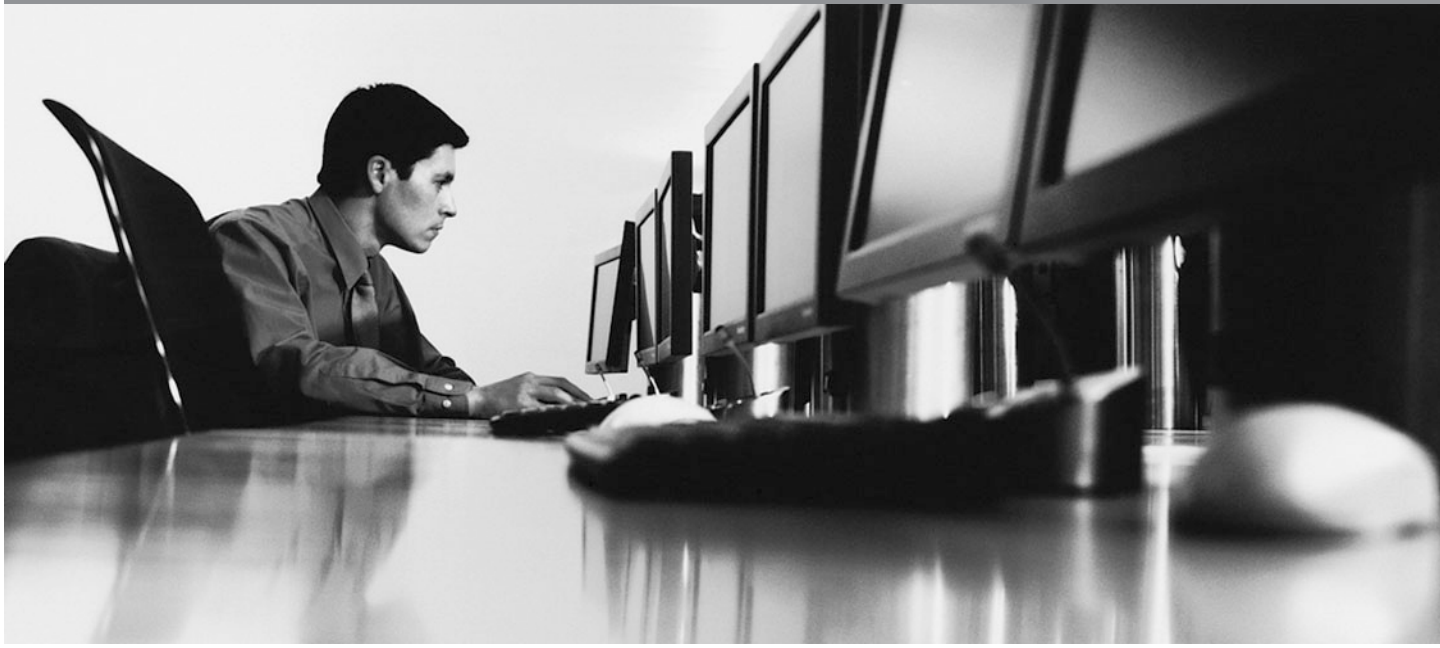Avocent®

CYCLADES® ACS 5000
Installation/Administration/User Guide

FCC Warning Statement

The Cyclades ACS 5000 advanced 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 ACS 5000 Advanced Console Server Models

To comply with FCC standards, the Cyclades ACS 5000 advanced console server requires the use of a shielded CAT 5 cable for the Ethernet interface. Notice that this cable is not supplied with the products and must be provided by the customer.

Canadian DOC Notice

The Cyclades ACS 5000 advanced 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'Cyclades ACS 5000 advanced console server n'émete 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.

Cyclades® ACS 5000

Installation/Administration/User Guide

Symbols Used

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.

Functional Earthing Terminal
This symbol indicates a terminal which serves the purpose of establishing chassis ground equal potential.

TABLE OF CONTENTS

Introduction

Overview

Each model in the Cyclades® ACS 5000 advanced console server family is a 1U appliance serving as a single access point for accessing and administering servers and other devices, supporting both IPv4 and IPv6 protocols. The following figure shows the front of the console server.
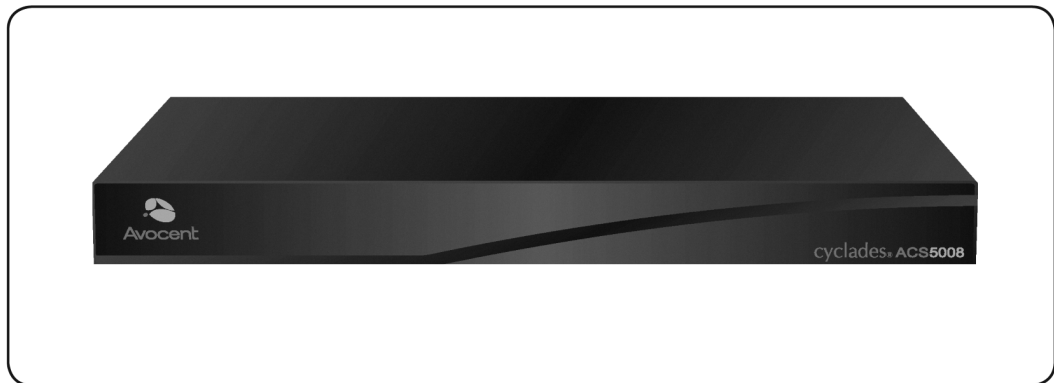
Figure 1.1: Front of the Console Server

Connectors on the Console Server

The following figure depicts the connectors on the back of a typical ACS 5000 console server.
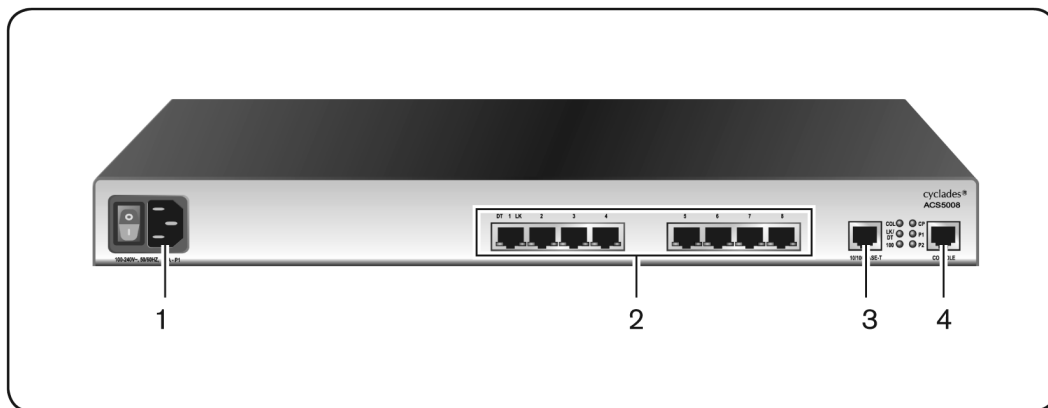
Figure 1.2: ACS 5000 Console Server Connectors

NOTE: The number of serial ports and power supplies depends on the model.

Table 1.1: ACS 5000 Console Server Connectors

Number	Description
1	Power connection. This may be single or dual power. Dual power requires two power cords.
2	Serial port connectors.
3	Ethernet port connectors.
4	Console port connectors.

Accessing the Console Server and Connected Devices

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

- Web manager through LAN/WAN IP networks.

- An external modem

- Using the web manager, you can log in and launch a console session such as Telnet or SSH to connect to the devices attached to the console server's serial ports.

- Connecting a server running a terminal emulation program enables an administrator to log into the console server and either enter commands in the console server shell or use the Command Line Interface (CLI) tool.

NOTE: Only one root or admin user can have an active CLI or web manager session. A second root or admin user must abort the session or close the other user's session.

CAUTION: If there are cron jobs running through automated scripts, a root or admin user login can cause the automated cron jobs to fail.

Web Manager

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 equipment connected to the console server.

The 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, cycle power and reboot connected devices.

Access the web manager using one of the following ways:

- The IP Network.
- A dial-in connection with an optional external modem connected to one of the serial ports.

Prerequisites for Using the Web Manager

The following conditions must be met prior to accessing the web manager.

- Basic network parameters must be defined on the console server so the web manager can be launched over the network.
- The dynamically-assigned IP address of the console server must be known. This address is found in one of the following three ways:
  - Make an inquiry to the DHCP server on the subnet that the console server resides, using the MAC address.
  - Connect to the 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 web manager user account must be defined. The admin has an account by default, and can add regular-user accounts to grant access to the connected servers or devices using the web manager.

Types of Users

The 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.

- Users who are in an Admin group with administrative privileges. The admin user belongs to this group.

- 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.

NOTE: It is strongly recommended that you change the default password **avocent** for the root and admin users before configuring the console server.

Security

The console server includes a set of security profiles that consists of predefined parameters to control access to the console server and its serial ports. This feature provides more control over the services that are active at any one time. As an additional security measure, all serial ports are disabled by default, allowing the administrator to enable and assign individual ports to users.

NOTE: The Default security profile parameters are the same as the Moderate profile.

Authentication

The console server supports a number of authentication methods to assist the administrator with user management. Authentication can be performed locally or with a remote server, such as RADIUS, TACACS+, LDAP or Kerberos. An authentication security fallback mechanism is also employed should the negotiation process with the authentication server fail. In such situations, the console server follows an alternate defined rule when the authentication server cannot authenticate the user.

The following table lists the supported authentication methods.

Table 1.2: Authentication Methods Supported

Authentication Type	Definition
None	No authentication.
DSView	Authentication is performed with a DSView® 3 server.
DSView/Local	DSView management software authentication is tried first, then Local.
DSViewDownLocal	Local authentication is performed only if the DSView 3 server is down.
Kerberos	Authentication is performed using a Kerberos server.
Kerberos/Local	Kerberos authentication is tried first, switching to Local if unsuccessful.
KerberosDownLocal	Local authentication is performed only when the Kerberos server is down.
LDAP	Authentication is performed against an LDAP database using an LDAP server.
LDAP/Local	LDAP authentication is tried first, switching to Local if unsuccessful.
LDAPDownLocal	Local authentication is performed only when the LDAP server is down.
LDAPDownLocal/Radius	Local authentication is performed only when the LDAP server is down, switching to Radius if unsuccessful.
Local	Authentication is performed locally. For example using the /etc/passwd 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.
Local/NIS	Authentication is performed locally first, switching to NIS if unsuccessful.
NIS	NIS authentication is performed.
NIS/Local	NIS authentication is tried first, switching to Local if unsuccessful.
NISDownLocal	Local authentication is performed only when the NIS server is down.
OTP	Uses the one time password (OTP) authentication method.
OTP/Local	Uses the local password if the OTP password fails.
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.

IPv6

The console server is compliant with IPv4, IPv6 and dual stack protocols so that you can enable IPv4 only, IPv6 only or both protocols, with support for dial-up connections and primary network connections. You can configure the appliance to obtain its IPv6 network parameters from a DHCPv6 server, by static configuration (IP address, prefix length and default gateway) or stateless auto-configuration. You can add an appliance to the local network using either its IPv6 address or a DNS name.

Services not supporting IPv6

The following services do not support IPv6:

- NIS authentication
- NFS data logging
- Virtual ports

VPN

The console server administrator can set up VPN connections to establish an encrypted communication between the console server and a host on a remote network. The encryption creates a security tunnel for dedicated communications.

You can use the VPN features on the console server to create a secure connection between the console server and every machine on the subnet at the remote location or between the console server and a single remote host.

To set up a security gateway, install IPSec on any machine performing networking over IP, including routers, firewall machines, application servers and end-user machines.

The ESP and AH authentication protocols are supported. RSA Public Keys and Shared Secret are supported.

For detailed information and procedures to configure a VPN connection, see *VPN Connections* on page 75.

Packet Filtering

The administrator can configure the device to filter packets like a firewall. IP filtering is controlled by chains and rules.

Structure of IP filtering

The Firewall Configuration form in the web manager is structured on two levels:

- The view table of the Firewall Configuration form containing a list of chains.

- The chains which contain the rules controlling filtering.

Chain

A chain is a named profile that includes one or more rules defining either a set of characteristics to look for in a packet or what to do with any packet having all the defined characteristics.

The console server filter table contains a number of built-in chains, each referenced according to the packet type they handle. As defined in the rules for the default chains, all input and output packets and packets being forwarded are accepted.

Rule

Each chain can have one or more rules that define either the packet characteristics being filtered or what to do when the packet matches the rule.

Each filtered packet characteristic is compared against the rules. All defined characteristics must match. If no rules are found then the default action for that chain is applied.

Administrators can:

- Add a new chain and specify rules for that chain

- Add new rules to existing chains

- Edit a built-in chain or delete the built-in chain rules

Add rule and edit rule options

When you add or edit a rule, you can define any of the options described in the following table.

Table 1.3: Add Rule and Edit Rule Option Definitions

Filter Options	Description
Source IP and Mask Destination IP and Mask	With source IP, incoming packets are filtered for the specified IP address. With destination IP, outgoing packets are filtered.
	If you fill in a source or destination mask, all packets are filtered for IP addresses from the subnetwork in the specified netmask.
	NOTE: For IPv6, only one field is available: <IP Address>/<Prefix>.
Protocol	Select protocol options for filtering from ALL, Numeric, TCP, UDP, ICMP (IPv4 only) and ICMPv6 (IPv6 only).
Input Interface	The input interface (eth0) used by the incoming packet.
Output Interface	The output interface (eth0) used by the outgoing packet.

Flag any of the above elements with *Inverted* to perform target action on packets not matching any criteria specified in that line. For example, if you select *DROP* as the target action, specify *Inverted* for a source IP address 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.

Numeric protocol options

If you select *Numeric* as the protocol when specifying a rule, you need to specify the desired number.

TCP protocol options

If you select *TCP* as the protocol when specifying a rule, you can define the following options.

Table 1.4: TCP Protocol Option Definitions

Field/Menu option	Definition
Source or Destination Port	Specify a source or destination port number for filtering. Specify a range to filter TCP packets for any port number within the range.
TCP Flags	Specify any of the flags: SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), URG (urgent), PSH (push) and one of the Any, Set, or Unset conditions to filter TCP packets for the specified flag and selected condition.

UDP protocol options

Select UDP options by selecting UDP as the protocol when selecting a rule. Choose either the Source or Destination Port from the field, as defined above.

ICMP protocol options

When you select ICMP as a protocol when specifying a rule, you can select the ICMP options available on the display.

Target actions

The Target is the action to be performed on an IP packet that matches all the criteria specified in a rule.

NOTE: If the *LOG* and *REJECT* targets are selected, additional options are available.

For detailed information on LOG target options, see *LOG target* on page 83.

For detailed information on REJECT target options, see *REJECT target* on page 84.

SNMP

The administrator can activate the Simple Network Management Protocol (SNMP) agent that resides on the console server so that the SNMP agent sends notifications about significant events or traps to an SNMP management application. The console server SNMP agent supports SNMP v1/v2 and v3.

For more information, see *To configure SNMP:* on page 78

Notifications, Alarms and Data Buffering

The administrator can set up logging, notifications and alarms to alert administrators of problems. System generated messages on the console server and the connected servers or devices can be sent to syslog servers for handling. The administrator can also configure data buffering to store data from communication on serial ports for monitoring.

Data from communication with serial-connected consoles can be stored locally in the console server's flash memory or remotely either on an NFS server or a syslog server.

Syslog servers

Messages about the console server and connected servers or devices can be sent to central logging servers, called syslog servers. Console data from devices connected to serial ports can be stored in data buffer files on syslog servers. By default, logging and data buffering are not enabled.

Prerequisites for logging to syslog servers

Before configuring syslogging, ensure the syslog server is pre-configured with a public IP address and is accessible from the console server. The system administrator must obtain both the IP address of the syslog server from the syslog server's administrator and the facility number for messages from the console server. Facility numbers are used on the syslog server for handling messages generated by multiple devices.

Facility numbers for syslog messages

Each syslog server has seven local facility numbers available for its administrator to assign to different devices or groups of devices, at different locations. The available facility numbers are local0 through local7.

Example of using facility numbers

The syslog system administrator sets up a server called syslogger to handle log messages from two console servers. One console server is located in São Paulo, Brazil and the other in Fremont, California. The syslog server's administrator wishes to aggregate messages from the

São Paulo console server into the local1 facility and to aggregate messages from Fremont console server into the local2 facility.

On syslogger the system administrator has configured the system logging utility to write messages from the local1 facility to the /var/log/saopaulo-config file and the messages from the local2 facility to the /var/log/fremont-config file. If you were in Fremont and identifying the syslog server using the web manager, according to this example, you would select the facility number local2 from the Facility Number pull-down menu on the Syslog form.

Managing Users of Connected Devices

This section provides a list of tasks that a console server administrator can perform to enable access to connected devices.

Configuring access to connected devices

During hardware installation of the console server, the installer connects the servers, devices and any IPDUs to the serial ports. During software configuration, the console server administrator performs the common tasks listed in the following table.

Table 1.5: Common Administrator Tasks for Configuring Software

Task	Where Documented
To Configure a Serial Port Connection Protocol for a Console Connection	*To configure a serial port connection protocol for a console connection:* on page 107
To Configure User Access to Serial Ports	*To configure user access to serial ports:* on page 112

Console Server and Power Management

Authorized users can turn on, turn off and reboot (turn off and turn on) devices that are plugged into one of the following types of power devices, which can be optionally connected to any of the serial ports:

- Avocent PM Power Distribution Units (PM PDUs) - With Avocent PM PDUs, up to 128 PDU outlets can be daisy-chained from a single serial port.

- Cyclades PM Intelligent Power Distribution Units (IPDUs) - With Cyclades PM IPDUs, up to 128 IPDU outlets can be daisy-chained from a single serial port.

