# BLACK BOX®
# Advanced Console Server
## Installation, Administration, and User's Guide

Software Version 2.6.0

**BLACK BOX® Corporation**
1000 Park Drive
Lawrence, PA 15055-1018
877-877-2269
http://www.blackbox.com
Release Date: December 2005

# Contents

## Chapter 2: Installation and Configuration ............. 29

# Tables

# Figures

# Procedures

# Before You Begin

This installation, administration, and user’s guide provides background information and procedures for installing, configuring, and administering the BLACK BOX® Advanced Console Server and for accessing connected servers and other connected devices.

## Audience

This manual is intended for installers and system administrators of the CS and for users who may be authorized to connect to devices, to manage power through the CS, and to monitor the CS’s temperature.

This document describes configuration, administration, and use of the CS only. It does not describe how to set up and administer other external services or servers that the CS may access for authentication, system logging, IPMI control, SNMP notifications, data logging, file sharing, or other purposes. This document assumes that users who are authorized to connect to servers and other devices through the CS already know how to use the connected devices.

## Document Organization

The document contains the following chapters:

1: Introduction — An overview of the features of the Advanced Console Server and necessary prerequisite information for understanding the rest of the information in this guide.

2: Installation and Configuration

A list of tasks for installing and configuring the Advanced Console Server and connecting devices, with pointers to the needed background information and procedures.

3: Web Manager for Regular Users

Describes how authorized users use the Web Manager to access devices that are connected to ports on the CS.

4: Web Manager for Administrators

Explains how the CS administrator uses the Web Manager to add and delete users, define port access, and perform other common administration tasks.

5: Configuring CS in Wizard Mode

Describes the 6-step procedure to configure the Advanced Console Server in Wizard mode. Selecting a Security Profile, configure network settings, configure serial ports and access, and configure settings such as data buffering and system logging.

6: Configuring the CS in Expert Mode

Provides an introduction to the Expert mode. Describes the forms in each section, and provides a mapping to each form with a link to the desired section.

7: Applications Menu & Forms

Provides an overview of each form associated with the “Applications” menu, describes the functionality of the individual elements in each form, and provides step-by-step configuration procedures.

8: Network Menu & Forms

Provides an overview of each form associated with the “Network” menu, describes the functionality of the individual elements in each form, and provides step-by-step configuration procedures.

9: Security Menu & Forms

Provides an overview of each form associated with the “Security” menu, describes the functionality of the individual elements in each form, and provides step-by-step configuration procedures.

| | |
|---|---|
| 10: Ports Menu & Forms | |
| | Provides an overview of each form associated with the "Ports" menu, describes the functionality of the individual elements in each form, and provides step-by-step configuration procedures. |
| 11: Administration Menu & Forms | |
| | Provides an overview of each form associated with the "Administration" menu, describes the functionality of the individual elements in each form, and provides step-by-step configuration procedures. |
| Appendices | Appendix A provides hardware specifications, and Appendix B details safety information. |
| Index | Provides a way to look up terms. In the online version of this manual, clicking the terms in the index brings you to where they are used in the manual. |

# Related Documents

The following document for the BLACK BOX® Advanced Console Server is shipped with the product.

- Advanced Console Server Quick Start Guide (hard-copy)

# Typographic and Other Conventions

The following table describes the typographic conventions used in BLACK BOX® manuals.

**Table v-1:** Typographic Conventions

| Typeface | Meaning | Example |
|---|---|---|
| Links | Hypertext links or URLs | Go to:<br>http://www.blackbox.com |

**Table v-1:** Typographic Conventions

| Typeface | Meaning | Example |
|---|---|---|
| *Emphasis* | Titles, emphasized or new words or terms | See the Advanced Console Server Quick Start. |
| `Filename or Command` | Names of commands, files, and directories; onscreen computer output. | Edit the `pslave.conf` file. |
| **`User type`** | What you type in an example, compared to what the computer displays | [root] **`ifconfig eth0`** |

The following table describes other terms and conventions.

