor Sie das Innere berühren

Vorsichtsmassnahmen gegen Elektrostatische Entladung (ESD)

Zur Vermeidung von Beschädigungen sind bei Arbeiten an elektronischen Komponenten oder Baugruppen die folgenden Vorsichtsmaßnahmen einzuhalten

- Bitte immer ein Erdungsarmband während der Arbeit an elektronischen Platinen tragen
- Bitte alle Baugruppen, Komponenten und Steckkontakte als elektrostatisch sensitiv behandeln
- Bitte Arbeiten auf Teppichböden vermeiden
- Zur Minimierung von elektrostatischen Aufladungen alle Körperbewegungen während Ein- oder Ausbau von Boards auf ein Minimum reduzieren

FCC warning statement

The Cyclades CS console server has been tested and found to comply with the limits for Class A digital devices, 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 Installation and Service 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 is required to correct the problem at his or her own expense.

Notice about FCC compliance for all Cyclades CS console server models

To comply with FCC standards, the Cyclades CS console server requires the use of a shielded CAT 5 cable for the Ethernet interface. Notice that this cable is not supplied with either of the products and must be provided by the customer.

Canadian DOC notice

The Avocent Cyclades CS console server 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.

L'Avocent Cyclades CS console server server 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 edicté par le Ministère des Communications du Canada.

Aviso de Precaución S-Mark Argentina

Por favor de leer todos los avisos de precaución como medida preventiva para el operador y el Cyclades CS console server.

IMPORTANTE: No hacer funcionar el Cyclades CS console server con la tapa abierta.

IMPORTANTE: Para prevenir un corto circuito en el Cyclades CS console server al desconectarlo de la red, primero desconectar el cable del equipo y luego el cable que conecta a la red. Para conectar el equipo a la red, primero conectar el cable a la red y luego al equipo.

IMPORTANTE: Asegurarse que el equipo este conectado a tierra, para prevenir un shock eléctrico. El cable eléctrico del equipo viene con tres clavijas para conectar asegurar conexión a tierra. No use adaptadores o quite la clavija de tierra. Si se tiene que utilizar una extensión, utilice una que tenga tres cables con clavija para conexión a tierra. Para proteger al Cyclades CS console server de fluctuaciones en corriente eléctrica, utilice una fuente eléctrica de respaldo. Asegurarse de que nada descansa sobre los cables del Cyclades CS console server, y que los cables no obstruyan el paso. Asegurarse de no dejar caer alimentos o bebidas en el Cyclades CS Console Server Installation, Administration and User's Guide. Si esto ocurre, avise a Avocent Corporation.

IMPORTANTE: No empuje ningún tipo de objeto en los compartimientos del Cyclades CS console serverserver. Hacer esto podría ocasionar un incendio o causar un corto circuito dentro del equipo.

IMPORTANTE: Mantenga el Cyclades CS console server fuera del alcancé de calentadores, y asegurarse de no tapar la ventilación del equipo.

IMPORTANTE: El Cyclades CS console server con alimentación de corriente directa (CD) solo debe ser instalado en áreas con restricción y de acuerdo a los artículos 110-18, 110-26, y 110-27 del National Electrical Code, ANSI/NFPA 701, Edición 1999. Para conectar la corriente directa (CD) al sistema, utilice cable de 0.75 mm (18 AWG). Instalar el interruptor corriente directa (CD) aprobado por UL entre la fuente de alimentación y el Cyclades CS console server. El límite mínimo del interruptor deberá ser 2 amperes, con conductor de 0.75 mm (18 AWG).

Trabajar dentro del Cyclades CS console server

No intente dar servicio al Cyclades CS console server, solo que este bajo la dirección de Soporte Técnico de Avocent. Si este es el caso, tome las siguientes precauciones:

Apague el Cyclades CS console server. Asegurase que este tocando tierra antes de tocar cualquier otra cosa, que puede ser al tocar la parte trasera del equipo.

Appendix C: Technical Support

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

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

INDEX**A**

- access 70
- access requirements, port 11
- access server
 - (CAS) profile, console 65
- accessing the web manager, other methods of 8
- active ports sessions 56
- adding
 - a group 54
 - a user 54
 - users 7
- admin 53
- administrative modes, overview of 15
- administrator forms, common features of 13
- alarm
 - notification 86
 - notification, serial ports 86
- alias 81
- alias, port IP 74
- authentication 57
 - for Cyclades CS logins, configuring 57
 - methods 70
 - servers, configuring 58
- authorization
 - raccess 58
- authorized users/groups 70
- authtype 57

B

- backup configuration 90
- banner, login 75

- basic installation procedures 3
- baud rate 20, 81
- boot configuration 89
- boot, to configure Cyclades CS 90
- bootp 89
- break 82
- break interval 75
- break sequence 75
- buffering
 - data 71
- bytes, RX 82
- bytes, TX 81

C

- Canadian doc notice 102
- CAS
 - profile, console access server 65
- CDMA 1
- Certificate for HTTP Security 61
- command, wiz 5
- common features of administrator forms 13
- community 39
- configuration
 - backup 90
 - boot 89
 - firewall 41
- configuring
 - authentication for Cyclades CS logins 57
 - authentication servers 58
 - ports 7
- connect 10, 29
- connect to Cyclades CS 11

- connect to serial ports 11
- connect, host to 75
- connection
 - protocol 12, 19
 - protocol modem 67
 - protocols terminal server (TS) profile 66
- console
 - access server CAS profile 65
 - raw 66
 - SSH 66
 - Telnet 66
 - TelnetSSH 66
- CPU usage 56
- CSLIP 67
- Cyclades CS
 - boot, to configure 90
 - connect to 11
 - firmware, to upgrade 92
 - logins, configuring authentication for 57
 - to reboot 93
- Cyclades CS console server
 - mounting 3
 - working inside the 100
 - working inside the console server 100