- Avocent SPC power control devices.

- Server Technology Sentry™ family of Switched Cabinet Power Distribution Units (CDUs) and switched CDU Expansion Module (CW/CX) power devices.

- Server Technology Sentry Power Tower XL™ (PTXL) and Power Tower Expansion Module (PTXM) power devices.

- Server Technology Sentry Smart CDU (CS) and smart CDU Expansion Module power devices with version 6.0g or later.

NOTE: The term PDU is used to refer to any of these types of power devices.

The console server automatically recognizes and supports a Cyclades PM IPDU or Avocent SPC device when the serial port to which the power device is connected has been configured for power management.

Additional requirements for Server Technology IPDUs

For supported Server Technology IPDUs the following additional requirements apply:

- The console server must be managed by a DSView 3 server (DSView 3 software version 3.4.1 or above).

- The needed power device license must be present, and the power device must be added to the DSView 3 software.

The license is automatically downloaded from the DSView 3 server onto the console server. Configuration and management can then be performed either through the DSView 3 software or through the web manager.

Conventions used to identify outlets

Several formats (such as outlet names, outlet groups, IPDU IDs and port names) can be used to identify outlets during configuration, as described below:

- An administrator can configure optional names for each outlet to replace the default names assigned by the system. Outlet names must begin with a letter. Valid characters are letters, numbers, dash (-) and underscore (_). When an outlet name is configured, the name can be used in other power management configurations.

- An administrator can configure outlet groups. Once defined, outlet groups are specified with the dollar sign ($) prefix followed by the outlet group name: $outlet_groupname. For example, $Cyclades_IPDU specifies an outlets group called Cyclades_IPDU.

- An administrator can specify outlets in any of the following ways:

    - With a name that was configured for the outlet

    - With an outlet group name preceded by the $ suffix

- With the IPDU ID assigned to the IPDU

- With the port number to which the IPDU is connected

The IPDU and port number are always followed by one or more outlet numbers in brackets: [outlets]. Commas between outlet numbers indicate multiple outlets. Hyphens indicate a range. For example, [1,5-8] specifies outlets 1, 5, 6, 7 and 8.

- IPDU ID - An IPDU ID is automatically assigned to each IPDU when the port to which it is connected is configured for power management. An administrator can optionally assign a name to each IPDU. Both automatically assigned and administrator-assigned names are referred to as IPDU IDs.

  - Specify outlets with the IPDU ID in the following format: IPDU_ID[outlets]. For example, ilA[4,5] specifies outlets 4 and 5 on an IPDU whose ID is ilA.

  - When devices are plugged into more than one IPDU, you can separate multiple IPDU entries with commas in the form IPDU_ID[outlets],IPDU_ID[outlets]. For example, i1A[1,5],i1B[2] specifies two outlets on IPDU i1A and one outlet on a daisy-chained IPDU whose IPDU ID is ilB.

- Port number - To specify outlets by the port number to which the IPDU is connected, use the suffix !ttyS followed by the port number followed by [outlets]. For example, !ttyS2[16] indicates outlet 16 on an IPDU that is connected to serial port 2.

  You can specify outlets in a chain of IPDUs with the port ID two different ways:

  - By the outlet sequence. For example, in !ttyS3[2,16], outlet number 2 is the second outlet on the first IPDU in a chain that is connected to port 3. If the first IPDU has 10 outlets, outlet number 16 would be the sixth outlet on the second IPDU.

  - By IPDU sequence, identified with alphabetic characters. The first IPDU is A and the second is B and so forth. Precede the character with a hyphen. For example, !ttyS3-B[6] would also refer to the sixth outlet on the second IPDU in the chain connected to port 3.

Configuring power management

Administrators commonly perform power management through the web manager to assign power management permissions to users, configure IPMI devices and configure ports for power management.

Configuring ports for power management by authorized users

Administrators of connected devices who have power management permissions can do power management while connected by using a hotkey that brings up a power management screen.

For IPMI power management, the default hotkey is **Ctrl+Shift+I**. For IPDU power management, the default hotkey is **Ctrl+p**.

Options for managing power

Authorized users can perform power management through the console server by using forms in the web manager, from a power management screen while logged into a device or from the command line while logged into the console server.

An authorized user with administrative privileges can perform IPDU and IPMI power management. A regular user with permissions to the connected devices can perform IPDU power management.

Power management through the web manager

Users with power management permissions can perform power management through the web manager. The web manager menu includes two power management options, both discussed in Chapter 6.

Power management from the console server command line interface (CLI)

Console server administrators can use the **ipmitool** command to manage power on IPMI devices while logged into the console server with administrative rights. The **ipmitool** command is documented in the Cyclades ACS 5000 Command Reference Guide.

Hostname Discovery

An administrator can configure hostname discovery on the console server. When hostname discovery is enabled for a serial port, the console server attempts to discover the hostname of the server connected to the port. If the hostname of a server is successfully discovered, the hostname of the device connected to it is shown as the serial port alias.

If the server is later moved to another port, and the new port is also configured for hostname discovery, the hostname for the server is again discovered at the new serial port.

NOTE: If the console server is being managed through DSView 3 software, hostname discovery can be configured through the DSView 3 software.

An administrator can also configure site-specific probe and answer strings. These strings are used to probe the target device that is connected to the selected serial port and extract the hostname from the answer that is received in response to the probe string. The result of each probe string is matched against all answer strings. If no match is found, the next probe string is sent until there are no more probe strings or a match occurs. The default strings have a broad range and work in most cases.

NOTE: Probe string configuration requires knowledge of C-style escape sequences. Answer strings require knowledge of POSIX extended regular expressions. Hostnames longer than 31 characters are truncated when the hostname is assigned to the serial port alias.

CHAPTER 2

Installation

Important Pre-installation Requirements

Before installing and configuring the console server, ensure 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 internet browser that supports the console server web manager.

- Java 2 Runtime Environment (JRE) version 1.4.2 or later.

Basic Installation Procedures

Mounting the console server

You can mount the 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.
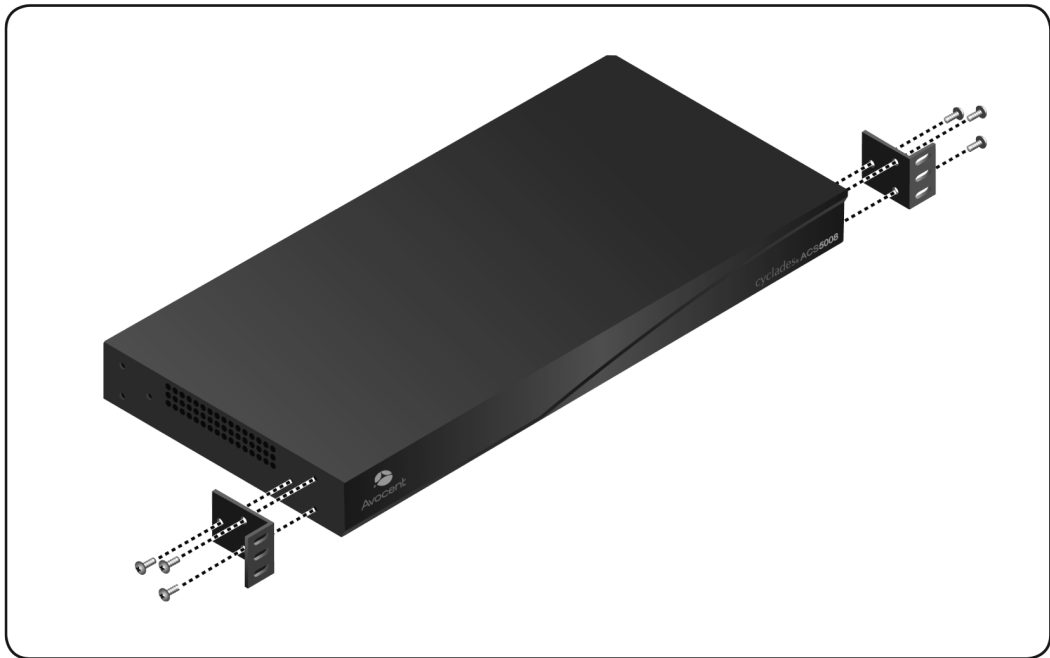
Figure 2.1: Placement of Mounting Brackets

To rack mount the console server:

1. Install the brackets on to the front or back edges of the console server using a screwdriver and the screws provided with the mounting kit.

2. Mount the console server in a secure position.

Making an Ethernet connection

Connect a CAT5 patch cable from the console server port labeled 10/100Base-T 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.

On your Microsoft® Windows workstation, ensure that a terminal emulation program is installed. 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 in 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 port labeled Console 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 pin-out information

The following table provides the serial port pin-out information for the console server.

Table 2.1: ACS 5000 Console Server Serial Port Pin-out

Pin No.	Signal Name	Input/Output
1	RTS	OUT
2	DTR	OUT
3	TxD	OUT
4	GND	N/A
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 avoid problems with components on 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.

NOTE: If your console server is equipped with dual-power supplies, make sure you turn both power switches on. After system initialization, a beep sound may warn if one of the power supplies is off.

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**.

```
ACS 5000 console server login: root
Password: avocent
```

WARNING: For security reasons, it is recommended that you change the default password for root (**avocent**) and admin (**avocent**) as soon as possible. To change the default password of a root user, enter the **passwd** command at the prompt and enter a new password when prompted. To change the default password of an admin user, enter **passwd admin** at the prompt and enter a new password when prompted.

NOTE: The Security Advisory appears the first time the 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 below, the system displays the configuration wizard banner and begins running the wizard.

```
************************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
************************************************************
INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system
and press ENTER or
2) Press ENTER if you are satisfied with the value
within the brackets [ ] and want to go on to the
next parameter or
3) Press ESC if you want to exit.
NOTE: For some parameters, if there is nothing within
the brackets, it will continue to ask for a value.
In that case, you must enter a valid value or # if you
do not wish to configure the value.
Press ENTER to continue...
```

2. At the prompt, press **Enter** to view the default settings.

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

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

4. Press **Enter** to accept the default hostname, or enter your own hostname and then press **Enter**.

   ```
   Hostname [CAS]: <hostname server name>
   ```

5. The IP version Configuration form is displayed. Select the IP version you wish to run and press **Enter**. Choices are IPv4 enabled (**0**), IPv6 enabled (**1**) or Dual Stack (**2**).

NOTE: Depending on which IP configuration you choose, the wizard will direct you to the appropriate form.

To configure for IPv4 protocol:

1. If you have typed **0** or **2** for IP version configuration, the IPv4 Configuration form will appear and give you the choice to use DHCP to assign an IP address for your system. Default is **Y**.

2. Press **Enter** to keep DHCP enabled or type **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, the 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] :
   ```

NOTE: If you choose to use DHCP and have selected IPv4 enabled (option **0**), the IPv4 Current Configuration verification screen will be displayed as shown below.

```
*************************************************************
*********** C O N F I G U R A T I O N  W I Z A R D ***********
*************************************************************
Current configuration:
Hostname : Rogreto
Domain name : corp.company.com
Primary DNS Server : 172.26.29.4
Second DNS Server : #
IPv4 Configuration:
DHCP : enabled
IPv6 Configuration: Disable
Are all these parameters correct? (y/n) [n] :
```

3. Verify that the configuration is correct and press **Enter**. You will be prompted to activate the configuration settings.

4. If you typed **n** to change the default static IP address, enter a valid IPv4 system address.

   ```
   System IP[192.168.160.10]: <ACS_5000_console_server_IP_address>
   ```

5. Press **Enter**. Enter the IP address for the gateway.

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

6. Press **Enter**. Enter the netmask for the subnetwork.

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

7. Press **Enter**.

NOTE: If you have selected IPv4 enabled and have set the static IP, gateway and netmask addresses, the IPv4 Current Configuration verification screen will be displayed. Check all parameters and press **Enter.** You will be prompted to activate the configuration settings.

To configure for IPv6 protocol:

1. If you entered option **1** or **2** for IP version configuration, the IPv6 Configuration Method form will be displayed.

2. Choices for IPv6 configuration are Stateless Only (**0**), Static (**1**) or DHCP (**2**). The default is Stateless Only. Type the number corresponding to your choice and press **Enter**. The choice you enter selects the method used to assign the IPv6 system address.

- Stateless Only: The router will multicast the IPv6 prefix along with the console server's MAC address, then listen for the other devices on the local network to allow the router to assign the IPv6 address.

- Static: You must manually assign a unique IPv6 address for the console server.

- DHCP: The router will request the IPv6 address from the DHCPv6 server.

3. The DHCPv6 options form is displayed. Choices are None (**0**), DNS (**1**), Domain (**2**) and DNS and Domain (**3**). Type the number corresponding to your choice and press **Enter**.

- From None (**0**): Enter your domain name.

- From Domain (**1**): Enter your domain name.

- From DNS (**2**): Follow the on-screen instructions.

- From DNS (**3**): The Current Configuration screen is displayed.

4. If None (**0**) or Domain (**1**), enter your domain name.

   ```
   Domain name[corp.avocent.com] :
   ```

5. Enter the IPv4 or IPv6 address for the Primary DNS (domain name) server.

   ```
   Primary DNS Server[172.26.29.4] : <DNS_server_IPv4_or_IPv6_address>
   ```

6. Press **Enter**. The Current Configurations screen appears. If correct, 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
   ```

7. To confirm the configuration, enter the **ifconfig** command.

8. After the initial configuration, proceed to the web manager to select a security profile as described in the following section.

NOTE: To use the web manager, obtain your console server's IP address. The console server may be set up with a static IP address at your site. By default, the console server uses the IP address provided by the DHCP server. If your network does not use DHCP, then the console server defaults to 192.168.160.10.

Selecting a security profile using the web manager

After the initial configuration, connect to the web manager by entering the IP address of the console server in a supported browser.

NOTE: Once you log in to the web manager, a security profile must be selected to further configure the console server using the web manager. For this reason your browser redirects to Wizard - Step1: Security Profiles.

Selecting a security profile

Select a pre-defined security profile or define a custom profile for specific services. The profiles are:

- Secured - Disables all protocols except sshv2, HTTPS and SSH to serial ports.
- Moderate - Enables sshv1, sshv2, HTTP, HTTPS, Telnet, SSH and Raw connections to serial ports, ICMP and HTTP redirection to HTTPS.
- Open - Enables Telnet, sshv1, sshv2, HTTP, HTTPS, SNMP, RPC, ICMP, SSH and Raw connections to serial ports.
- Default - Sets the profile to the same configuration as Moderate profile.
- Custom - Allows custom configuration of individual protocols and services.

For detailed information on security profiles, see *Security Profiles* on page 98.

The administrator can perform the following tasks using the web manager.

- Administer the console server and its connected devices.
- Configure user and group permissions.
- Access the serial ports and the connected devices.

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 89 and *Ports Menu and Forms* on page 103

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. Turn on 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 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, http://192.168.160.10, to bring up the web manager and log in.

Connecting PDUs

You can connect Avocent PM PDUs and Cyclades PM IPDUs to the serial ports on the console server using an RJ-45 to RJ-45 UTP cable. Avocent PM PDUs and Cyclades IPDUs include two RS-232 outlets for serial management and daisy-chaining. Any combination of Avocent PM PDUs and/or Cyclades IPDUs up to 128 outlets can be daisy-chained into a single virtual power distribution unit.

The daisy chain can include Avocent PM PDUs and Cyclades IPDUS with the following restrictions:

•   Avocent PM PDUs should be the first in the daisy chain.

•   All Cyclades IPDUs should have firmware version 1.9.2 or later.

Connecting third-party IPDUs

IPDUs from SPC and ServerTech can be connected to and managed by the console server. Special cabling and an adaptor is required for this purpose. These cables and adaptors are available from Avocent, or you can build your own cable as needed. See *Console server serial port pin-out information* on page 17 for this purpose.

NOTE: ServerTech IPDU installation, management and operation is license-based through Avocent's DSView® 3 management software only.

To daisy-chain PDUs to the console server:

This procedure assumes that you have one Avocent PM PDU or Cyclades IPDU connected to a serial port on the console server.

NOTE: Daisy-chaining is not possible with SPC power control devices. ServerTech PDUs will allow only one level (Master and Slave) of daisy chaining.

1. Connect one end of a UTP cable with RJ-45 connectors to the OUT port of the PDU connected to the serial port on the console server.

2. Connect the other end of the cable to the IN port of the next PDU.

3. Repeat steps 1 and 2 until you have connected the desired number of PDUs. Only one additional level is allowed with ServerTech PDUs.

Contact Avocent Technical Support for more information on:

• Installing SPC devices and ServerTech PDUs

• Replacing an Avocent CCM console management appliance with a console server

• Cabling requirements for using the console server with SPC devices and ServerTech PDUs

CHAPTER 3

Web Manager for Regular Users

Using the Web Manager

Console server users perform most tasks through the web manager. The web manager runs in a browser and provides a real-time view of all equipment connected to the console server.

Authorized users can access devices connected to serial ports:

- If a device console is connected, the user can access the console of the target device.
- If a terminal is connected, the user can connect from the terminal to the console server and access other servers.
- If a modem is connected, a user can dial in and access the console server and connected devices.
- If an IPDU is connected, a user can manage power for devices connected to the outlets of the IPDU.

To log into the web manager:

1. Type the console server's IP address in your browser's address field.

NOTE: Refer to Chapter 2 for requirements to start the web manager.