**Table v-2:** Other Terms and Conventions

| Term or Convention | Meaning | Examples |
|---|---|---|
| Hot keys | • When hot keys are shown with a plus (+) between two or three keys means that they must be pressed at the same time. | • Pressing `Ctrl+p` brings up the IPMI power management. |
| Navigation shortcuts | Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager forms. | Go to Port > Physical Ports> Modify Selected Ports > Power Management |

## *BLACK BOX® firmware Upgrades*

BLACK BOX® offers periodic firmware upgrades for the Advanced Console Server. These upgrades are available free of charge to current BLACK BOX® customers. Visit ftp://ftp.blackbox.com/lan/Term-Servers/ to download the latest firmware.

See “Upgrade Firmware” on page 313 for instructions on how to upgrade the firmware on your Advanced Console Server.

# Introduction

This chapter introduces the Advanced Console Server family of advanced console servers, provides an overview of its features, and briefly describes the features for understanding the information and procedures in the rest of this manual.

# Overview

The Advanced Console Server is a 1U device that serves as a single access point for using and administering servers and other devices. The following figure shows the front of the CS with its two PCMCIA card slots, and the back of a LS1032A with its Serial, Ethernet, and Console ports.

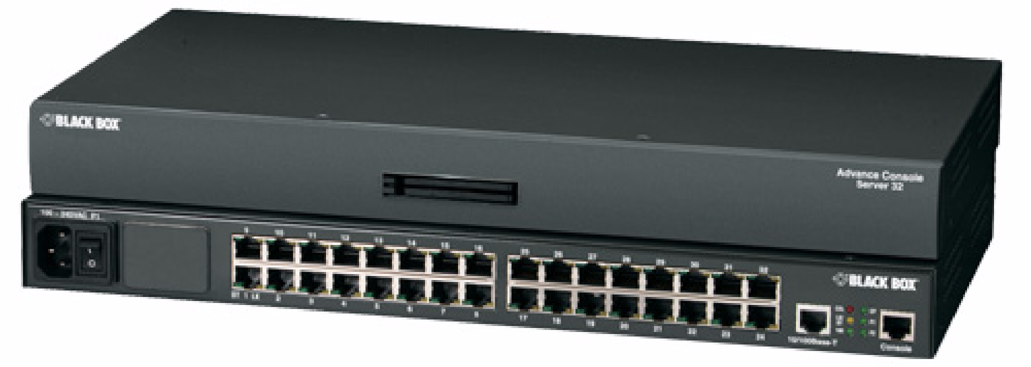


**Figure 1-1:** LS1032A Front and back with PCMCIA Card Slots

# Product Models and Configurations

The following table shows the available configurations. See Appendix A for hardware specifications.

**Table 1-1:** Model Numbers and Configuration Options

| Model Number | Serial Ports |
|---|---|
| **LS1001A** | 1 |
| **LS1004A** | 4 |

**Table 1-1:** Model Numbers and Configuration Options

| Model Number | Serial Ports |
|---|---|
| **LS1008A** | 8 |
| **LS1016A** | 16 |
| **LS1032A** | 32 |
| **LS1048A** | 48 |

The following figure illustrates the BLACK BOX® family of advanced console servers.