D

- data buffering 71
 - Destination 25
 - File Size 25
 - Mode 25
 - NFS File Path 25
 - time stamp 25
- data size 20
- data buffering events 84
- daylight savings time 89

- default IPaddress 8

E

- email notification 84
- email notifications 84
- Ethernet 90
- events, data buffering 84
- Expert mode 16
 - menus and forms mapping 28

F

- fallback mechanism 70
- FCC compliance 101
- FCC warning statement 101
- firewall configuration 41
- firmware, to upgrade the ACS's 92
- flash 89
- flow control 19
- forms
 - common features of administrator 13
 - mapping, Expert mode 28
 - regular user 10
- fragments 46
- frame 82
- FTP 91
- FTP server, using 91

G

- Group Authorization on LDAP 60
- group, adding 54
- groups, users 53
- GSM 1

H

- host settings 34
- host table 49

host to connect 75

I

IDE timeout 74

input interface 46

installation procedures, basic 3

inverted checkbox 44

IP alias, port 74

IPaddress, default 8

ISDN 1

J

JCPU 56

K

keep-alive interval, TCP 74

L

LDAP 70

LDAP/local 70

LDAPdownlocal 71

local terminal 67

local/radius 71

local/TACACS+ 71

logging into the web manager 14

login banner 75

logins, configuring authentication for Cyclades CS
57

M

management information base (MIB) 37, 85

mapping, Expert mode menus and forms 28

master 77

menus and forms mapping, Expert mode 28

methods of accessing the web manager, other 8

MIB 37, 85

management information base 37, 85

mode

Expert 16

wizard 15

Modem 67

modem

connection protocol 67

modes, overview of administrative 15

mounting the Cyclades CS console server 3

multi-user 73

N

notification

alarm 86

email 84

pager 85

serial ports alarm 86

SNMP trap 85

notifications 84

NTP 87

server, using 87

O

OID 39

online help 94

OpenSSH 61

OpenSSL 61

options, stty 74

other methods of accessing the web manager 8

output interface 46

overflow 82

overview of administrative modes 15

P

pager notification 85

- parity 19, 82
- PCPU 56
- PCPU processing time 56
- physical ports 63
- port
 - TCP 74
- port access requirements 11
- port IP alias 74
- port number
 - TCP 12
- ports
 - configuring 7
 - physical 63
 - statistics 81
 - status 80
 - virtual 77
- ppp 67
- ppp-no auth 67
- pre-installation requirements 3
- profiles
 - security 60
 - serial port settings and security 60
- protocol
 - connection 12, 19
 - modem connection 67
 - terminal server (TS) profile connection 66

R

- raccess 58
- raccess authorization 58
- Radius 71
- Radius/local 71
- Radiusdownlocal 71
- RAM 90
- raw socket 67

- raw, console 66
- reboot 93
- reboot the Cyclades CS 93
- regular user 53
- regular user forms 10
- requirements, port access 11
- requirements, pre-installation 3
- root 1, 6
- routes, static 49
- RS232 signal 81
- RX bytes 82

S

- safety precautions 99
- Security Certificates 61
- security profiles 60
- security profiles, and serial port settings 60
- serial port settings and security profiles 60
- serial ports alarm notification 86
- serial ports, connect to 11
- sessions, active ports 56
- set the time and date 87
- settings, host 34
- simple network management protocol (SNMP) 37
- slave 77
- SLIP 67
- SNMP 37
- SNMP trap notification 85
- SNMP trap notifications 85
- SNMP, simple network management protocol 37
- SNMPv1 85
- SNMPv2 85
- SSH, console 66
- SSHv1 66
- SSHv2 67

- SSL certificate 61
- static routes 49
- statistics, ports 81
- status, ports 80
- stop bits 20
- storage device 91
- storage device, using 92
- stty options 74
- swpcached 83
- syscontact 39
- syslocation 39
- syslog 36
- system information 83
- system information, to view 84

T

- table, host 49
- TACACS+ 71
- TACACS+/local 71
- TACACS+downlocal 71
- TCP
 - flags 45
 - keep-alive interval 74
 - port 74
 - port numbers 12
- Technical support 104
- Telnet 66
- Telnet, console 66
- TelnetSSH, console 66
- terminal profile menu 30
- terminal server (TS) profile connection protocols 66
- terminal type 75
- terminal, local 67
- TFTP 89

- time/date 87
 - daylight savings time 89
- timer, watchdog 89
- to configure ACS boot 90
- to reboot the ACS 93
- to set the time and date 87
- to upgrade the ACS's firmware 92
- to view system information 84
- trap notification, SNMP 85
- TS profile connection protocols, terminal server 66
- TTY 56
- TX bytes 81

U

- upgrade
 - Cyclades CS's firmware 92
 - firmware 92
- usage, CPU 56
- user
 - adding 54
 - multi 73
 - regular 53
- user forms, regular 10
- users
 - adding 7
 - types of 3
- users and groups 53
- users/groups, authorized 70
- using a storage device 92
- using an FTP server 91
- using an NTP server 87

V

- view system information 84
- virtual ports 77

W

watchdog timer 89

web manager

 logging into 14

 other methods of accessing 8

wiz command 5

wizard mode 15

working inside the console server 100

X

X.509 Certificate on SSH 61



Avocent[®]

The Power of Being There[®]

For Technical Support:

www.avocent.com/support

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201 USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Canada
20 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1K3 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99