2. Press **Enter**. The web manager Login form is displayed.
3. Enter your username and password.

Features of Regular User Forms

The following figure shows features of the web manager when a regular user logs in.
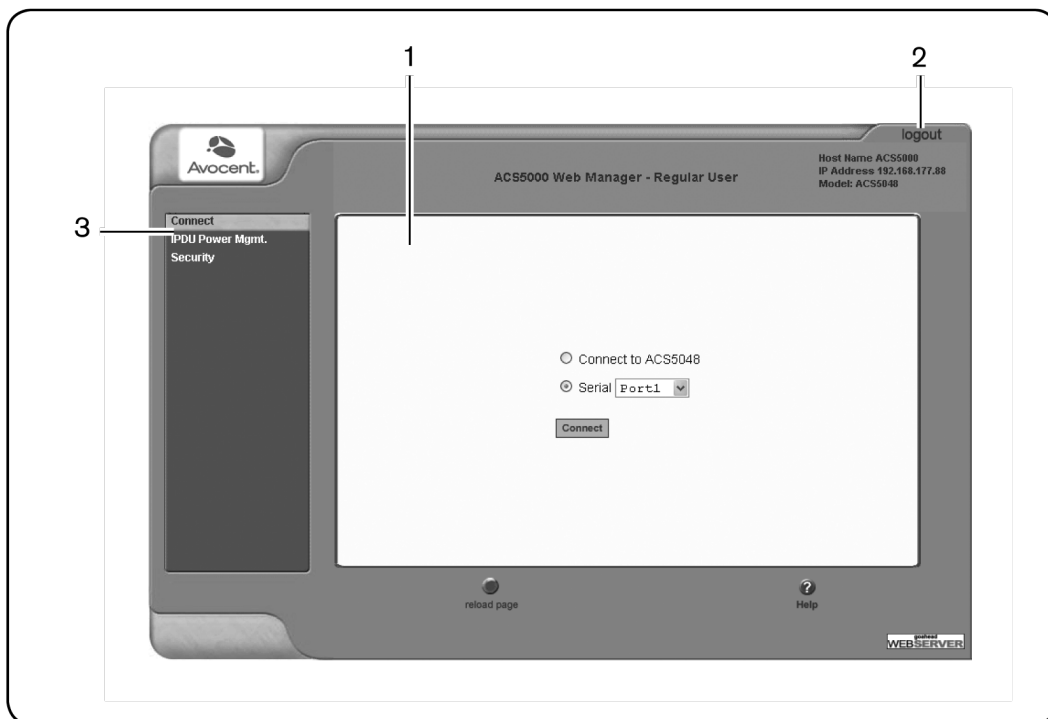
Figure 3.1: Regular User Form

NOTE: The form area changes according to which menu option is selected.

Table 3.1: Description of Regular User Web Interface

Number	Description
1	Form area.
2	Console server information area and logout button. This area contains the following information: logout button - Press logout to exit the current session. The login screen is displayed. Host Name - Displays the console server's hostname selected by the administrator. IP Address - Displays the console server's current IP address. Model - The model number of the console server.
3	Side navigation menu. Select one of the options to change the content in the form area. For regular users, the choices are Connect, IPDU Power Mgmt. and Security.

Connect

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

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

Connect to the console server

When you click the *Connect to ACS 5000* radio button on the Connect form, a Java applet viewer appears running an SSH session on the console server. A Java applet displays when you connect to the console server. The IP address of the console server is followed by the session type.

The following table describes the available buttons in the Java applet:

Table 3.2: Java Applet Buttons

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 the 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 in a gray area 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. The following table shows the protocols available for the serial ports.

Table 3.3: 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
Other	Power Management, Bi-directional Telnet

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.

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

For this procedure, you need the username configured to access the serial port, the TCP port number and the hostname of the console server or its IP address.

• To use SSH in a shell, enter the following command:

```
SSH - # ssh -l username:TCP_port_number <console_server_IP_address|or
the hostname>
```

To close an SSH session:

Enter the hotkey defined for the SSH client followed by a period. The default is **~**.

NOTE: Make sure you enter the escape character followed by a period at the beginning of a line to close the SSH session.

IPDU Power Management

IPDU management allows you to manage the power outlets on power management appliance products. If you have permission to manage outlets on a power management appliance, selecting the *IPDU Power Mgmt.* option will display a form with two tabs, Outlets Manager and View IPDUs Info.

Access the forms under IPDU Power Mgmt. menu to manage outlets or view IPDU information.

Outlets Manager

When you select *IPDU Power Mgmt. - Outlets Manager*, an error message appears either if you do not have permission to manage power on any of the IPDU outlets or the console server cannot detect an IPDU that has been configured for power management.

If you have permission to manage power on one or more outlets of the power management appliance, the Outlets Manager form is displayed.

The form shows separate entries for each serial port configured for power management, a name for the configured serial port if one is defined by the administrator and the number of IPDUs connected. The matrix displays a line item for each outlet you are authorized to manage.

The authorized user can perform the following for any listed outlet:

- Edit the outlet name. Enter a name to identify the server or device plugged into the outlet.

- Cycle. Turn power briefly off and on again.

- Turn the power On/Off to the outlet.

- Lock or unlock the outlet to prevent accidental changes to the power state (available for Avocent PM PDUs and for Cyclades IPDUs).

- Edit the post-on delay. The post-on delay is the time interval (in seconds) the system waits between turning on the currently-selected outlet and the next outlet. The default is set at 0.5 seconds (available for Avocent PM PDUs, Cyclades IPDUs and ServerTech PDUs).

- Edit minimum on time and minimum off time. This is the minimum time the outlet should be on or off before changing the state to off or on (available for Avocent SPC devices).

- Edit the wake state. The wake state is the outlet state when the PDU is turned on (available for Avocent SPC devices and for ServerTech PDUs).

- Edit post-off delay. The post-off delay is the delay (in seconds) the system waits between turning off the currently-selected outlet and the next outlet (available for some models of Avocent PM PDUs).

- Edit current thresholds - high critical, high warning, low warning and low critical (available for some models of Avocent PM PDUs).

The following table describes the corresponding buttons to perform the previous operations.

Table 3.4: Regular User - Outlet Management Buttons

Button or icon	Purpose
Edit	Lets you edit an outlet name and the turn-on interval.
Cycle	Turn power briefly off and then on again.
Bulb	
Lighted (yellow)	Power is on. Click to turn power off to that outlet.
Unlit (gray) bulb	Turn power off.
Padlock	
Locked	Outlet is locked. Click to unlock the outlet.
Unlocked	Outlet is unlocked. Click to lock the outlet.

Outlets Group Ctrl

Select *IPDU Power Mgmt. - Outlet Groups Ctrl* to display the Group Name Outlets page.

If a user has been authorized to control specific outlet groups assigned by an administrator, any group names are displayed under Group Name Outlets. In this mode, the user can turn on, turn off, lock, or cycle the outlets in the group all at once using the controls under Group Ctrl (Ipdu and Ports).

NOTE: The Lock button can only be used with Avocent PM PDUs and Cyclades IPDUs.

View IPDU info

Select *IPDU Power Mgmt. - View IPDUs Info* to display the Power Management Information page.

The following information is displayed for each port configured for power management.

Table 3.5: Power Management Display Information by Detected IPDU

Form Heading	Description	Example
ID	Either a default name or administrator-configured ID.	i1A

Form Heading	Description	Example
Model	IPDU model number.	Avocent Cyclades PM20i/30A PDU
Number of Outlets	IPDU number of outlets.	20
Number of Banks	IPDU number of banks/circuits.	2
Single-Phase/3-Phase	IPDU number of phases.	Single-Phase
Software Version	IPDU firmware version.	1.9.2
PDU Current	IPDU current level in amperes.	0.0
PDU Voltage	The nominal input voltage feeding the power device in volts.	210
PDU Power Consumption	IPDU power consumption in watts.	0.0
PDU Power Factor	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.	1.0
Bank Information		
Bank (Name)	Name of the bank.	A
Current	Bank current level in amperes.	0.0
Voltage	Bank voltage in volts.	119 V
Power Consumption	Bank power consumption in watts.	0.0 A
Power Factor	Bank power factor.	0.00
Phase Information		
Phase (Name)	Name of the phase.	N/A
Current	Phase current level in amperes.	N/A
Voltage	Phase voltage in volts.	N/A
Power Consumption	Phase power consumption in watts.	N/A
Power Factor	Phase power factor.	N/A
Environmental Sensors Information		

Form Heading	Description	Example
Type (Name)	Type of the sensor.	Temperature-Internal

Current information displays the actual alarm state of the current level based on the configured thresholds when available. The alarm state can have one of the following values:

- Tripped - when hardware overcurrent protection is tripped
- High Critical - when the value is greater than the high critical threshold
- High Warning - when the value is greater than the high warning threshold and less than the high critical threshold
- Low Warning - when the value is greater than the low critical threshold and less than the low warning threshold
- Low Critical - when the value is less than the low critical threshold

Voltage, Power Factor and Power Consumption display either the Estimated or Measured value.

NOTE: Some power devices do not have the capability to read the real input voltage/power factor using proper voltage/power factor sensors; in this case the values are configurable.

When recorded maximum value is provided by the PDU, it is shown in the same row of the actual value.

Security

Use the following procedure to set or change your password.

To change your password:

1. Select the *Security* option from the menu panel.
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.

CHAPTER 4

Web Manager for Administrators

This chapter is for system administrators who use the web manager to configure the 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 ACS 5000 Command Reference Guide.

The console server's web manager for administrators describes two modes of operation, Wizard and Expert.

This section provides an overview of the web manager forms. Subsequent sections describe the menus, forms and the configuration procedures of the web manager in Wizard and Expert modes. If you are a regular user, see *Web Manager for Regular Users* on page 25.

Common Features of Administrator Forms

The following figure shows the control buttons displayed at the bottom of the form when logged into the web manager as an administrator.
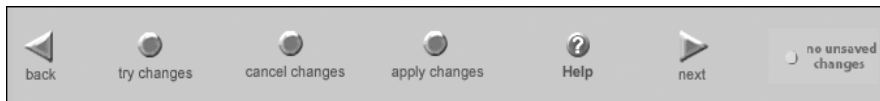
Figure 4.1: Administrator - Web Manager Buttons

The following table describes the uses for each control button.

Table 4.1: Description of Administrator Web Manager Buttons

Button name	Use
back	Only appears in Wizard mode. Returns the previous form.
try changes	Tests the changes entered on the current form without saving them.
cancel changes	Cancels all unsaved changes.
apply changes	Applies and saves all unsaved changes.

Button name	Use
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 various web manager actions for trying, saving and restoring configuration changes are summarized in the following table.

Table 4.2: Administrator - Options for Trying, Saving and Restoring Configuration Change

Task	Action	Result
try changes	Click the *try changes* button	Updates the appropriate configuration files. Changes are preserved if you log in and log out and even if you restart the system. Changes stay in effect unless the cancel changes button is clicked. The changes can be restored at any time until the apply changes button is clicked.
cancel changes	Click the *cancel changes* button	Restores the configuration files from the backup that was created the last time changes were applied.
apply changes	Click the *apply changes* button	If try changes has not been previously clicked, updates the appropriate configuration files. Overwrites the backed up copy of the configuration files.

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

Table 4.3: Administrator - Logout Button and Other Information in the Upper Right

Form Area Button and Information	Purpose
logout	Click this button to log out.
Host Name: Cyclades IP Address: 192.168.48.11 Model: ACS5016	Displays the hostname, IP address assigned during initial configuration and the model number of the 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 log in to the console server.

To log into the web manager:

1. Enter the IP address of the console server in the address field of your browser.

NOTE: The 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 and admin 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*.

NOTE: Be sure to read the security advisory message that appears on the screen. Your pop-up blocker must be disabled for the security advisory to appear.

Overview of Administrative Modes

The web manager operates in one of two modes, Wizard or Expert.

NOTE: If you select *Wizard*, the mode button will read Expert. If you select *Expert*, the mode button will read Wizard.

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, by default the system point to Expert Mode-Ports-Ports Status form.

The following is a typical form of the web interface in Wizard Mode. The user entry form varies depending on the selected menu item.
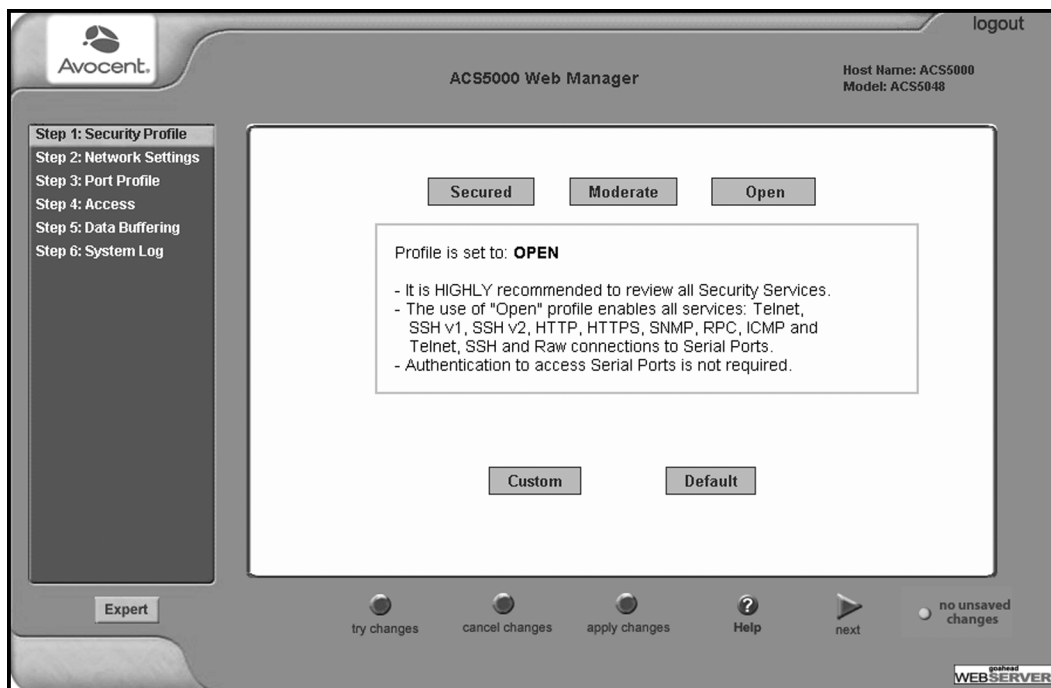
Figure 4.2: Example of Web Manager Form in Wizard Mode

Expert mode

Expert is the default mode when logging in to the 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. Occasionally, an Expert mode menu selection has multiple forms identified by tabs as shown in Figure 4.3.

Figure 4.3: Example of Web Manager Form in Expert Mode

Configuring the Console Server in Wizard Mode

Step 1: Security Profile

A security profile consists of a set of parameters that can be configured in order to have more control over the services active at any time.

Pre-defined security profiles

There are three pre-defined security profiles:

• Secure - Authentication to access serial ports is required and SSH root access is not allowed.

NOTE: SSH root access is enabled when the security profile is set to Moderate or Open. If a Secured security profile is selected, you must switch to a Custom security profile and enable the *allow root access* option.

• Moderate - The Moderate profile is the recommended security level. This profile enables sshv1, sshv2, HTTP, HTTPS, Telnet, SSH and Raw connections to the serial ports. In addition, ICMP and HTTP redirection to HTTPS are enabled. Authentication to access the serial ports is not required.

• Open - The Open profile enables all services such as Telnet, sshv1, sshv2, HTTP, HTTPS, SNMP, RPC, ICMP, SSH and Raw connections to the serial ports. Authentication to access serial ports is not required.

Default security profile

See the following tables for the list of enabled services when the Default security profile is used.

Custom security profile

The Custom security profile opens up a dialog box to allow custom configuration of individual protocols or services.

NOTE: By default, a number of protocols and services are enabled in the Custom profile; however, they are configurable to a user's requirements.

The following tables illustrate the properties for each of the security profiles. The enabled services in each profile are designated.

Table 5.1: Enabled Protocols to Access the Appliance for Each Security Profile

Access to console server	Secure	Moderate	Open	Default
Telnet			Yes	
sshv1		Yes	Yes	Yes
sshv2	Yes	Yes	Yes	Yes
Allow SSH root access		Yes	Yes	Yes
HTTP		Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes
HTTP redirection to HTTPS		Yes		Yes

Table 5.2: Wizard - Serial Port Enabled Services for Each Security Profile

Access to Serial Ports	Secure	Moderate	Open	Default
Console (Telnet)		Yes	Yes	Yes
Console (ssh)	Yes	Yes	Yes	Yes
Console (Raw)		Yes	Yes	Yes
Serial Port Authentication	Yes			
Bidirect (Dynamic Mode Support)		Yes	Yes	Yes

Table 5.3: Wizard - Enabled Services for Each Security Profile

Other Services	Secure	Moderate	Open	Default
SNMP			Yes	
RPC			Yes	
ICMP		Yes	Yes	Yes
FTP				
IPSec				

The first step to configure your console server is to select a security profile. One of the following situations is applicable when you boot the console server.

- The console server is starting for the first time or after a reset to factory default. In this situation when you boot the console server and log in as an administrator to the web manager, a security warning dialog box appears. The web manager is redirected to Step 1: Security Profile in the Wizard mode. Further navigation to other sections of the web manager is not possible without selecting or configuring a security profile. Once you select or configure a security profile and apply the changes, the web manager restarts for the security configuration to take effect.

- The console server firmware is upgraded and the system is restarting with the new firmware. In this situation the console server was already in use and certain configuration parameters were saved in the Flash memory. In this case the console server automatically retrieves the Custom Security Profile parameters saved in the Flash memory and behaves as it was a normal reboot.

- The console server is restarting normally. In this situation, the console server detects the pre-defined security profile. You can continue working in the web manager.

Serial port settings and security profiles

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

If you reconfigure the security profile and restart the web manager, make sure the serial ports protocols and access methods match the selected security profile. A reminder dialog box will appear before you can proceed to Step 2: Network Settings.

To select or configure a security profile:

The following procedure assumes you have installed a new console server or you have reset the unit to factory default.