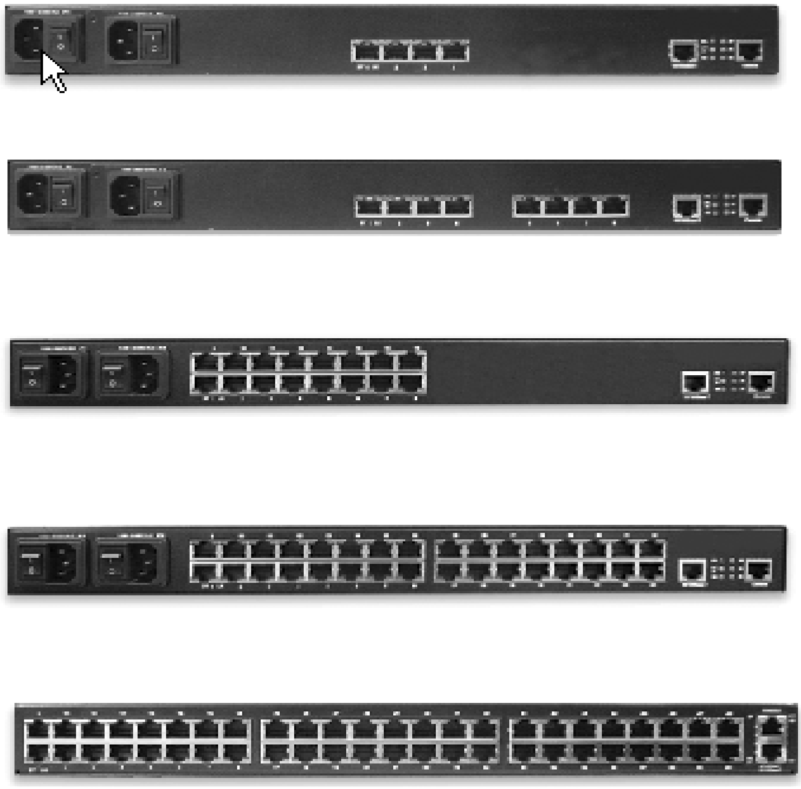


**Figure 1-2:** BLACK BOX® CS family of Advanced Console Servers

# Connectors on the BLACK BOX® CS

The following figure depicts the connectors on the back of a LS1008A.

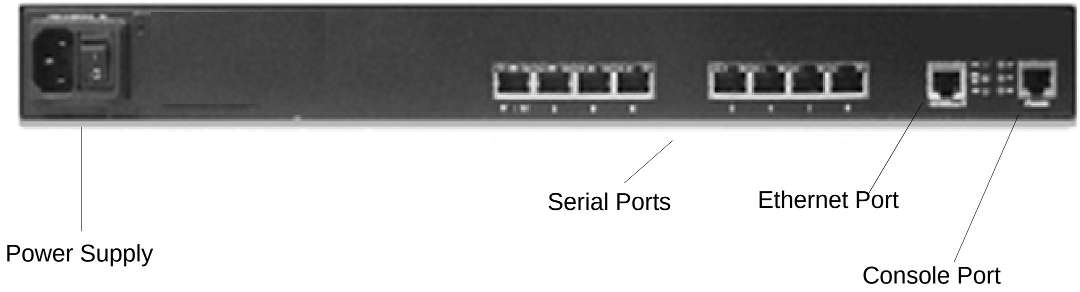


**Figure 1-3:** LS1008A Connectors

The number of serial ports and power supplies depends on the model, see table 1-1 for model numbers and configurations options.

# Accessing CS and Connected Devices

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

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

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

**Note:** If there are cron jobs running through automated scripts, a “root” or “admin” user login can cause the automated cron jobs to fail. Make sure that the users with administrative privileges are aware of this.

# Web Manager

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

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

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

- Through the IP Network.
- Through a dial-in or callback connection with one of the following:
  - An optional external modem connected to one of the serial ports.
  - A modem on an optional PCMCIA modem card.
  - An optional CDMA, GSM, or ISDN card.

# Prerequisites for Using the Web Manager

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

- Basic network parameters must be defined on the CS so the Web Manager can be launched over the network.

  See “Performing Basic Network Configuration Using the wiz Command” on page 38.

- The IP address of the CS must be known.

  When DHCP is enabled, a leased IP address is assigned to CS. The leased IP address may change every time CS reboots. Therefore, an additional step needs to be taken to find out the dynamically-assigned IP address before the Web Manager can be accessed through the browser. Following are three ways to find out the dynamically-assigned IP address:

    - Make an inquiry to the DHCP server on the subnet that the CS resides, using the MAC address (The MAC address is labeled at the bottom of the CS).
    - Connect to CS remotely using Telnet or SSH and use the `ifconfig` command.
    - Connect directly to the CS and use the `ifconfig` command through a terminal emulator application.
- A user account must be defined on the Web Manager.

  By default, the "admin" has an account on the Web Manager. An administrator can add regular user accounts to grant access to the connected servers or devices using the Web Manager.

# Types of Users

CS supports the following user account types:

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

**Note:** It is strongly recommended to change the default password "**bb**" before setting up the CS for secure access to the connected servers or devices.

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

# Security

The Advanced Console Server includes a set of security profiles that consists of predefined parameters to control access to CS 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, which allows the administrator to enable and assign individual ports to users. See "Security Profiles" on page 226 for detailed information and procedures.

# Authentication

CS supports a number of authentication methods that can help the administrator with the 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 fails. In such situations, the CS follows an alternate defined rule when authentication server is down or does not authenticate the user.