1. Enter the assigned IP address of the console server in your browser and login as an administrator.

2. Review the security advisory and click the *Close* button.

NOTE: Your browser's pop-up blocker must be disabled to see the advisory.

---

3. The web manager is automatically redirected to Wizard - Step 1: Security Profile.

4. Select a pre-defined security profile by pressing one of the *Secure, Moderate, Open* or *Default* profiles or create a custom profile.

CAUTION: Take the required precautions to understand the potential impacts of each individual service configured under the Custom profile.

NOTE: It is not possible to continue working in the web manager without selecting a security profile. A reminder dialog box will appear if you attempt to navigate to other sections of the web manager.

5. Once you select a security profile or configure a custom profile and apply the changes, the web manager must restart for the changes to take effect. A reminder dialog box is displayed. Click *OK* to continue.

6. Select *apply changes* at the bottom of the web manager form to save the configuration to Flash.

7. Log in after web manager restarts and click on the *Wizard* button to switch to Wizard mode.

8. Proceed to Step 2: Network Settings.

Step 2: Network Settings

Selecting *Step 2: 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 current settings are correct.

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

To configure the network settings:

1. Select Step 2: 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 to use DHCP during initial setup.

2. If you are using Dual Stack with DHCP, proceed to Step 3: Port Profile; if not, select the mode and select/deselect DHCP and enter your network settings manually.

3. Enter the required network information.

4. Select *apply changes* to save configuration to Flash or continue the configuration.

5. Select the *Next* button or proceed to Step 3: Port Profile.

Step 3: Port Profile

Selecting *Step 3: 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.

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.

NOTE: All serial ports are disabled from the factory by default. The administrator can enable ports and assign specific users to individual ports through the Expert mode.

The following table lists the parameters with the available options and a brief description for each.

Table 5.4: 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.
Baud Rate (Kbps)	9600 [Default] Options range from 2400–230400 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.

Parameter	Options	Description
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+, LDAP, Kerberos or NIS go to Expert mode and select *Security - Authentication*.

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.

If the connected devices require different connection protocols and speed, configure individual settings in Expert mode - Ports - Physical Ports.

1. Change serial ports 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 or continue the configuration.

4. Select the *Next* button or proceed to the next section, Step 4: Access.

Step 4: Access

Selecting *Step 4: Access* 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.

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 table defines the information required in the fields.

Table 5.5: Wizard - Add User Dialog: Field Names and Definitions

Field name	Definition
User Name	The username for the account being added.
Password and Repeat Password	The password for the account.
Group	The choices in the Group menu are Regular User [Default] or Admin. **NOTE:** To configure a user to be able to perform administrative functions, select the Admin group.
Shell	Optional. The default shell when the user makes an SSH or a Telnet connection. Choices are: sh [Default] or bash.
Comments	Optional notes about the user's role or configuration.

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 username 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 menu.

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 username 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 and admin passwords 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 5: Data Buffering

Selecting *Step 5: 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 table provides description for each field whether local or remote destination is selected.

Table 5.6: 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 serial driver buffering 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. In linear mode, the serial driver buffering is used. Once the 4Kb of Rx buffer is reached, a flow control stop (depends on configured flow control for the serial port) is issued to prevent the serial port from receiving further data from the remote peer.
File Size (Bytes)	For Local Destination Circular Mode - 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.

The following table shows the differences between remote and local data buffering.

Table 5.7: Differences Beween Remote and Local Data Buffering

Option	Description
Remote server	Data is stored in files sequentially. The NFS server must be configured with the mount point shared (exported). 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.
Local files	Set a file size greater than zero. For circular mode, make sure the file size does not exceed the space available on the console server's RAM disk.

NOTE: You can perform advanced configuration in Expert mode including the option of setting up data buffering separately for individual or groups of serial ports.

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 step.

    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/acslogs, enter **/var/adm/acslogs** 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.

6. 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.

7. 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.

8. Click *apply changes* or continue the configuration.

Step 6: System Log

Selecting *Step 6: System Log* displays a form for identifying one or more syslog servers to receive syslog messages generated by the console server's serial ports. Syslogging for IPDUs is also possible if IPDU power management is configured.

NOTE: To configure syslog with data buffering features for specific ports, switch to the Expert mode, *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 IP address of the syslog server and the facility number for messages coming from the appliance.

To add a syslog server:

This procedure assumes you have the IP address of the syslog server and the facility number for messages coming from the console server.

1. Select *Step 6: 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*.

CHAPTER 6

Applications

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 6.1 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.
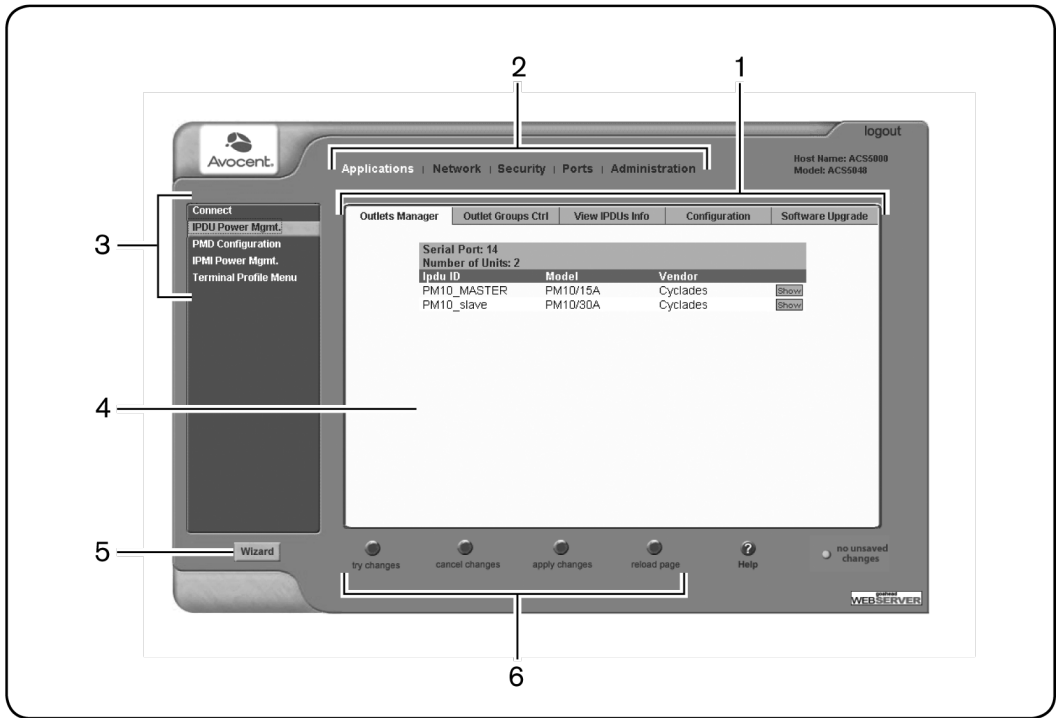
Figure 6.1: Expert Mode Screen Elements

Table 6.1: Expert Mode Screen Elements

Number	Description
1	Top menu. Selecting any one of the top menu items will change the left navigation menu and form areas to view status or configure the related console server options or parameters.
2	Left navigation menu. Selecting any of the left navigation menu items will change the information and options in the form area.
3	Wizard/Expert button. If you are in Expert mode, the button will say Wizard. If you are in Wizard mode, the button will say Expert. Select the button to display the other mode.
4	Tabs. Tabs are additional buttons that change the content of the form area related to the item you have selected in the left navigation menu. Tabs are displayed only with specific forms.
5	Form area. The form area contains the user - controlled text fields, checkboxes and pull-down menus for configuring the console server.

Number	Description
6	Command buttons. The command buttons are common to all web manager screens and are used to try changes, cancel changes, apply changes, reload pages or select the online help.
	NOTE: The unsaved changes / no unsaved changes indicator at the far right is green (no unsaved changes) when you have not made any changes that need to be saved, and flashes red (unsaved changes) when you have made changes but have not selected *Apply Changes*.

NOTE: Procedures in this manual use shortcuts to tell how to get to web manager forms. For example, a step telling the user to access the Outlets Manager form uses the following convention: In Expert mode, select *Applications-IPDU Power Mgmt.- Outlets Manager*.

Applications Menu and Forms

The remainder of this chapter describes the Applications menu and the related forms. The following table provides a description of the left menu panel and links to the detailed information and associated procedure. If you are in Wizard mode and need to perform advanced configuration, clicking the *Expert* button at the bottom of the left menu panel to switch the web manager to Expert mode.

Connect

Using the Connect form, you can connect directly to the console server or to devices connected to the serial ports.

Connecting to the console server

Clicking the *Connect to ACS 5000* radio button and then clicking on *Connect* displays a Java applet running an SSH session.

NOTE: SSH root access is enabled when the security profile is set to Moderate or Open. If a Secured security profile is selected, you need to switch to a Custom security profile and enable allow root access option.

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 username 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 ACS* 5000 radio button.

3. Click the *Connect* button. A Java applet viewer appears.

NOTE: The login prompt is displayed whenever your security profile is set to *Moderate* or *Open*; otherwise, an authentication form appears. You cannot authenticate unless you change the security profile to *Custom* and enable *allow root access*.

To connect to a device through a serial port:

1. Select *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.

IPDU Power Management

The console server recognizes and supports all Cyclades PM series IPDUs as well as Avocent PM PDUs, Avocent SPC power devices and ServerTech Switched/Smart CDU IPDUs through the common interface. The console server's PMD structure accommodates the differences in each of these IPDUs to allow more flexibility with power management options.

NOTE: ServerTech IPDU installation, management and operation is licensed based through Avocent's DSView 3 management software only.

Selecting *IPDU Power Mgmt.* displays five tabs in the form area, as follows:

• Outlets Manager

• Outlet Groups Ctrl

• View IPDUs Info

• Configuration

• Software Upgrade

NOTE: Using the IPDU power management forms, you can manage the power to connected devices only if the serial port where the devices are connected is configured for power management.

Applications - IPDU Power Mgmt - Outlets Manager

On the Outlets Manager form under Applications-IPDU Power Mgmt., you can perform the following tasks for all outlets on all connected IPDUs.

• Check the status of outlets

- Turn outlets on and off

- Cycle power

- Lock outlets to prevent accidental changes in power state (Avocent PM PDUs and Cyclades IPDUs only)

- Unlock the outlets (Avocent PM PDUs and Cyclades IPDUs only)

- Assign an alias to the outlet (to identify the device for which it provides power)

- Save the current configuration to Flash memory in the IPDU

- Edit the outlet configuration (post-on/off delay, minimum on time, wake-up state, current thresholds) (depends on the PDU vendor)

A list shows the port ID, IPDU ID, the model and vendor for IPDUs connected to ports that are configured for power management. The Show button shows details about a selected IPDU. For Avocent PM PDUs, the Outlet, Outlet Name, Outlet State, Current, Power and Alarm are displayed. For other PDUs, the Outlet Number, Outlet Name and Outlet State are displayed

The following table illustrates what each icon indicates

Table 6.2: Expert - Outlets Manager Icons Description

Button	Purpose
⚲ ⚲	Yellow bulbs indicate an outlet is switched ON. Gray bulbs indicate an outlet is switched OFF.
🔓 🔓	An opened padlock indicates that an outlet is unlocked. A closed padlock indicates that an outlet is locked.
Cycle	An orange Cycle button is active next to each outlet that is on.
Edit	Displays a dialog box to configure an Outlet Name and Post On Delay. Outlet names must begin with a letter. Valid characters are letters, numbers, dash (-) and underscore (_). The post on delay is the amount of time (in seconds) that elapses after the selected outlet is turned on before another outlet is turned on.

Clicking the *Edit* button displays the dialog box for specifying Outlet Name and Post On Delay [turn-on (PU) interval] for Cyclades IPDUs.

You can specify a name for the outlet, such as the server or device name and change the post on delay (turn-on interval).

NOTE: The turn-on interval is the amount of time (in seconds) that elapses after the selected outlet is turned on before another outlet can be turned on.

Avocent PM PDU information displayed

Avocent PM PDUs will display the Outlet Name, Post On Delay, Post Off Delay, Current High Critical Threshold, Current High Warning Threshold, Current Low Warning Threshold and Current Low Critical Threshold.

Third-party IPDU information displayed

SPC power devices will display the Outlet Name, Minimum On Time, Minimum Off Time and Wake State.

ServerTech IPDUs will display Outlet Name, Post On Delay and Wake State.

To view status, lock, unlock, rename or cycle power outlets:

NOTE: For a group of outlets, the Cycle button operates only if all outlets of the group are turned ON.

1. Select *Expert - Applications - IPDU Power Mgmt. - Outlets Manager*. The Outlets Manager screen appears with each IPDU listed.

2. Click the *Show* button associated with the IPDU whose outlets you want to manage. A list of outlets appears.

3. To switch an outlet (or an outlet group) on or off, click its light bulb icon.

NOTE: For Avocent SPC power devices or Server Technology IPDUs, an alert window prompts you that you may need to refresh your browser to view the change in the Outlets Manager. Click *OK* and continue.

4. To lock or unlock an outlet (or an outlet group), click its padlock icon.

NOTE: The outlet locking function is available on Avocent PM PDUs and Cyclades IPDUs only.

5. To cycle power to an outlet, click the adjacent *Cycle* button.

6. To change the outlet's name or other values for the outlet, click the adjacent *Edit* button. The Edit Outlet dialog box appears.

   a. To change the name assigned to the outlet, enter a new name in the Outlet Name field. Names must begin with a letter. Valid characters are letters, numbers, dash (-) and underscore (_).

   b. To change the outlet configuration, change the value in the field.

NOTE: An outlet name should not be changed if the new outlet name is used elsewhere.

7. Click *OK*.

8. Click the *Save Outlets State* button (saves outlet states to the IPDU only).

9. Click *apply changes*.

NOTE: For Avocent SPC power devices or Server Technology IPDUs, an alert window prompts you that the screen is automatically reloaded. Click *OK* and wait for confirmation that the page has been reloaded.

Applications - IPDU Power Mgmt. - Outlets Group Ctrl

An administrator can select *Expert - Applications - IPDU Power Mgmt. - Outlet Groups Ctrl* to view the status of outlet groups and turn power off and then on again for an entire group of outlets.

NOTE: Outlet groups can be defined under *PMD Configuration - Outlet Groups*.

The Cycle button only can be used to cycle the entire group of outlets when all the outlets are on.

The following table describes the information available from the Outlet Groups Ctrl form.

Table 6.3: Expert - Ouatlet Groups Ctrl Information

Form Heading	Description
Group Name: Outlets	IPDU Group name followed by the individual outlets belonging to that group.
Group Ctrl (IPDU and Port)	Group Ctrl shows status icons for defined group controls; (IPDU and Port) shown in parentheses are the IPDU ID number and the serial port to which it is connected on the console server. Status icons under the Group Ctrl heading are active.
Individual Status	Shows status icons (passive) for individual outlets within the group.

Applications - IPDU Power Mgmt. - View IPDUs Info

An administrator can select *Expert - Applications - IPDU Power Mgmt. - View IPDUs Info* to view information about each IPDU controlled by the console server.

The buttons to Clear/Reset Max values will be displayed when the IPDU has the max detected value for the sensor. Possible buttons:

- Clear Max Current - reset the maximum detected current value
- Clear Max Power - reset the maximum detected or estimated power consumption value
- Reset Max Env Sensors - reset the maximum detected value of environmental sensors (Temperature, Humidity, Air Flow)
- Reset HW OCP - reset the HW over current protection (valid only for Avocent PM PDUs)
- Reset Max Voltage - reset the maximum detected voltage value
- Reset Max Power Factor - reset the maximum detected power factor

Table 6.4: Expert - Applications - Ipdu Power Mgmt - View IPDUs Info Description

Form Heading	Description	Example
ID	Either a default name or administrator-configured ID.	i1A
Model	IPDU model number.	Avocent Cyclades PM20i/30A
Number of Outlets	IPDU number of outlets.	20
Number of Banks	IPDU number of banks/circuits.	2
Single-Phase/3-Phase	IPDU number of phases.	Single-Phase
Software Version	IPDU firmware version.	1.9.2
PDU Current	IPDU current level in amperes.	0.0
PDU Voltage	The nominal input voltage feeding the power device in volts.	210
PDU Power Consumption	IPDU power consumption in watts.	0.0
PDU Power Factor	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.	1.0
Bank Information		
Bank (Name)	Name of the bank.	A
Current	Bank current level in amperes.	0.0
Voltage	Bank voltage in volts.	120
Power Consumption	Bank power consumption in watts.	0.0
Power Factor	Bank power factor.	1.0
Phase Information		
Phase (Name)	Name of the phase.	N/A
Current	Phase current level in amperes.	N/A
Voltage	Phase voltage in volts.	N/A
Power Consumption	Phase power consumption in watts.	N/A

Form Heading	Description	Example
Power Factor	Phase power factor.	N/A
Environmental Sensors Information		
Type (Name)	Type of the sensor.	Temperature-Internal

Current information displays the actual alarm state of the current level based on the configured thresholds when available. The alarm state can have one of the following values:

- Tripped - when hardware overcurrent protection is tripped

- High Critical - when the value is greater than the high critical threshold

- High Warning - when the value is greater than the high warning threshold and less than the high critical threshold

- Low Warning - when the value is greater than the low critical threshold and less than the low warning threshold

- Low Critical - when the value is less than the low critical threshold

Voltage, Power Factor and Power Consumption display the Estimated or Measured value.

NOTE: Some power devices do not have the capability to read the real input voltage/power factor using proper voltage/power factor sensors; in this case the values are configurable.

When recorded maximum value is provided by the PDU, it is shown in the same row of the actual value.