The following table lists the supported authentication methods.

**Table 1-2:** CS Supported Authentication Methods

| 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. |

| Authentication Type | Definition |
|---|---|
| **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. |
| **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. |

# VPN

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

You can use the VPN features on CS to create the following types of connections:

- A secure tunnel between CS and a gateway at a remote location so every machine on the subnet at the remote location has a secure connection with CS.
- Create a secure tunnel between CS and a single remote host

To set up a security gateway, you can install IPSec on any machine that does 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 also supported.

For detailed information and procedures to configure a VPN connection, see “VPN Connections” on page 176.

# Packet Filtering on CS

The CS administrator can configure the box 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 which contains a list of chains.
- The chains which contain the rules that control filtering.

## Chain

A chain is a named profile that includes one or more rules that define the following:

- A set of characteristics to look for in a packet
- What to do with any packet that has all the defined characteristics

The CS filter table contains a number of built-in chains. The CS administrator can define additional chains and can edit the built-in chains. The built-in chains are referenced according to the type of packet they handle as shown in the following list:

- INPUT - For incoming packets.
- FORWARD - For packets being routed through CS.
- OUTPUT - For outgoing packets.

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 the following:

- The packet characteristics being filtered.

  The packet is checked for characteristics defined in the rule. For example, a specific IP header, input and output interfaces, TCP flags and protocol.

- What to do when the packet matches the rule.

  The packet can be handled according to a specified target policy such as accepted, dropped, returned, logged, or rejected.

When a packet is filtered, its characteristics are compared against the rules one-by-one. All defined characteristics must match. If no rules are found then the default action for that chain is applied.

Administrators can do the following to specify packet filtering:

- 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:** Filter Options for Packet Filtering Rules

| Filter Options | Description |
|---|---|
| **Source IP and Mask**<br>**Destination IP and Mask** | If you specify a source IP, incoming packets are filtered for the specified IP address. If you specify a destination IP, outgoing packets are filtered for the specified IP address.<br>If you fill in a source or destination mask, incoming or outgoing packets are filtered for IP addresses from the subnetwork in the specified netmask. |
| **Protocol** | You can select a protocol for filtering from one of the following options:<br>• ALL<br>• Numeric Protocol Options<br>• TCP Protocol Options<br>• UDP Protocol Options<br>• ICMP Protocol Options |
| **Input Interface** | The input interface (eth*N*) used by the incoming packet. |
| **Output Interface** | The output interface (eth*N*) used by the outgoing packet. |
| **Fragments** | The types of packets to be filtered:<br>• All packets<br>• 2nd, 3rd... fragmented packets<br>• Non-fragmented and 1st fragmented packets |

You can flag any of the above elements with *inverted* so that 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, 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 Packet Filtering Options

| Field/Menu Option | Definition |
|---|---|
| **Source Port**<br>- OR -<br>**Destination Port** | You can specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. You can also specify a range so that TCP packets are filtered for any port number within the range. |
| **TCP Flags** | Specifying 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, filters TCP packets for the specified flag and the selected condition. |

### *UDP Protocol Options*

When you select UDP as a protocol when specifying a rule, you can select the UDP options defined in the following table.

**Table 1-5:** UDP Protocol Packet Filtering Options

| Field | Definition |
|---|---|
| **Source Port**<br>- OR -<br>**Destination Port** | Specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field.<br>You can specify a source or destination port number for filtering in the “Source Port” field. You can also specify a second number so that UDP packets are filtered for any port number within the range. |

### *ICMP Protocol Options*

When you select ICMP as a protocol when specifying a rule, you can select the following ICMP options.

- all
- echo-reply
- destination-unreachable
- network-unreachable
- host-unreachable
- protocol-unreachable
- port-unreachable
- fragmentation-needed
- source-route-failed
- network-unknown
- host-unknown
- network-prohibited
- host-prohibited
- TOS-network-unreachable
- TOS-host-unreachable
- communication-prohibited
- host-precedence violation

- precedence-cutoff
- source-quench
- redirect
- network-redirect
- host-redirect
- TOS-network-redirect
- TOS-host-redirect
- echo-request
- router-advertisement
- router-solicitation
- time-exceeded
- ttl-zero-during-transit
- ttl-zero-during-reassembly
- parameter-problem
- ip-header-bad
- required-option-missing
- timestamp-request
- timestamp-reply
- address-mask-request
- address-mask-reply

### *Target Actions*

The “Target” is the action to be performed on an IP packet that matches all the criteria specified in a rule. The target actions are:

- ACCEPT
- DROP
- RETURN
- LOG
- REJECT

If the “LOG” and “REJECT” targets are selected, additional options are available.