To view and reset IPDU information:

1. Select *Applications - IPDU Power Mgmt. - View IPDUs Info*. The View IPDUs Info screen appears.

2. To clear the stored maximum values, click the *Clear* or *Reset* button.

Applications - IPDU Power Mgmt. - Configuration

An administrator can select *Expert - Applications - IPDU Power Mgmt. - Configuration* to configure each configured IPDU.

NOTE: The operating parameters may differ depending on the make and model of IPDU.

Table 6.5: IPDU Power Mgmt Configuration Description

Shown	Element Type	Description
ID:	Heading	Static heading shows current IPDU name and port assignment.
Model:	Heading	Shows the make and model of IPDU at the designated port.
ID	Text field	Enter whatever name you wish for this IPDU.
Polling Rate	Number field	Enter the polling time (how often the console server accesses the IPDU for updates) in milliseconds. Default is 30000ms.
Power Cycle Interval	Number field	Set the Power Cycle Interval in seconds. This interval is the time the PDU is turned off during a power cycle.
Enable Syslog	Checkbox	Click this checkbox to enable/disable syslog logging (Cyclades IPDUs only).
Enable Buzzer	Checkbox	Click this checkbox to enable/disable IPDU alarm buzzer (Cyclades IPDUs only).
Default Voltage	Number field	The nominal input voltage feeding the power device. **NOTE:** Some power devices do not have the capability to read the real input voltage using proper voltage sensors.
Power Factor	Number field	The ratio of the real power to the apparent power; a number between 0 and 1 that is frequently expressed as a percentage. Real power is the capacity of the circuit for performing work in a particular time. Apparent power is the product of the current and voltage of the circuit.
Display	Dropdown	Set up the display orientation: Normal/Current or Inverted/Current.
Display Cycle	Number field	Set the display cycle in seconds.
PDU Thresholds	Number field	Enter the current threshold for IPDU: High Critical, High Warning, Low Warning and Low Critical.
Software Overcurrent Protection	Checkbox	Set whether overcurrent protection is off or on. When it is on, exceeding the high critical threshold will prevent the PDU from turning on outlets until the problem is corrected.
Cold Start Delay	Number field	Enter the time in seconds a PDU waits to turn on outlets after the PDU receives power.
Banks thresholds	Number field	Enter for each bank the current threshold: High Critical, High Warning, Low Warning and Low Critical.

Shown	Element Type	Description
Phases thresholds	Number field	Enter for each phase the current threshold: High Critical, High Warning, Low Warning and Low Critical.
Environmental threshold	Number field	Enter the thresholds for each environmental sensor: High Critical, High Warning, Low Warning and Low Critical.

Applications - IPDU Power Mgmt. - Software Upgrade

An administrator can select *Expert - Applications - IPDU Power Mgmt. - Software Upgrade* to upgrade software (firmware) for Cyclades PM IPDUs only. The screen shows the currently installed software version on the selected IPDU. If a newer software version is available, you can download new software for your IPDU using the following procedure.

To download Cyclades IPDU software:

Use this procedure to download software from the Avocent website.

1. Type **http://www.avocent.com/web/en.nsf/Content/Cyclades_Download-PM** in your browser address field to open the Downloads page.

NOTE: Your web server must be in the same subnet as the console server.

2. Compare the displayed version number to the version shown in the Applications - IPDU Power Mgmt. - Software Upgrade screen.

3. If a newer firmware version is available, click the *Firmware* link associated with the appropriate version. The download starts.

4. After the download completes, copy the file into the /tmp folder and rename it with the filename pmfirmware.

To upgrade software on a Cyclades PM IPDU [Expert]:

1. Select *Power Mgmt. - Software Upgrade*. The Software Upgrade screen is displayed.

2. Click *Refresh*. If a /tmp/pmfirmware exists containing a more recent version of the PM firmware than the one currently installed, an Update button is displayed.

3. Click *Update*.

4. Click *apply changes*.

To upgrade software on non-Cyclades IPDUs:

Avocent SPC power devices are not user upgradable. For Server Technology IPDUs, upgrades must be done through a network port. Contact Server Technology support to check if new

software is available and for information on how to upgrade the device.

To upgrade software on a Avocent PM PDU:

1. Download the new firmware in /tmp directory.

2. Use the **pmfwupgrade** command to perform the upgrade. See the ACS 5000 Command Reference Guide for more detailed instructions.

Expert - Applications - PMD Configuration

When an administrator selects *Expert - Applications - PMD Configuration*, the following three tabs appear:

• General

• Outlet Groups

• Users Management

An administrator can use these tabs to configure the username and password for IPDUs, create groups and authorize users and groups to access specific outlets.

To find the IPDU ID [Expert]:

1. Select *Expert - Access - IPDU Power Management - View IPDUs Info*.

2. Note the string in the ID field.

Applications - PMD Configuration- General

An administrator can select *Expert - Applications - PMD Configuration - General* to configure a username and password for each supported IPDU type. The fields are labeled: Cyclades (for Avocent PM PDUs and Cyclades PM IPDUs), SPC (for Avocent SPC power devices) and Server Tech (for supported Server Technology IPDUs). The username and password are used to authenticate communication between the console server and the IPDU. If the IPDU username and password are changed in the IPDU firmware, the username and password must be changed in this screen so the console server can use the correct username and password to communicate with the IPDU.

Applications - PMD Configuration- Outlet Groups

An administrator can select *Expert - Applications - PMD Configuration - Outlet Groups* to configure outlet groups.

Any configured outlet groups are listed in the Group column, followed by the string used to identify the group during configuration (in the form IPDU_ID[outlets] as shown). The Add, Edit and Delete buttons are used to configure the outlet groups.

Specify groups of outlets using the following format:

```
IPDU_ID[outlets]
```

Where IPDU_ID is the name configured for the IPDU (such as ilA) and outlets are numbers separated with commas or with dashes (to indicate a range), as in the following example:

```
ilA[1,2,5-15]
```

You can assign outlets from more than one IPDU to a group by using commas to separate them. The following example defines an outlet group for two IPDUs, one named ilA and the other ilB:

```
ilA[1,5-8],ilB[1,3,4]
```

For more information, see *Conventions used to identify outlets* on page 11. See also *Applications - PMD Configuration- General* on page 62 to find out the IPDU ID.

To configure an outlet group:

1. Click the *Add* button. The Add/Edit Outlet Groups dialog box appears.

2. In the Group field, enter the name of the group you want to add or edit the existing name.

3. In the Outlets field, add the IPDU ID followed by the specific outlets to assign to the group in brackets. For example, i1A[1,5-8] creates a group of outlets numbered 1, 5, 6, 7 and 8 on IPDU ID ilA. You can assign more than one IPDU to the group, with a comma between each IPDU.

4. Click *OK*.

To delete an outlet group:

1. Click the *Delete* button.

2. Select the group name you want to delete.

3. Click *OK*.

Applications - PMD Configuration - Users Management

An administrator can select *Expert - Applications* - PMD Configuration - *Users Management* to configure users to access outlets.

The listed users are authorized to access and control the outlets specified under the Outlets heading.

To authorize a user for IPDU power management:

1. Select *Expert - Applications - PMD Configuration - Users Management*.

2. Click *Add*. The Add/Edit PM Users dialog box appears.

3. In the User field, enter the username.

4. In the Outlets field, enter the group name, IPDU number and outlets that the user can control.

5. Click *OK*.

Outlet entry conventions

In the most basic case, only the IPDU's ID and the outlets named in brackets following the ID are needed to specify which outlets will be accessible by the user. It is sometimes desirable to have more control over outlet groups, daisy-chained IPDUs or which serial port on the console server must be used for the permissions to be valid. The following table shows the prefix, suffix and syntax information used to specify outlets in various circumstances.

Table 6.6: Conventions Used in Specifying Outlets for User Accessibility

Symbol	Type	Signifies	Example
$	Prefix	Group	**$Cyclades_PDU** would specify the Cyclades_PDU outlets group, and that the user specified has permission to control that group of outlets.
!ttyS	Prefix	Serial port	**!ttyS2** would specify serial port 2 on the console server would be the only one the user would have permissions to use for IPDU management, regardless of the IPDU or outlets specified.
A through Z	Suffix	Order of IPDU in daisy-chain	**!ttyS2-B[1-8]** would indicate that serial port 2 on the console server would be used to control the second IPDU in the chain (B), followed by the outlet or range of outlets on that IPDU with user permissions.

NOTE: Daisy-chained IPDUs (A, B, C, etc.) create sequentially numbered outlets across IPDUs.

The following figure shows two daisy-chained (master/slave) IPDUs connected to serial port 2 on the console server.

Figure 6.2: Various Outlet Designations on Daisy-chained IPDUs

Table 6.7: Outlet Designations on Daisy-chained IPDUs (PM10 shown)

Number	Description
1	Console server with serial connection shown at Port 2. The IPDU can be connected to any serial port.
2	This is the first IPDU in the chain.
3	This is the second IPDU in the chain.

There are three methods to specify an outlet. The following table describes the three methods.

Table 6.8: Methods for Specifying a Specific Port on Daisy-chained IPDUs

Method	Description
By name	If the outlet has been assigned a name, such as "myoutlet," entering **myoutlet** is sufficient and no other path name is needed.
By IPDU then outlet	Entering **IPDUB[3]** will designate the same outlet.
By serial port then outlet	Entering **!ttyS2-B[3]** will designate the same outlet.

All three methods will designate the same outlet. Note that when a specific IPDU is named in the chain, the outlet number reverts to the IPDU-specific outlet number (3). When only the serial port is used, the IPDU chain is seen as a continuous series of outlets numbered accordingly.

Expert - Applications - Terminal Profile Menu

An administrator can select *Expert - Applications - Terminal Profile Menu* to configure a terminal command menu. This menu is used if a terminal is connected to one of the serial ports and the serial port is configured as a local terminal. A connection to a serial port configured as a local terminal launches a session on the terminal with access to the Linux commands on the console unless you configure a menu here.

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 several remote hosts.

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

To create a menu for a local server terminal:

1. Select *Expert - Applications - Terminal Profile Menu*. The Terminal Profile menu appears.

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 appears.

   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 7.1: Expert - Network Menu Descriptions

Menu Selection	Use This Menu to:
Host Settings	Configure the network parameters such as Host Name, IP addresses, DNS services and Gateway. Additional tabs are displayed for IPv4 and IPv6 protocol configuration.
Syslog	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.
VPN Connections	Configure one or more VPN connections to other systems or attached devices.
SNMP	Configure SNMP with community names, OID and usernames. This section and the dialog boxes guide you to configure the required parameters.
Firewall Configuration	Configure static IP tables and how packets should be filtered.
Host Table	View information about the local network environment. View table of hosts; create, edit and delete hosts.
Static Routes	Manually add routes. Static routes are a very quick and effective way to route data from one subnet to different subnets.

Host Settings

Use the Host Settings form to set up basic host network configuation for the types of Internet protocols you need. The three tabs across the top of the form are General, IPv4 and IPv6.

General host settings

The following table describes the fields on the Network - Host Settings form.

Table 7.2: Network - Host Settings General Tab Form Field

Field name	Field type	Description
Mode	Pull-down menu	Select Internet protocol from IPv4, IPv6 or Dual-Stack, which allows concurrent use of both IPv4 and IPv6 protocols. **NOTE:** Selecting *IPv4* will enable IPv4 protocol configuration and disable IPv6. Selecting *IPv6* will enable IPv4 protocol and will disable IPv4. Selecting *Dual-Stack* will enable configuration for both IPv4 and IPv6 protocols.
Host Name	Text field	Enter the fully qualified domain name identifying the specific host server on the network.
Console Banner	Text field	Enter a text string designed to appear on the console when logging in to or exiting from a port as a way to verify and identify the port connection.
DNS Service		
Primary DNS Server	Text Field	Enter the address of the of the domain name server.
Secondary DNS Server	Text Field	Enter the address of the backup domain name server, if used.
Domain		
Name	Text field	Enter the name of the host domain.

Disabling and enabling IPv4 or IPv6 protocols

The console server allows you to permanently enable or disable either IPv4 or IPv6 protocols during configuration from the Network - Host Settings - General Mode pull-down menu.

Disabling IPv4

If you disable IPv4, configuration of IPv4 addresses will not be allowed. A warning message will be displayed advising you that services not supporting IPv6 will be unavailable. The IPv4

tab will be disabled.

NOTE: If services not supporting IPv6 are needed, you will have to select *Dual-Stack* (IPv4 and IPv6) and those services will be available only for IPv4.

Disabling/Enabling IPv6

If you disable IPv6, configuration of IPv6 addresses will not be allowed and the IPv6 tab will be disabled. If you change IPv6 from disabled to enabled, a warning message will be displayed advising you that some services not supporting IPv6 will be unavailable and that you will have to configure those services supporting IPv6 for them to work properly.

NOTE: If services not supporting IPv6 are needed, you will have to select *Dual-Stack* (IPv4 and IPv6) and those services will be available only for IPv4.

When IPv6 is enabled, you will need to configure the following parameters and services to work in IPv6 mode:

- network parameters
- authentication servers
- DNS
- SNMP
- SNMP traps
- syslog
- NTP
- VPN connections (if any)
- host table addresses
- firewall configuration
- static routes (if any)

NOTE: Both Wizard and Expert modes of the web interface can be used to configure network parameters. Beyond the network parameters stated above, other services must be configured in Expert mode.

NOTE: Change in the configuration of the Mode (Ipv4, IPv6 or dual-stack) will require reboot of the appliance after apply configuration.

IPv4 settings

Select *Network - Host Settings - IPv4*, to navigate to the IPv4 Settings page.

Check *DHCP* (checked by default) to have the console server pull network parameters from the DHCP server. If this box is not checked (DHCP disabled), the following fields are displayed in the form.

Table 7.3: Network - Host Setting - IPv4 Field Defintions

Field name	Field Definition
Primary Address	Enter the primary IPv4 address of the console server.
Network Mask	Enter the 32-bit number used to group IPv4 addresses together or to indicate the range of IPv4 addresses for a subnet.
Secondary Address	The secondary IPv4 address of the console server. By configuring a second IPv4 address, the unit will be available for more than one network.
Secondary Network Mask	Optional.
MTU	Maximum Transmission Unit used by the TCP protocol.

IPv6 settings

Select *Network - Host Settings - IPv6* to navigate to the IPv6 Settings page.

The following table provides definitions of the IPv6 form fields.

Table 7.4: Network - Host Setting - IPv6 Field Defintions

Field name	Field Definition
DHCPv6	Select *None*, *DNS*, *Domain* or *DNS-Domain* from the pull-down menu. Choosing one selects the options for the information that will be retrieved from the DHCPv6 server. None: No further data is retrieved from the server. DNS: The DNS server IP address is retrieved from the server. Domain: The domain path is retrieved from the server. DNS-Domain: Both the DNS server IP address and the domain path are retrieved from the server.

Field name	Field Definition
Method	Select *Stateless only*, *Static* or *DHCP* methods from the pull-down menu for the desired Ethernet port configuration method. Selecting one of these options chooses the method used to obtain and configure IPv6 addresses.
	Stateless only: IPv6 local addresses will be obtained dynamically from the IPv6 router in the local network. This method should be used only if the other two methods are unavailable. Local IPv6 addresses obtained by the router cannot be used outside of the local network.
	Static: This method configures a static IPv6 address and its prefix length for the interface.
	DHCP: The IPv6 address and its prefix length will be obtained dynamically from a DHCPv6 server.
Static Address	Enter the static IPv6 or IPv4 address of the Ethernet port. If entering an IPv6 address, enter both the IPv6 address and its prefix length:
	`<ipaddress>/<prefix_length>`
	Configuring a static IPv6 address is available only if the IPv6 Method selected is *Static*.

IPv6 Ethernet interfaces

All Ethernet interfaces must be either configured or dynamically assigned. Ethernet IPv6 can be dynamically assigned by a DHCPv6 server.

IPv6 serial interfaces

All serial interfaces can be configured with IPv6 addresses (port IP alias).

IPv6 PPP interfaces

All PPP interfaces can be either configured or dynamically assigned with IPv6 addresses. This includes all interface types you might configure to use PPP protocol, such as serial ports with extended modems.

Other interfaces

All interfaces other than Ethernet and PPP will also be configured with IPv6 addresses, including all sub-interfaces and virtual interfaces such as VPN tunnels (static IPSec tunnels). The following list shows the network services that will be configured to support the IPv6 protocol:

• Access to DNS servers

- SNMP

- Sending SNMP trap

- Remote authentication (except to NIS)

- Access to hosts

- Stateful and stateless packet filtering (firewall)

- Static routes

- Sending messages and events to SMTP servers

- Sending data to data buffering servers

- Access to NTP server

- FTP for configuration backup

- FTP for firmware upgrade

NOTE: Virtual ports (virtualization) are not supported by IPv6.

To configure host settings [Expert] from the General form:

1. Go to *Network - Host Settings*. The Host Settings - General form appears.

2. Select *Dual-Stack, IPv4* or *IPv6* from the Mode pull-down menu.

NOTE: If *Dual-Stack* is selected, both IPv4 and IPv6 will remain active and will run concurrently. Selecting *IPv4* will disable IPv6, and selecting *IPv6* will disable IPv4 in the Host Settings form.

3. Enter the name assigned to the IP address of the console server in the Host Name field.

4. Enter a console banner in the Console Banner field.

5. Enter the Primary DNS Server IP address.

6. Enter the Secondary DNS Server IP address, if used.

7. Enter the domain in the Domain Name field.

8. When finished, click *apply changes*.

To configure IPv4 protocol:

1. If IPv4 is enabled (tab is active) select the *IPv4* tab. The IPv4 form will be displayed.

2. If configuring IPv4 using DHCP is desired, click the *DHCP* checkbox.

NOTE: If DHCP is enabled, all other fields on the form will not be displayed.

3. Under Ethernet Port, complete or edit the following fields as necessary.

    a.   Enter the IP address of the console server in the Primary Address field.

    b.   Enter the netmask in the Network Mask field.

    c.   Enter the address of the secondary console server in the Secondary Address field, if used.

    d.   Specify the network mask of the secondary IP in the Secondary Network Mask field.

    e.   Specify the desired maximum transmission unit in the Maximum Transmission Unit field.

4.   When finished, click *apply changes*.

To configure IPv6 protocol:

1.   If IPv6 is enabled (tab is active), select the *IPv6* tab. The IPv6 form will be displayed.

2.   From the DHCPv6 pull-down menu, select *None*, *DNS*, *Domain* or *DNS-Domain*. If *DHCP* is selected, then the DHCP options will define the address configuration information is retrieved from the DHCPv6 server. DHCP options are:

    •   None (only the IP address will be retrieved)

    •   DNS (the DNS address will be retrieved from the DHCPv6 server)

    •   Domain (the domain path will be retrieved from the DHCPv6 server)

    •   DNS-Domain (both DNS server and domain path will be retrieved from the DHCPv6 server)

NOTE: If either *DNS* or *DNS-Domain* is selected, DNS Service and its associated fields will not be displayed.

3.   Under Ethernet Port, complete or edit the following fields as necessary.

    a.   Choose your configuration method from the Method pull-down menu. Choices are Stateless only, Static or DHCP.

NOTE: It is recommended that Stateless only be used only when none of the other methods is available. This means that local configuration from the local router and only the link_local address will be available to the ACS 5000 console server.

    b.   If the DNS Service fields are active (*none* or *Domain DHCP* selected in Step 2) and *Static* has been selected under Ethernet Port, enter the Primary DNS server IP address. If there is a backup DNS server, enter the address of the secondary DNS server in the Secondary DNS server field.

4.   When finished, click *apply changes*.

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. Obtain the facility numbers from the syslog server's administrator.

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 *Add*.

5. Configure the message filtering as per your requirements.

6. Click *apply changes*.

VPN Connections

Virtual Private Network (VPN) enables a secured communication between the console server and a remote network by utilizing a gateway and creating a secured connection between the console server and the gateway. IPSec is the protocol used to construct the secure tunnel. IPSec provides encryption and authentication services at the IP level of the protocol stack.

When VPN Connections is selected under Network, the VPN Connections form appears.

You can use the form to add a VPN connection or edit one already in the list. When you click the *Edit* or *Add* buttons, a New/Modify Connection form appears. The form displays different fields depending on whether *RSA Public Keys* or *Shared Secret* is selected.

The remote gateway is referred to as the Remote or Right host and the console server is referred to as the Local or Left host. If left and right are not directly connected, then you must also specify a NextHop IP address.

The next hop for the remote or right host is the IP address of the router to which the remote host or gateway running IPSec sends packets when delivering them to the left host. The next hop for the left host is the IP address of the router to which the console server sends packets to for delivery to the right host.

A Fully Qualified Domain Name in the ID fields for both the Local ('Left') host and the Remote ('Right') host where the IPSec negotiation takes place should be indicated.

The following table describes the fields and options on the form. Check with your system administrator who defined and configured the security protocols, if needed. The information must match exactly on both ends, local and remote.

Table 7.5: Field and Menu Options for Configuring a VPN Connection

Field Name	Definition
Connection Name	Any descriptive name you wish to use to identify this connection such as **MYCOMPANYDOMAIN-VPN**.
Authentication Protocol	The authentication protocol used, either ESP (Encapsulating Security Payload) or AH (Authentication Header).
Authentication Method	Authentication method used, either RSA Public Keys or Shared Secret.
ID	This is the hostname that a local system and a remote system use for IPSec negotiation and authentication. It can be a fully qualified domain name preceded by @. For example, **hostname@xyz.com**
IP Address	The IP address of the host.

Field Name	Definition
NextHop	The router through which the console server (on the left side) or the remote host (on the right side) sends packets to the host on the other side.
Subnet	The netmask of the subnetwork where the host resides. **NOTE:** Use CIDR notation. The IP number followed by a slash and the number of 'one' bits in the binary notation of the netmask. For example, 192.168.0.0/24 indicates an IP address where the first 24 bits are used as the network address. This is the same as 255.255.255.0.
RSA Key (If RSA Public Keys is selected)	You need to generate a public key for the console server and find out the key used on the remote gateway. You can use copy and paste to enter the key in the RSA Key field.
Pre-Shared Secret (If Shared Secret is selected)	Pre-shared password between left and right users.
Boot Action	The boot action configured for the host, either *Ignore*, *Add* or *Start*.

To configure VPN:

To enable VPN, make sure that *IPSec* is enabled through the security profile section.

1. Go to *Security - Security Profile*. The Security Profiles screen appears.

2. To enable IPSec, click on *Custom*. The Security Custom Profile dialog box opens.

3. To enable IPSec, click the checkbox next to *IPSec*.

4. Click on *OK*.

5. Click on *apply changes*.

6. To add a VPN Connection, click the *Add* button. The New/Modify Connection dialog box appears.

7. Enter any descriptive name you choose for the connection in the Connection Name field.

8. Select either *ESP* or *AH* from the Authentication Protocol pull-down menu.

9. Select *Shared Secret* or *RSA Public Keys* from the Authentication Method pull-down menu.

10. Set up the right and left hosts by doing the following steps.

    a. Enter the fully qualified domain name of the hosts in the ID fields. These are the hostnames where the IPSec negotiation and authentication happens. For example, hostname@xyz.com.

    b. Enter the IP address of the host in the IP Address fields.

c. Enter the IP address of the router through which the host's packets reach the Internet in the NextHop fields.

d. Enter the netmask for the subnet in the Subnet fields in CIDR notation. For example, 192.168.0.0/24 which translates to 255.255.255.0.

e. If *RSA Key* is selected, generate the key for the console server (left host) and find out the key from the remote gateway (right host). You can use copy and paste to enter the key in the RSA Key field.

f. If *Shared Secret* is selected, enter the shared secret in the Pre-Shared Secret field.

11. Select either *Ignore*, *Add* or *Start* from the Boot Action pull-down menu.

12. Click *OK*.

13. 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's 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: username, password, OID and permission.

You can 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 7.6: 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, acs5000_admin@cyclades.com.
SysLocation	The physical location of the console server.

Field or Menu Option	Description
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.

Clicking the *Add* or *Edit* buttons under SNMPv3 Configuration displays the 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. To edit any SNMP configuration, perform the following steps.

    a. For SNMPv1 or SNMPv2 select the entry from the SNMPv1/SNMPv2 configuration list and click the *Edit* button.

    b. To edit an SNMPv3 entry, select an entry from the SNMPv3 Configuration list and click the *Edit* button. The New/Modify SNMP Daemon Configuration dialog box appears.

4. 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.

5. For SNMP v3 configuration, enter or change the following information:

    a. Enter the username in the User Name field.

    b. Enter the password in the Password field.

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

6. 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.

7. Click *OK*.

8. 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.

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.

The administrator can configure the device to filter packets like a firewall. Packet filtering relies on defined chains and rules.

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. 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 opens the 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 appears.

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.

- 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* buttons 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.
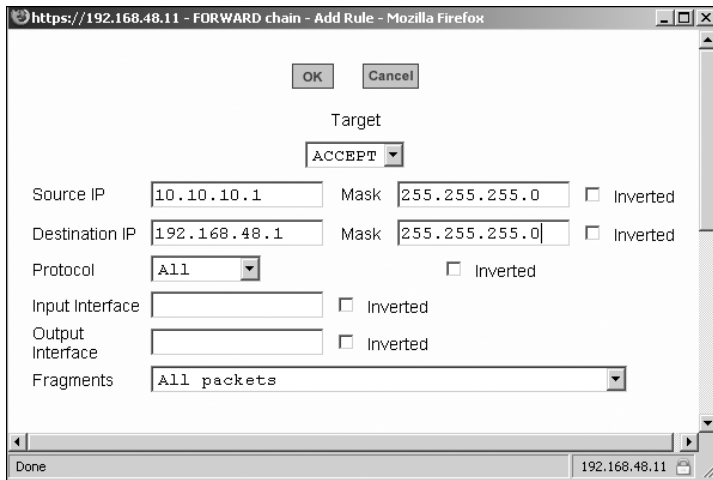
Figure 7.1: Expert - Firewall Configuration Add Rule and Edit Rule Dialog Boxes

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 table appear on the bottom of the form.

Table 7.7: 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 table appear at the bottom of the form.

Table 7.8: UDP Options

Field	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.
Inverted	By checking this box, the UDP options are Inverted. Inverting an item negates the selected rules. Rules will apply to everything except the selected options.

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 table along with the options on the Fragments pull-down menu.

Table 7.9: Expert - Firewall Configuration Input/Output Interface and Fragments Fields

Field	Definition
Input Interface	The input interface (eth0) for the packet.
Output Interface	The output interface (eth0) 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:
	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 table appear in the LOG Options Section at the bottom of the form.

Table 7.10: Expert - Target LOG Options Selection Fields

Field or Menu Name	Definition
Log Level	One of the options in the pull-down menu.
Log Prefix	The prefix is included in the log entry.
TCP Sequence	Includes the TCP sequence in the log.
TCP Options	Includes TCP options in the log.
IP Options	Includes IP options in the log.

REJECT target

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

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

Table 7.11: Reply Packet Names and Definitions

Field Name	Definition
Reject with	*Reject with* means that the filter will drop the input packet and send back a reply packet according to any of the reject types listed below.
icmp-net-unreachable	ICMP network unreachable alias.
icmp-host-unreachable	ICMP host unreachable alias.
icmp-port-unreachable	ICMP port unreachable alias.
icmp-proto-unreachable	ICMP protocol unreachable alias.
icmp-net-prohibited	ICMP network prohibited alias.
icmp-host-prohibited	ICMP host prohibited alias.
echo-reply	Echo reply alias.
tcp-reset	TCP RST packet alias.

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 85

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. The Edit Chain dialog box appears.

NOTE: User-defined chains cannot be edited.

3. Select the desired policy from the Policy pull-down menu.

4. Click *OK*.

5. Click *apply changes*.

6. To edit any rules for this chain, go to To Edit a Rule

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.

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.*Firewall Configuration* on page 79

5. Click *OK*.

6. Click *apply changes*.

Host Table

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

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 hostname in the Name field.

NOTE: IPv6 must be enabled under Host Settings to add or edit IPv6 host addresses.

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.

NOTE: IPv6 must be enabled under Host Settings for adding or editing IPv6 addressing.

The following table describes the fields that appear when you select a routing type from the New/Modify Route dialog boxes.

Table 7.12: Routing Type Fields in the New/Modify Route Dialog Box

Field or Menu Name	Definition
Route	Choices are Default, Network or Host.
Network IP	Appears only when Network route is selected. Type the IP address of the destination network. NOTE: IPv6 must be enabled before IPv6 addresses are allowed.
Network mask	Appears only when Network route is selected. Type the netmask of the destination network.

Field or Menu Name	Definition
Host IP	Appears only when Host route is selected. Type the IP address of the destination host.
Go to	Choices are Gateway or Interface.
[*Adjacent field*]	Type the IP address of the gateway or the name of the interface.
Metric	Type the number of hops to the destination.

To configure static routes [Expert]:

1. Select *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.

   -or-

   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*.

CHAPTER

8

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's 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 are two root users for the initial setup of the console server by the administrator. These usernames are **root** with the default password **avocent** and **admin** with the password **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 Users and Groups form, which you can use to perform the following:

- Add or delete users
- Assign or change user passwords
- Add or delete groups for serial port access configuration
- 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.

Table 8.1: Expert - Add User Dialog Field Names and Definitions

Field Name	Definition
User Name	Name of the user to be added.
Password	The password associated with the username.
Group	On the Group pull-down menu, select Regular User [Default] or Admin. **NOTE:** To configure a user to be able to perform all administrative functions, select the Admin group.
Shell	Optional. The default shell is /bin/sh when the user makes a SSH or Telnet connection.
Comments	Optional notes about the user's role or configuration.

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 username in the User Name field.

4. Enter the password in the Password and Repeat Password fields.

5. Assign a group from the Group pull-down menu.

6. Optional: Select a shell from the Shell pull-down menu.

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 username or multiple comma-separated usernames 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 Active Ports Sessions form, which 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 8.2: Expert - Active Ports Sessions Information

Field Name	Definition
User	First eight characters of the username.
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. If you are using this form to view the information you are done.

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 six tabs, AuthType, RADIUS, TACACS+, LDAP, Kerberos and NIS.

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's 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 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 console server.

For example, if LDAP authentication were to be used for logins to the console server and Kerberos for logins to serial ports, then the console server needs to have network access to an LDAP and a Kerberos 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 set up an authentication server for every authentication method to be used by the console server and its ports.

The following table lists the procedures that apply to each authentication method.

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*.

Group authorization on RADIUS

Group information retrieval from a RADIUS authentication server adds another layer of security by adding a network-based authorization. It retrieves the group information from the authentication server and performs an authorization through the console server.

> **NOTE:** When configuring the RADIUS authentication server, select the *Enable Service-Type attribute checking* checkbox to authorize the console server to retrieve the level of the user (admin or regular) based on the Service-Type attribute from the RADIUS server. Deselect the checkbox to authorize the console server to retrieve the level of user based on the group_name attribute sent by the RADIUS server.

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*.

Group authorization on TACACS+

Using an authorization method in addition to authentication provides an extra level of system security. Selecting *Security - Authentication - TACACS+* in Expert mode displays the TACACS+ form where an administrators can configure a TACACS+ authentication server and can also enable user authorization checking.

By checking the Enable Raccess Authorization checkbox, an additional level of security checking is implemented. After each user is successfully authenticated through the standard login procedure, the console server uses TACACS+ to determine whether or not each user/group is authorized to access specific serial ports.

By default the Enable Raccess Authorization is disabled allowing all users full authorization. When this feature is enabled by placing a check mark in the box, users/groups are denied access unless they have the proper authorization, which must be set on the TACACS+ authentication server itself. To see the configuration procedures for a TACACS+ authentication server, refer to the Cyclades ACS 5000 Command Reference Guide.

To configure an 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, LDAPDownLocal or LDAPDownLocal/Radius).

Before starting this procedure, you will need the following information from the LDAP server administrator:

•   The distinguished name of the search base

•   The LDAP domain name

•   Whether to use secure LDAP

•   The authentication server's IP address

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 in to 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 LDAP authentication:

1. Select *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.

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.

Group Authorization on LDAP

Group information retrieval from an LDAP authentication server adds another layer of security by adding a network-based authorization. It retrieves the group information from the authentication server and performs an authorization through the console server.

To configure a Kerberos authentication server:

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

Before starting this procedure, find out the following information from the Kerberos server administrator:

- Realm name and KDC address

- Host name and IP address for the Kerberos server

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the console server and connected devices know the passwords assigned to the accounts:

- An account for admin

- If Kerberos authentication is specified for the console server, accounts will be needed for all users who need to log in to the console server to administer connected devices

- If Kerberos authentication is specified for the serial ports, accounts will be needed for users who need administrative access to connected devices

Make sure an entry for the console server and the Kerberos server exist in the console server's /etc/hosts file.

1. Go to *Network - Host Table* in Expert mode. The Host Table form appears.

2. Add an entry for the console server if none exists and an entry for the Kerberos server.

    a. Click *Add*. The New/Modify Host dialog appears.

    b. Enter the address in the IP Address field.

    c. Enter the name in the Name field.

    d. Enter an optional alias in the Alias field.

3. Make sure that time, date and timezone settings are synchronized on the console server and on the Kerberos server.

NOTE: Kerberos authentication depends on time synchronization. Time and date synchronization can be achieved by setting both the console server and the Kerberos server to use the same NTP server.

4. To specify an NTP server, see *To configure time and date using an NTP server:* on page 136

5. To set the time and date on the console server manually, see *To set the time and date manually:* on page 135.

6. Work with the Kerberos authentication server administrator to synchronize the time and date between the console server and the Kerberos server.

7. Set the time zone on the console server by going to *Administration - Time/Date* in Expert mode. The default is GMT.

8. Go to *Security - Authentication - Kerberos* in Expert mode.

9. Fill in the form according to your local setup of the Kerberos server.

10. Click *apply changes*.

To configure a NIS authentication server:

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

1. Go to *Security - Authentication - NIS* in Expert mode.

2. Fill in the form according to your configuration of the NIS server.

3. Click *apply changes*.

NOTE: NIS does not work if the Security Profile is set to Moderate or Secured. It only works if the Security Profile is Open.

Security Profiles

A Security Profile consists of a set of parameters that can be configured in order to have more control over the services that are active at any time.

Pre-defined security profiles

There are three pre-defined security profiles:

•   Secure - The Secure profile disables all protocols except sshv2, HTTPS and SSH to serial ports. Authentication to access serial ports is required and SSH root access is not allowed.

NOTE: SSH root access is enabled when the security profile is set to Moderate or Open. If a Secured security profile is selected, you need to switch to a Custom security profile and enable the allow root access option.

•   Moderate - The Moderate profile is the recommended security level. This profile enables sshv1, sshv2, HTTP, HTTPS, Telnet, SSH and Raw connections to the Serial Ports. In addition, ICMP and HTTP redirection to HTTPS are enabled. Authentication to access the serial ports is not required.

•   Open - The Open profile enables all services such as Telnet, sshv1, sshv2, HTTP, HTTPS, SNMP, RPC, ICMP and Telnet, SSH and Raw connections to the serial ports. Authentication to access serial ports is not required.

Default security profile

The Default Security Profile uses the same parameters as the Moderate profile. See the following tables for the list of enabled services when the Default security profile is used.