The following table describes the options for the “LOG” Target.

**Table 1-6:** LOG Target Action Options

| Options | Definition |
|---|---|
| **Log Level** | emerg<br>alert<br>crit<br>err<br>warning<br>notice<br>info<br>debug |
| **Log Prefix** | The prefix to use 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. |

The following list shows the options for the REJECT Target:

- icmp-net-unreachable
- icmp-host-unreachable
- icmp-port-unreachable
- icmp-proto-unreachable
- icmp-net-prohibited
- icmp-host-prohibited
- echo-reply
- tcp-reset

### *Firewall Configuration Procedures*

The following table has links to the procedures for defining packet filtering using the Web Manager.

| | |
|---|---|
| To Add a Chain | Page 199 |
| To Edit a Chain | Page 199 |
| To Add a Rule | Page 200 |
| To Edit a Rule | Page 201 |

# SNMP

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

The following table shows the tasks related to administering SNMP on the CS and provides links to where they are documented.

| | |
|---|---|
| To Configure SNMP | See “To Configure SNMP” on page 184. |
| To configure one or more serial ports to send SNMP traps. | See “SNMP Trap Notifications Entry” on page 302 |

# Notifications, Alarms, and Data Buffering

The CS administrator can setup logging, notifications, and alarms to alert administrators about problems. System generated messages on CS 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 CS’s flash memory, or
- Remotely either on an NFS server or a syslog server.

## *Syslog Servers*

Messages about the CS and connected servers or devices can be sent to a 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 done.

### Prerequisites for Logging to Syslog Servers

Before configuring syslogging, the CS administrator must ensure that syslog server is pre-configured with a public IP address, and it is accessible from CS. The CS administrator must be able to obtain the following information from the syslog server’s administrator.

- The IP address of the syslog server
- The facility number for messages coming from the CS.

  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.

### An Example of Using Facility Numbers

The syslog system administrator sets up a server called “syslogger” to handle log messages from two CS boxes. One CS is located in São Paulo, Brazil, and the other in Fremont, California. The syslog server’s administrator wants to aggregate messages from the São Paulo CS into the `local1` facility, and to aggregate messages from Fremont CS 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.

# Administering Users of Connected Devices

This sections provides a list of task that an CS administrator can perform to enable access to connected devices.

## Planning Access to Connected Devices

The CS administrator needs to perform specific tasks to setup and configure user access to the connected servers, IPDUs, or other devices. An advanced planning can minimize issues that may arise during software configuration.

Some of the planning steps includes the following:

- Create a list of servers or devices to connect to the serial ports.
- Create a list of users with the type of access each user requires.
- Create a matrix of users and required access to each connected server or device.
- Create meaningful aliases to assign to port numbers.
- List all devices that need to be connected to IPDUs and the users who need to access them.

## *Configuring Access to Connected Devices*

During hardware installation of CS, the installer connects the servers, devices, and any IPDUs to the serial ports.

During software configuration, the CS administrator performs the common tasks listed in the following table.

**Table 1-7:** Tasks for Configuring Access to Connected Devices

| Task | Where documented |
|---|---|
| Configure a serial port connection protocol for a console connection | Page 246 |
| Configure user access to serial ports. | Page 261 |
| Configure a serial port for IPDU or IPMI power management | Page 274 |
| Configure a user for IPDU power management | Page 276 |

# CS and Power Management

CS enables users who have power management permissions to power off, power on, and reboot devices. The CS offers the following power management options:

- Remote power management of servers that have IPMI controllers. The CS's implementation of the Intelligent Platform Management Interface (IPMI) protocol lets authorized users manage power for servers that have embedded IPMI controllers. IPMI servers do not need to be connected to the CS because their IPMI controllers respond to out-of-band IPMI commands. Authorized users can also perform IPMI power management of serially-connected devices. The CS uses IPMI V1.5.

- Remote power management of devices that are plugged into an IPDU that is connected to CS
- The intelligent power distribution unit (IPDU) can be an AlterPath PM connected to any serial port. Up to 128 IPDU outlets can be daisy-chained.
- The diagram below shows a typical setup of the CS and an AlterPath PM unit.

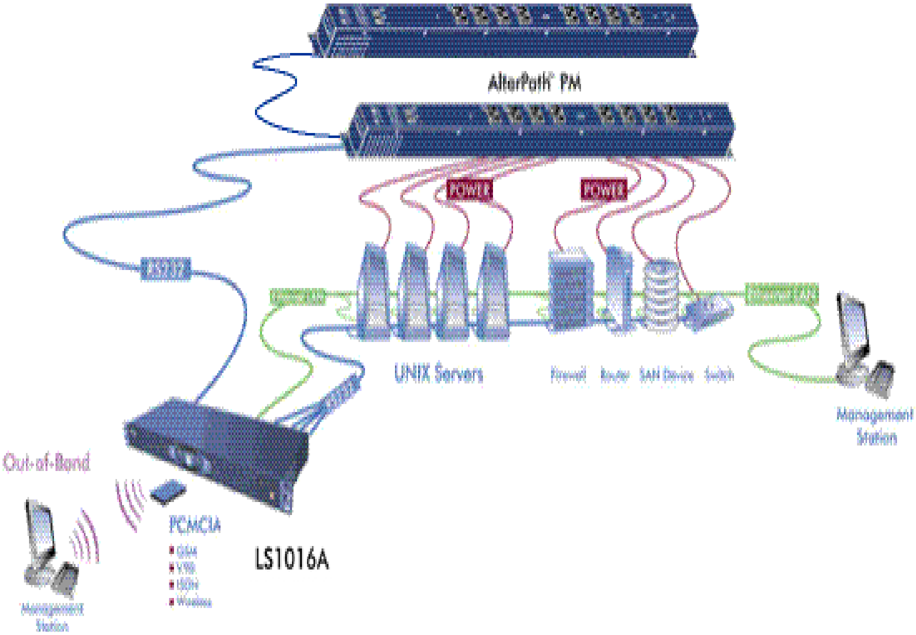


**Figure 1-4:** IPDU Integration With CS

## 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.

The following table list the tasks for power management and where they are described.

Table 1-8: Tasks for Configuring Power Management

| Task | Where Documented |
|---|---|
| Configure users to manage power on IPDUs | “To Configure a User for IPDU Power Management While Connected To a Serial Port” on page 276 |
| Identify servers for IPMI power management | “To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management” on page 142 |
| Configure ports for power management by authorized users | “To Configure a Serial Port for IPDU or IPMI Power Management” on page 274. |

## 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 “hot key” that brings up a power management screen.

For IPMI power management the default hot key is Ctrl+p. For IPDU power management the default hot key is Ctrl+Shift+I.

## Configuring Ports for Power Management Using the CLI

CS administrators can use the `CLI` command with the `config ipmi` options to manage power on IPMI devices while logged into the CS with administrative rights. The `ipmitool` command is documented in the *BLACK BOX® Advanced Console Server Command Reference Guide.*

# *Options for Managing Power*

The sections listed below describe the different ways that the authorized users can perform power management through CS.

- From forms in the Web Manager
- From a power management screen while logged into a device
- From the command line while logged into CS

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 the two power management options listed in the following table, with links to where each is documented.

Table 1-9: Power Management Options in the Web Manager

| Form Name | Where Documented |
|---|---|
| IPDU Power Mgmt | • "IPDU Power Mgmt." on page 120<br>• "To View Status, Lock, Unlock, Rename, or Cycle Power Outlets" on page 123 |
| IPMI Power Mgmt | • "IPMI Power Management" on page 139<br>• "To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management" on page 142<br>• "To Manage Power on an IPMI Device" on page 143 |

## Power Management from the CS Command Line

CS administrators can use the `ipmitool` command to manage power on IPMI devices while logged into the CS with administrative rights. The `ipmitool` command is documented in the *BLACK BOX® Advanced Console Server Command Reference Guide*.

# Chapter 2
# Installation and Configuration

This chapter covers the topics listed in the following table.