Custom security profile

The Custom Security Profile opens up a dialog box to allow custom configuration of individual protocols or services.

NOTE: By default, a number of protocols and services are enabled in the Custom profile; however, they are configurable to a user's custom requirements.

The following tables illustrate the properties for each of the Security Profiles. The enabled services in each profile is designated.

Table 8.3: Enabled Services to Access the Appliance Under Each Security Profile

Access to the Console Server	Secure	Moderate	Open	Default
Telnet	N/A	N/A	Yes	N/A
sshv1	N/A	Yes	Yes	Yes
sshv2	Yes	Yes	Yes	Yes
Allow SSH root access	N/A	Yes	Yes	Yes
HTTP	N/A	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes
HTTP redirection to HTTPS	N/A	Yes	N/A	Yes

Table 8.4: Enabled Services to Access the Serial Ports Under Each Security Profile

Access to Serial Ports	Secure	Moderate	Open	Default
Console (Telnet)	N/A	Yes	Yes	Yes
Console (ssh)	Yes	Yes	Yes	Yes
Console (Raw)	N/A	Yes	Yes	Yes
Serial Port Authentication	Yes	N/A	N/A	N/A
Bidirect (Dynamic Mode Support)	N/A	Yes	Yes	Yes

Table 8.5: Enabled Protocols for Each Security Profile

Other Services	Secure	Moderate	Open	Default
SNMP	N/A	N/A	Yes	N/A
RPC	N/A	N/A	Yes	N/A
ICMP	N/A	Yes	Yes	Yes
FTP	N/A	N/A	N/A	N/A
IPSec	N/A	N/A	N/A	N/A

The first step in configuring your console server is to define a security profile. One of the following situations is applicable when you boot up the console server.

•   The console server is starting for the first time or after a reset to factory default parameters.

    In this situation when you boot up your console server and log in as an administrator to the web manager, a security warning dialog box appears. The web manager is redirected to Step1: Security Profile in the Wizard mode. Further navigation to other sections of the web manager is not possible without selecting or configuring a security profile. Once you select or configure a security profile and save the changes, the console server restarts.

•   The console server firmware is upgraded and the system is restarting with the new firmware.

    In this situation the console server was already in use and certain configuration parameters were saved in the flash memory. In this case the console server automatically retrieves the Custom Security Profile parameters saved in the flash memory and behaves as it was a normal reboot.

•   The console server is restarting normally.

    In this situation the system detects the pre-defined security profile. You can continue working in the web manager.

Serial port settings and security profiles

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

The following situations apply to serial ports when you modify or change a security profile.

- If you reconfigure the security profile and restart the web manager, you need to make sure the serial ports protocols and access methods match the selected security profile.

To select or configure a security profile:

The following procedure assumes you have installed a new console server at your site or you have reset the unit to factory default.

1. Enter the assigned IP address of the console server in your browser and log in as an administrator.
2. Review the security advisory and click the *Close* button.
3. The web manager is redirected to Wizard - Step 1: Security Profile.
4. Select a pre-defined security profile by selecting one of the *Secure*, *Moderate*, *Open* or *Default* profiles or create a *Custom* profile. The following dialog box appears when you select the Custom profile.

CAUTION: Take the required precautions to understand the potential impacts of each individual service configured under the Custom profile.

It is not possible to continue working in the web manager without selecting a security profile.

Once you select a security profile or configure a custom profile and apply the changes, the console server web manager restarts in order for the changes to take effect.

5. Select *apply changes* to save the configuration to Flash. The web manager restarts.
6. Log in after web manager restarts.
7. The web manager defaults to Ports - Ports Status page.

Security certificates

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

NOTE: It is highly recommended that you use the openssl tool to replace the console server-generated certificate.

Certificate 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 procedures to obtain a Signed Digital Certificate is documented in the Cyclades ACS 5000 Command Reference Guide.

User configured digital certificate

You can generate a self-signed digital certificate. The procedures to configure a self-signed digital certificate is documented in the Cyclades ACS 5000 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 ACS 5000 Command Reference Guide.

Ports Menu and Forms

Physical Ports

By selecting *Ports - Physical Ports* in Expert mode, 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 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, do 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 another port or ports.

   c. To select multiple ports that are not in a range, click the first port in the list and then hold down the **Ctrl** key while selecting another port.

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 in Expert Mode, if you select one or more ports from the ports list and click the *Modify* button, the General form appears.

The General form allows you to define general port settings, connect to an IPDU port 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.

Clicking *Ports - Physical Ports - General* and selecting the appropriate connection protocol on the 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.

The following table shows the options from the list of connection protocols when the console server serial port is connected to the console port of a server or a device.

Table 9.1: Connections Protocols When a Serial Port is Connected to a 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.

Protocol Name	Result
Console (TelnetSSH)	Authorized users can use Telnet and/or SSH to connect to the console of the connected device simultaneously. When 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 terminal is connected to the serial port of the appliance, 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 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.

The following table describes the connection protocols that can be selected if a terminal is connected to the selected serial port.

Table 9.2: Available Connection Protocols When Terminal is Connected to a Serial Port

Protocol Name	Result
Telnet	Dedicates a terminal connected to a serial port to access a server using the Telnet protocol. When the attached terminal is turned 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 terminal connected to the selected serial port to access a server using the SSHv1 protocol. When the attached terminal is turned 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.

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 turned 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 terminal connected to the selected serial port for connecting to the console server. When the attached terminal is turned 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 terminal connected to the selected serial port to access a specific remote host using the Raw Socket protocol. When the attached terminal is turned 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.

The console profile features such as data buffering, multiple users and event notifications are not available under this profile.

When the attached terminal is turned on and the **Enter** key is pressed, a login banner and a login prompt is displayed.

NOTE: If the user does not log in within a configurable timeframe, the serial port returns to an idle state. The timeout period can be configured through the Web Manager Ports - Physical Ports - Access form.

The administrator can build custom menus using the Terminal Profile Menu form accessible from the web manager, Applications - Terminal Profile Menu or from a terminal window using the menush_cfg command. You should specify the bidirectional shell command, /bin/menush in the web manager, Ports - Physical Ports - Access form.

Bidirectional Telnet protocol

Bidirectional Telnet protocol can be selected from the Ports - Physical Ports - General from.

Bidirectional Telnet supports both a CAS profile Telnet connection and a TS profile menu shell. Both connection protocols are supported on one port; however, connections cannot be opened simultaneously.

Modem and power management connection protocols

The following table shows the connection protocols for modems or IPDUs connected to the serial ports.

Table 9.3: Connection Protocols for Modems or IPDUs.

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.
Power Management	Configures the serial port for power management. Assumes an IPDU is connected to the serial port.

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 and 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).

4. If you wish to change any of the other current settings, see *To configure serial port settings to match the connected devices:* on page 111.

5. To further configure the serial port's connection protocol:

    •   For user access and authentication methods see *Access* on page 112.

    •   For TCP Port number and other port configuration options see *Other* on page 121.

To configure a serial port connection protocol for a Bidirectional Telnet:

The following procedure assumes that the selected serial port is physically connected to a terminal. For more information on Bidirectional Telnet connection protocol, see *Bidirectional Telnet protocol* on page 106.

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 yellow.

3. To change the connection protocol, select Bidirectional Telnet from the Connection Protocol pull-down menu.

4. If you wish to change any of the other current settings, see *To configure serial port settings to match the connected devices:* on page 111.

5. Go to the *Access* tab and configure the following settings:

   a. In the Authorized Users/Groups field restrict or deny access to a serial port by specifying one or more users or groups.

   b. From the Type pull-down menu, select an authentication type for the serial port. The default is no authentication (Type=None).

   c. In the Bidirection Login Timeout field enter the time for the serial port to return to an idle state. When the username is not entered in the terminal window after the login banner is displayed, the serial port returns to an idle state. The default timeout value is 60 seconds.

   d. In the Bidirection Shell Command field enter the menu shell command, for example, **/bin/menush** to build a custom menu for the TS profile.

6. To customize a menu shell, go to the web manager, Applications - Terminal Profile Menu form. For more information on configuring a menu shell see *Applications* on page 51.

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 105.

1. Go to *Ports - Physical Ports* in Expert mode, select a port or ports to modify and 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 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. Terminal Profile Menu form is at 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:* on page 111.

NOTE: Most modems have hardware flow control configured; this requires configuration of hardware flow control in the serial port settings.

---

5. To further configure the serial port's connection protocol:

   • For user access and authentication methods, see *Access* on page 112.

   • To configure modem initialization and PPP options see *Other* on page 121.

6. If you are finished, click *Done*.

7. Click *apply changes*.

To configure a power management protocol for an IPDU:

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

1. Go to *Ports - Physical Ports* in Expert mode, select a port or ports to modify and 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.

3. To change the connection protocol, select *Power Management* from the Connection Protocol pull-down menu.

4. Enter a desired name for the IPDU in the Alias field.

5. Select an access method for the IPDU from the Allow Access by pull-down menu. The options are SSH, Telnet or SSH and Telnet. Selecting an access option activates the Access and Other tabs.

6. Go to the *Access* tab.

   a. Enter the users/groups authorized to access the serial port.

   b. Select an authentication type for the serial port from the pull-down menu.

NOTE: Authentication type None is not a valid option when the serial port is configured for Power Management connection protocol. The system defaults to Local if no authentication type is selected.

NOTE: Configuration for One Time Password (OTP) and OTP/Local is documented in the Cyclades ACS 5000 Command Reference Guide.

7. Select the *Other* tab. There are two fields: TCP Port and Port IP Alias.

   a. A default TCP port number is displayed in the TCP Port field. Enter an alternate port number if you are overriding the default.

   b. In the IP Alias field, enter the IP address for the port for direct telnet or SSH access (the same address used when the port is configured for console access).

NOTE: For the IP Alias address to work properly, you must select *Allow Access by* Telnet or SSH or both in the General tab form.

8. When finished, click *Done*.

9. 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 button.

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. To change the baud rate, select an option from 2400 to 230400 Kbps from the Baud Rate pull-down menu. The default is 9600.

3. To change the flow control, select *None*, *Hardware* or *Software* from the Flow Control pull-down menu. The default is None.

4. To change the parity, select *None*, *Odd* or *Even* from the Parity pull-down menu. The default is None.

5. To change the data size, select an option from 5 to 8 from the Data pull-down menu. The default is 8.

6. To change the stop bits, select *1* or *2* from the stop bits pull-down menu. The default is 1.

7. To change whether the DCD (Data Carrier Detect) State is disregarded or not, select either *Disregard* or *Regard*.

8. Click *Done*.

9. Click *apply changes*.

Access

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

The following table describes the menu and fields on the Access form.

Table 9.4: 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:
	!noadmin,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).
	NOTE: Authentication type None is not a valid option when the serial port is configured for Power Management connection protocol. The system defaults to Local if no authentication type is selected.
BidirectionLogin Timeout	Configure the time for the serial port to return to idle state, if the username is not typed in the terminal after the login banner is displayed. The default timeout value is 60 seconds.
	This field is available only when a Bidirectional Telnet protocol is selected from Ports - Physical Ports - General - Connection Protocol.
BidirectionShell Command	Specify the menu shell command in this field, for example, **/bin/menush** and build a custom menu for the TS profile using the web manager, Applications - Terminal Profile Menu form.
	This field is available only when a Bidirectional Telnet protocol is selected from Ports - Physical Ports - General - Connection Protocol.

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 Kerberos, 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. The following table describes the authentication methods and fallback mechanisms.

Table 9.5: Expert - Authentication Methods and Fallback Mechanisms

Authentication Type	Definition
None	No authentication.
Kerberos	Authentication is performed using a Kerberos server.
Kerberos/Local	Kerberos authentication is tried first, switching to Local if unsuccessful.
KerberosDownLocal	Local authentication is performed only when the Kerberos server is down.
LDAP	Authentication is performed against an LDAP database using an LDAP server.
LDAP/Local	LDAP authentication is tried first, switching to Local if unsuccessful.
LDAPDownLocal	Local authentication is performed only when the LDAP server is down.
Local	Authentication is performed locally. For example, using the /etc/passwd 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.
Local/NIS	Authentication is performed locally first, switching to NIS if unsuccessful.
NIS	NIS authentication is performed.
NIS/Local	NIS authentication is tried first, switching to Local if unsuccessful.

Authentication Type	Definition
NISDownLocal	Local authentication is performed only when the NIS server is down.
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 is selected from the Destination menu.

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.

The following table describes the fields available in the data buffering form.

Table 9.6: Data Buffering Form Fields

Field Name	Definition
Destination	Location for the data files. Either Local or Remote.
Mode (Local Destination)	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. Circular buffering requires the administrator to set up processes to examine the data during the timeframe before the data is overwritten by new data. In linear mode, the kernel serial driver buffer is used to store the Rx data. Once the 4Kb is reached, a flow control stop is issued to prevent the serial port from receiving further data from the remote peer.
File Size (Bytes) (Local Destination)	The maximum file size for the data buffer file. The file size must be greater than zero.
NFS File Path (Remote Destination)	The path for the mount point of the directory where data buffer file is to be stored. **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.
Record the timestamp.	Save a timestamp with the data in the data buffer file.
Syslog Server	The IP address for the preconfigured Syslog server.
Facility Number	Choose a facility number to assign to the console server. Obtain the facility number for the console server from the system administrator of the syslog server. The facility number is included in any syslog message generated from the console server. The server's administrator can use facility numbers to isolate logs from individual devices into individual files. Options range from Local0 to Local7.
Syslog Buffer Size	Maximum size of the buffer in the Syslog server.
Buffer SysLog at all times	As indicated.
Buffer SysLog only when no user is connected to the port	As indicated.
Hostname Discovery	Check to enable the console server to attempt to discover the hostname of the server connected to the serial port.

Field Name	Definition
Timeout (seconds)	Amount of time in seconds that the console server will try to discover the hostname. If it cannot be identified in that time, a default name will be assumed.
Show Menu	Choose from the following options to select what will be shown when connected to the serial port to see or work with the data buffering: *Show all options*, *No*, *Show data buffering file only*, *Show without the erase options* or *Show and erase data buffering file*.

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.

   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* 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 no user 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, select *Expert - Administration - Notifications*.

Multi User

Under Ports - Physical Ports in Expert Mode, after you select one or more serial ports and click *Modify Port(s)*, you can select *Multi User* 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 Allow Multiple Sessions pull-down menu, the Privilege Users field should be populated with the user names who have access rights.

The following table describes the available fields on the Multi User form.

Table 9.7: Expert - Multi User Form Fields

Field Name	Definition
Allow Multiple Sessions	Options are No, Yes (show menu), Read/Write (do not show menu) and ReadOnly (do not show menu).
Sniff Mode	Allow sniffing on multiple user connection to a serial port.
Privilege Users	Users with access rights to a multi user shared session.
Menu Hotkey	The hotkey for accessing the menu.
Notify Users	Checkbox to enable notify users of session access.

The following table describes the options from the Allow Multiple Sessions pull-down menu.

Table 9.8: 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.

Menu Option	Description
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:
	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) and 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*.

Power Management

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 Power Management form from the tabbed menu (it will

be available if there is at least one port configured as Power Mgmt or there is at least one IPMI server configured). The Power Management form appears.

You can use this form to make it possible for a user who is connected to a device through the selected serial port to perform power management. While connected to the device, the user displays a power management menu or dialog box by entering a hotkey.

NOTE: Enable power management on this form refers to IPDU power management, Applications - IPDU Power Mgmt.

Additional fields appear on the form if Enable Power management on this port and Enable IPMI on this port are checked.

The following table describes the available fields in the power management form.

Table 9.9: Expert - Power Management Form Fields

Field Name	Definition
Enable Power Management on this Port	Check mark to enable Power Management on the the selected port(s).
Enable IPMI on this port	Check mark to enable IPMI on the selected port(s).
IPMI Key (available only if IPMI is enabled)	The key sequence which the authorized user(s) can use to perform IPMI power management. The default for IPMI power management is **Ctrl+Shift+i (^I)**.
IPMI Server (available only if IPMI is enabled)	Select the device configured for IPMI power management.
PowerMgmt Port	View listbox for the PM enabled ports and the assigned outlet numbers.
Power Management Key	The key sequence which the authorized user(s) can use to perform power management. The default for IPDU power management is **Ctrl+p (^p)**.
Allow All Users	Radio button to allow all users to perform power management on the configured port.
Allow Users/Groups	Radio button to allow only selected users or groups to perform power management on the configured port.

Field Name	Definition
New User/Group (available only if Allow Users/Groups radio button is selected)	Entry field to add a new user/group.
Allowed Users/Groups (available only if Allow Users/Groups radio button is selected)	View list box of authorized users or groups.

Power management while connected to a port is possible only when one or both of the following conditions are true.

• The device connected to the console server is plugged into an IPDU and is configured for power management.

• The device connected to the console server is a server with an IPMI controller and the server is added to the IPMI device list. To see the list of previously configured IPMI devices or to add a new IPMI device, go to *Applications - IPMI Power Mgmt*.

If you click *Enable power management* and click the *Add* button, the Add Outlet dialog box appears. In this dialog box, you can specify the IPDU and the outlet number(s) into which the device is plugged.

To configure a serial port for IPDU power management:

1. Go to *Ports - Physical Ports*, select a port or ports to modify and click the appropriate Modify Ports button and the *Power Management* tab.

2. To enable power management of a device connected to the current port and plugged into a connected IPDU, click *Enable Power Management* on this port.

3. Select the name of a port configured for power management and click the *Add* button. The Add Outlet dialog box appears.

4. Enter the outlet number(s) into which the device is connected to separated by commas.

5. Click *OK*. The power management port and the specified outlet numbers are displayed on the PowerMgmt Port list.

6. Enter the power management hotkey in the Power Management Key field. Enter a caret (**^**) for the escape key, as in **^p**. The caret stands for the **Ctrl** key.