The following figure illustrates an example of an CS configured with connected devices.

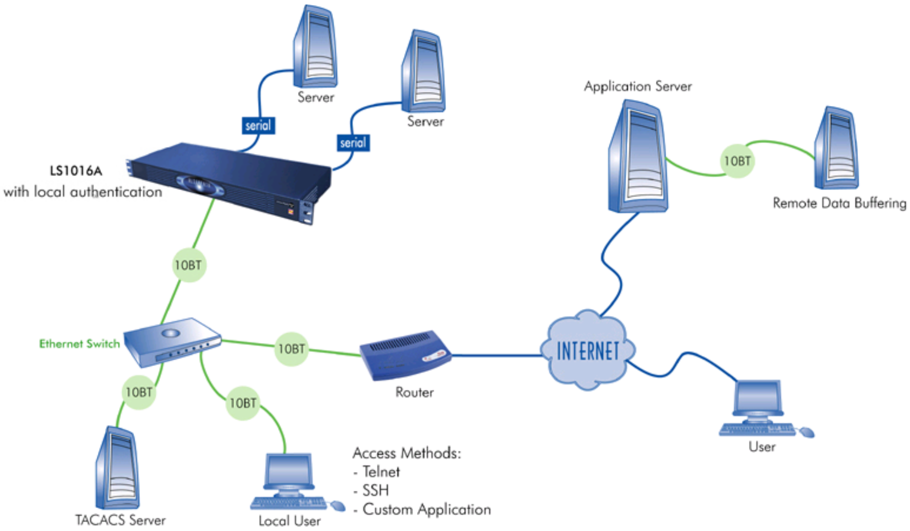


**Figure 2-1:** CS Setup Example

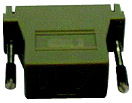
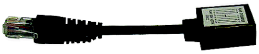
# Shipping Box Contents

The shipping box contains the CS along with the items shown in Table 2-1 and Table 2-2 for CS4 through CS48, and CS1 respectively. The entry for each part provides an illustration, its part number, description, and purpose. You can use checkboxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

The list is numbered for internal cross-referencing among descriptions within this table.

**Table 2-1:** Shipping Box Contents for LS1004A - LS1048A

| R | Item | Description | Purpose |
|---|---|---|---|
| **1.**<br>□ | | Documentation CD | PDF copies of this guide. |

| R | Item | Description | Purpose |
|---|---|---|---|
| **3.**<br>□ | | Power cable. | To connect the CS to a power source. |
| **4.**<br>□ |  | RJ45 to DB25F crossover adapter | To connect the console port to a computer that has a DB-25 male connector. |
| **5.**<br>□ | | RJ45 to DB25M crossover adapter | To connect the console port to a computer that has a DB-25 female connector. |
| **6.**<br>□ | | RJ45 to DB9F crossover adapter | To connect the console port to a computer that has a DB-9 connector. |
| **7.**<br>□ |  | Sun/Netra crossover adapter | To connect the console port to a Sun Netra server, or other devices with the same pinout configuration. |
| **8.**<br>□ | | RJ45 to RJ45 7ft. CAT5 cable | Use for the following:<br>• To connect a device or an IPDU to a serial port.<br>• To connect an Ethernet port to the LAN.<br>• To connect a terminal to a console port. |

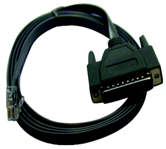
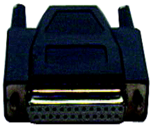
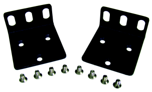
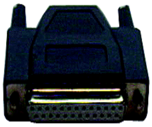
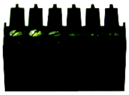
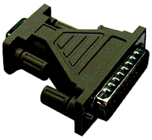
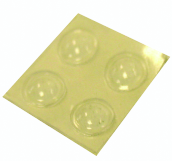
| R | Item | Description | Purpose |
|---|---|---|---|
| 9.<br>□ |  | RJ45 to DB25M straight-thru cable | Use for modems and other DCE devices. |
| 10.<br>□ |  | DB25F Loopback | Use to test and diagnose serial ports. |
| 11.<br>□ |  | 2 - Mounting brackets with<br>10 - screws (2 spares) | Use to mount the CS to a rack or cabinet. |