7. Click *Done*.

8. Click *apply changes*.

NOTE: If you wish to configure IPMI power management on this port, continue to the IPMI configuration procedure below.

To configure a serial port for IPMI power management:

This procedure assumes you have added the connected IPMI device in the Applications - IPMI Power Mgmt. form.

1. To enable IPMI Power Management of an IPMI device connected to the currently selected port, perform the following steps:

    a. Click the *Enable IPMI on this port* checkbox. The IPMI key and IPMI Server fields appear.

    b. Enter a key in the IPMI key field. Enter the key combination in the IPMI key field with **^**, as in **^i**. The caret (**^**) stands for the **Ctrl** key. The administrator of the device connected to this serial port uses this hotkey to bring up the IPMI power management screen.

    c. Select the name of the IPMI device from the IPMI Server pull-down menu.

2. Click *Done*.

3. Click *apply changes*.

To configure a user for IPDU power management while connected to a serial port:

Perform this procedure to allow a user to perform power management on a device while connected to it through one of the console server's serial ports.

1. Configure a serial port for IPDU power management as described in the previous section.

2. To permit everyone who can access this port to perform power management on this port, click the *Allow All Users* radio button.

3. To restrict power management on this port to a set of users authorized to access this port, click the *Allow Users/Groups* radio button.

4. Enter a valid username or groupname in the New User/Group field and click *Add*.

5. Click *Done*.

6. 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 9.10: 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 has. For example, a console server with 8 serial ports has TCP port numbers 7001 through 7008.
Port IP Alias	A name (alias) for the IP of the selected port. A port IP alias field appear when a console (CAS) profile is selected from the Connection Protocol pull-down menu on the General form.
Windows EMS	Checkbox to enable Windows EMS (Emergency Management Services). Appears only 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.
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**
Login Banner	Enter the text you wish to appear as a login banner when logging in to a terminal.
Host to Connect	This field should be populated with the IP address of the device you are connecting to. 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	Select the desired terminal server profile from the pull-down menu.
Serial Configuration Mode Key	The key sequence to perform serial port line configuration by a menu driven in the session opened against the serial port. Users that have access rights to the serial port will be authorized to perform this operation.

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 *Modify Selected Port(s)*.

3. Select the *Other* tab.

4. To change the port number for the serial port, enter another number in the TCP Port field.

5. To assign a name to the port's IP address, enter an alias in the Port IP Alias field (console connection protocol only).

6. If connecting to a Microsoft Windows Server 2003 operating system through the Emergency Management Services (EMS) console, enable the Windows EMS console connection protocol only.

7. To change the Keep-Alive interval, enter another number in the TCP Keep Alive Interval field.

8. To change the idle timeout interval, enter another value in the Idle Timeout field.

9. Specify stty options, if desired, in the STTY Options field.

10. To change the break interval, enter a new number in the Break Interval field.

11. To change the break sequence, enter a new sequence in the Break Sequence field.

12. To change the content of the login banner, enter new content in the Login Banner field.

13. Click *Done*.

14. 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

NOTE: Virtual Ports is available only for IPv4 protocol.

The virtual ports form allows you to perform clustering of the console server. 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.

NOTE: Multiple IPDUs should only be connected and daisy-chained through the serial port of the master console server when you are configuring a cluster.

This section shows you how to define and configure the slaves.

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

Table 9.11: New/Modify Port Dialog Box Fields.

Field Name	Definition
Number of Ports	Number of ports on each slave unit. Choices are 4, 8, 16, 32 and 48.
First Local Port Number	The first unallocated port number for the Slave. For example, if the master unit has 16 ports, ports 1-16 are allocated. The First Local Port Number is then 17.
Local IP	The IP address for the master console server or it can be the global IP address of the cluster in the network.
First Local TCP Port No.	The first TCP port number for the slave. For example, if the master unit has 16 ports, the allocated TCP port numbers to the master are 7001-7016. The First Local TCP Port No. is then 7017. This is a virtual TCP port number.

Field Name	Definition
Remote IP	The IP address of the slave.
First Remote TCP Port Number	The first TCP port number of the slave. The default is 7001.
Protocol	The communication protocol used by the Slave. The options are Telnet or SSH.

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 the 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.

2. From the pull-down menu select the number of ports that you wish to assign as slaves. Choices are 4, 8, 16, 32 and 48.

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 Port Names form.

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

Ports Status

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

Table 9.12: 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

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

Table 9.13: 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.
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.

Expert - Ports - Hostname Discovery

An administrator can use the Expert - Ports - Hostname Discovery screen to configure lists of probe and answer strings that apply to all serial ports that have been configured for hostname discovery. See *Hostname Discovery* on page 13 for details about how the strings are used for other configurations needed for hostname discovery to work.

If you want the console server to attempt to discover the hostname, select *Expert - Ports - Hostname Discovery* and enter the time-out value in seconds in the field provided. If the console server cannot discover the hostname in the allotted time, the default target device name is used.

The probe and answer strings can be left blank. The default strings have a broad range and work in most cases.

Table 9.14: Expert - Ports - Hostname Discovery Fields

Fields	Accepted Values
Hostname Discovery Probe Strings	A list of strings, delimited by double quotes (") and separated by spaces. The following C-style escape sequences are accepted: "\n" (new line; "\r" (carriage return); "\t" (horizontal tabulation); "\f" (form-feed); "\\" ((backslash) and "\"" (double-quote). Probe strings can have more than one escape sequence and use regular characters, but simpler sequences such as "\r" or "\n" are recommended. "\n" is the default if no strings are defined.
Hostname Discover Answer Strings	A list of strings, delimited by double quotes (") and separated by spaces. Must be written as POSIX extended regular expressions. If no strings are defined, then "([A-Za-z0-9\\.-_]+)[]+[Ll]ogin[:]?[]?$" is the default. If the user regex has more than one group, then only the first group is matched.

To configure hostname discovery probe and answer strings [Expert]:

1. Select *Expert - Ports - Hostname Discovery*. The Hostname Discovery screen appears.

2. Enter one or more strings delimited by double quotes and separated by spaces.

3. Click *apply changes*.

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 10.1: System Information Form

Information	Parameters
System Information	Serial Number
	Kernel Version
	Current Date
	Up Time
	Power Supply State
	System MAC Address
	IPv4 Address
	Static IPv6 Address
CPU Information	CPU Type
	Clock Speed
	Revision
	Bogomips

Information	Parameters	
Memory Information	MemTotal	SwapFree
	MemFree	Dirty
	Buffers	Writeback
	Cached	Mapped
	SwapCached	Slab
	Active	CommitLimit
	Inactive	Committed_AS
	HighTotal	PageTables
	HighFree	VmallocTotal
	LowTotal	VmallocUsed
	LowFree	VmallocChunk
	SwapTotal	
Ram Disk Usage	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.

The following table describes the available fields in the Notifications form.

Table 10.2: Notifications Form Fields

Field Name	Definition
Notification Alarm for Data Buffering	Enable by placing a checkmark in this field
[unlabeled view table]	List of alarm types and triggers
[unlabeled dropdown list]	Email, pager or SNMP notification methods

Clicking the *Add* button or selecting a previously specified event, then 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. The following table describes the available fields in the email notification entry dialog box.

Table 10.3: Email Notifications Dialog Box Fields

Field Name	Definition
Alarm Trigger	The trigger expression used to generate an alarm.
[untitled dropdown field]	The first time you specify an alarm trigger the pull-down menu is empty. A new trigger gets listed in the menu after it is created.
To/From/Subject/Body	The email for the designated recipient of the alarm notification.
SMTP Server IP	The IP address of the SMTP server.
SMTP Port	The port used by the SMTP server.

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 for 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. The following table describes the available fields in the pager notification entry dialog box.

Table 10.4: Pager Notification Add/Edit Dialog Box Fields

Field Name	Definition
Alarm Trigger	The trigger expression used to generate an alarm.
[untitled dropdown field]	The first time you specify an alarm trigger the pull-down menu is empty. A new trigger gets listed in the menu after it is created.
Pager Number	The pager number of the notification recipient.
Text	The text message for the pager.
SMS User Name	The user name of the notification recipient.
SMS Server	The name or the IP address of the SMS server.
SMS Port	The port used by the SMS server.

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 for 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.

Table 10.5: SNMP Trap Notifications Add/Edit Dialog Box Fields

Field name	Definition
Alarm Trigger	The trigger expression used to generate an SNMP trap.
[*untitled dropdown field*]	The first time you specify an alarm trigger the pull-down menu is empty. A new trigger gets listed in the menu after it is created.
OID Type Value	The value that uniquely identifies an object to the SNMP agent.

Field name	Definition
Trap Number	The trap type as defined in the MIB. The choices are: Cold Start Warm Start Link Down Link Up Authentication Failure EGP Neighbor Loss Enterprise Specific
Community	The password used to authenticate the traps.
Server	The IP address of the server running the SNMP.
Body	The content of the notification.

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 for 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 turned off

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 130.

7. Click *OK*.

8. Click *apply changes*.

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 menu. 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.

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 timezone 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.

To create a custom timezone selection:

1. Enter the name of the time zone you would like to appear in the Timezone pull-down menu on the main Time/Date form. (For example, **Pacific**).

2. Choose a preferred or standard acronym for the time zone (For example, **PST**).

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 will appear.

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 savings 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 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, you need to 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 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

The following table describes the boot configuration form fields.

Table 10.6: 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.
RAM Test	Select to test boot from RAM. You can skip this test, do a quick test or a full test.

Field Name	Definition
Fast Ethernet	The speed of the Ethernet connection. Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value): 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.

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.

The following table describes the available fields and buttons in the Backup Config form.

Table 10.7: Backup Configuration Settings 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.
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.

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

1. Go to *Administration - Backup Config* in Expert mode.

2. Enter the IP address of the FTP server in the Server IP field.

3. 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.acs-k26**.

4. Enter the username and password provided by your system administrator for the FTP server.

5. To backup a copy of the current configuration files, click the *Save* button.

6. To download a previously saved copy of the configuration files, click the *Load* button.

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: Download released firmware from the Avocent site to a local ftp server. Check the filename for the upgrade version and read the upgrade instructions carefully. Distinct procedures are required depending on the version you are upgrading from.

The following table describes the fields in the Upgrade Firmware form.

Table 10.8: Expert - Upgrade Firmware Form Fields

Field/Menu Name	Definition
Type	FTP is the only supported type.
FTP Site	The URL of the FTP server where the firmware is located.
Username	Username recognized by the FTP server.
Password	Password associated with the username.
Path and File Name	The pathname of the firmware on the FTP server.
Run Checksum	Runs the checksum program to verify the accuracy of the uploaded data.

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. Enter the URL of the FTP server in the FTP Site field.

3. Enter the username recognized by the FTP server in the Username field.

4. Enter the password associated with the username on the FTP server in the Password field.

5. Enter the path name of the file on the FTP server in the Path and Filename field.

6. Use the drop-down menu to enable or disable Run Checksum.

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/Cyclades server is not always possible due to firewall configurations, nor is it recommended. It is generally advisable for you to download the online help .zip file and run it from a local server.

Online help for the console server should be downloaded from www.avocent.com. For more information on downloading the online help, contact Technical Support. The procedure for configuring the online help on the local server follows.

Select *Administration - Online Help* in Expert mode. The online help configuration page is displayed.

The console server administrator can 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/acs5000/v_3.3.0 is the location specified in the field. It is recommended that the 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/acs-help
   #gunzip acs_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 in to the web manager as admin and go to *Administration - Online Help*. The Help configuration screen displays.

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 ACS 5000 console server 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 ACS 5000 Advanced Console Server Hardware

Hardware	
CPU	MPC855T (PowerPC Dual-CPU)
Memory	128MB DIMM SDRAM min./ 16MB Compact Flash min.
Interfaces	1 Ethernet 10/100BT on R-J45
	1 RS232 Console on RJ-45
	RS232 Serial Ports on RJ-45
Power	Internal 100-240VAC, 50/60 Hz
Dimensions	17 x 8.5 x 1.75 in (43.18 x 21.59 x 4.45 cm)
Environmental	
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-condensing

Hardware	
	FCC Part 15, A
	ICES-003
	C-Tick
	VCCI Class A
	MIC Class A
	CE
Safety and EMC Standards Approvals and Markings	EN55022, Class A
	EN55024
	EN60950-1
	GS
	CB
	CSA/UL 60950-1
	Solaris Ready™
	NOTE: Some marks may not apply for all models of the ACS 5000 console server.

Appendix B: 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 a Cyclades ACS 5000 advanced console server.

Folgendes sollte beim Rack-Einbau des Cyclades ACS 5000 berücksichtigt werden.

Temperature

The manufacturer's maximum recommended ambient temperature for the Cyclades ACS 5000 advanced console server is 112º F (44º C).

Temperatur

Die maximal empfohlene Umgebungstemperatur des Cyclades ACS 5000 beträgt 44º C (112º 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.

Erhöhte Umgebungstemperatur im betrieb

Bitte treffen Sie entsprechende Vorkehrungen um die Herstellerangaben zur maximalen Umgebungstemperatur einzuhalten. Bitte beachten Sie, dass bei einer Installation des ACS 5000 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 ACS 5000 advanced console server.

Sicherheitsvorkehrungen beim Betrieb des Cyclades ACS 5000 Advanced Console Server

Bitte lesen Sie alle folgenden Sicherheitsrichlinien um sich und Ihren Cyclades ACS 5000 advanced console server vor Schäden zu bewahren.

WARNING: Do not operate your Cyclades ACS 5000 advanced console server with the cover removed.

Bitte betreiben Sie den Cyclades ACS nicht mit geöffnetem Gehäuse.

CAUTION: To avoid shorting out your 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.

Um Schäden beim Entfernen des Netzwerkkabels zu vermeiden bitte immer zuerst das Kabel vom Host Server entfernen, anschließend die externe Stromzufuhr abklemmen und danach das Kabel aus der Netzwerkbuchse ausstecken. Beim Wiederherstellen der Verbindung immer zuerst das Kabel in die Netzwerkbuchse des ACS 5000 zuerst einstecken und danach das Kabel in den Host Server einstecken.

CAUTION: To help prevent electric shock, plug the 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.

Um Stromschläge zu vermeiden den ACS 5000 bitte mit einer ausreichend geerdeten Stromquelle verbinden. Zu diesem Zweck ist das Eingangskabel ist 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 ACS 5000 advanced 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.

Um den Cyclades ACS 5000 vor elektrischen Netzschwankungen zu bewahren bitte Überspannungsfilter, Entstörfilter oder eine UVS einsetzen. Stellen Sie bitte sicher dass sich keine Gegenstände auf den Kabeln des ACS 5000 befinden und dass die Kabel tritt- und stolpersicher geführt sind. Bitte keine Lebensmittel oder Flüssigkeiten über den ACS schütten.

CAUTION: Do not push any objects through the openings of the Cyclades ACS 5000 advanced console server. Doing so can cause fire or electric shock by shorting out interior components.

Zur Vermeidung von Brandgefahr oder elektrischen Schlägen bitte keine Gegenstände durch die Öffnungen des Cyclades ACS 5000 stecken.

CAUTION: Keep your Cyclades ACS 5000 advanced console server away from heat sources and do not block host's cooling vents.

Der Cyclades ACS 5000 muss vor Hitzequellen geschützt werden und die Lüfterausgänge dürfen nicht blockiert sein.

CAUTION: This unit has one or two power supply cords. Disconnect the power supply cord before servicing to avoid electric shock.

Cet appareil comporte un ou deux cordon d'alimentations. Afin de prévenir les choc électriques, debrancer les cordons d'alimentation avant de fairt le dépannage.

Das Geraet hat entweder ein oder zwei Netzverbindungen. Um elektrischen Schlag zu vermeiden muessen die Netzverbindungen getrennt sein bevor Wartungsarbeiten vorgenommen werden.

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 and

• Keep body movement to a minimum while removing or installing boards to minimize the buildup of static charge.

Arbeiten am Cyclades ACS 5000

Bitte versuchen Sie nicht den ACS 5000 selbst zu warten mit Ausnahme unter Befolgung der Anweisungen von Cyclades technischem Personal. In diesem Fall bitte folgenden Vorsichtsmaßnahmen einhalten:

1. Schalten Sie den ACS 5000 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 und.

• Zur Minimierung von elektrostatischen Aufladungen alle Körperbewegungen während Ein- oder Ausbau von Boards auf ein Minimum reduzieren.

Replacing the battery

CAUTION: There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Austausch der Batterie

Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Remplacement de la batterie

Il y a risque d'explosion si la batterie est remplacée par une batterie de type incorrect. Mettre au rebut les batteries usagées conformént aux instructions.

Trabajar dentro del Cyclades ACS 5000 Advanced Console Server

No intente dar servicio al Cyclades ACS 5000 advanced 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 ACS 5000 advanced console server. Asegurase que este tocando tierra antes de tocar cualquier otra cosa, que puede ser al tocar la parte trasera del equipo.

Baterìa

Una baterìa nueva puede explotar, si no esta instalada correctamente. Remplace la baterìa cuando sea necesario solo con el mismo tipo recomendado por el fabricante de la baterìa. Deshacerse de la baterìa de acuerdo a las instrucciones del fabricante de la baterìa.

FCC warning statement

The Cyclades ACS 5000 advanced 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 ACS 5000 advanced console server models

To comply with FCC standards, the Cyclades ACS 5000 advanced console server requires the use of a shielded CAT 5 cable for the Ethernet interface. Notice that this cable is not supplied with the product and must be provided by the customer.

Canadian DOC notice

The Cyclades ACS 5000 advanced 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'Cyclades ACS 5000 advanced console server n'émete 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.

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.

Avocent

The Power of Being There ®

For Technical Support:

www.avocent.com/support