**Table 2-2:** Shipping Box Contents for LS1001A

| R | Item | Description | Purpose |
|---|---|---|---|
| 1.<br>□ | | Documentation CD | PDF copies of this guide. |
| 3.<br>□ | | RJ45 to DB9F crossover adapter | To connect the console port to a computer that has a DB-9 connector. |
| 4.<br>□ |  | DB25F Loopback | Use to test and diagnose serial ports. |
| 5.<br>□ |  | 3.5mm Block Plug | Use to establish RS-485 connection. |
| 6.<br>□ |  | DB9F to DB25M adapter | Use to convert serial port connectors. |
| 7.<br>□ |  | Bumpon Protect Pads | Adhesive pads to protect and stabilize CS1. |

| | | | |
|---|---|---|---|
| **8.**<br>□ | | RJ45 to RJ45 7ft. CAT5 cable | Use for the following:<br>• To connect a device or an IPDU to a serial port.<br>• To connect an Ethernet port to the LAN.<br>• To connect a terminal to a console port. |
| **9.**<br>□ | | DB9F to DB25F crossover cable | To connect the RS-232 serial port to a computer that has a DB-25 male connector. |
| **10.**<br>□ | | Power Supply<br>+5V/2.5A | Power supply. |
| **11.**<br>□ | | Power Cable 6ft. 2-Pin | To connect the CS to a power source. |

# Important Pre-installation Requirements

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

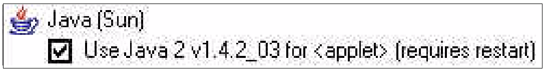
- Root Access on your local UNIX machine in order to use the serial ports.
- An appropriate Terminal application for your operating system.
- IP address, DNS, Network Mask, and Gateway addresses of your server or terminal, the CS, and the machine that CS is connected to.
- A web browser that supports the CS Web Manager, such as Netscape, Internet Explorer 6.0, Firefox, or Mozilla.
- Java 2 Runtime Environment (JRE) version 1.4.2 or later. J2RE can be downloaded from http://java.com.

# Java Plug-In Requirement for Serial Port Access

The JRE version 1.4.2 or later must be installed for a user to be able to access a serial port using the Java applet viewing window. After you download and install J2RE version 1.4.2 or later, check your browser configuration to see if the Java plug-in is configured with your browser.

## ▼ *To check Java Plug-in Support in the Browser*

1. To check Internet Explorer on Windows, do the following steps.
   - **a.** Go to Tools > Internet Options > Advanced
   - **b.** Scroll down and look for a section on Java.
   - **c.** There should be a check box that says “Use Java 2 v1.4.2...." As shown in the following figure.



Java (Sun)

☑ Use Java 2 v1.4.2_03 for <applet> (requires restart)

   - **d.** If an option similar to the above figure does not appear, it means that JRE is not installed on your system. Or, if the option appears, but the checkbox is not enabled, this means your browser is not activated to use the Java plug-in that came with JRE.
2. To check Netscape or Mozilla on Windows, do the following steps.
   - **a.** Go to Edit > Preferences >Advanced.
   - **b.** Check the “Enable Java” checkbox.
   - **c.** To see what version of the Java plug-in is registered, do the following steps.
     - **i.** Go to Help > About Plug-ins.
     - ii. Scroll to the Java Plug-in section.
     - iii. Check whether the registered Java plug-in is the same as the version you installed.

## ▼ *To Install JRE Version 1.4.2 or later and Register the Plug-in*

1. Make sure that JRE 1.4.2 or later is installed on the computer.

If needed, download the JRE from http://java.com. The web site automatically checks your configuration and installs the latest version of JRE if one is not available.

2. If JRE is already installed on your system and you just want to activate your browser, do the following steps.
   a. Go to your system's Control Panel > Java Plug-in > Browser
   b. Enable the browser(s) for Java Plug-in.
   c. Test your browser(s) to see if the correct Java Plug-in is being used.

# Basic Installation Procedures

The following table lists the basic installation tasks in the order in which they should be performed and shows the page numbers where the tasks are described in more detail.

**Table 2-3:** CS Basic Installation Tasks

| Task | Where Documented |
|---|---|
| Mount the CS | "Mounting the CS" on page 35 |
| Make an Ethernet connection | "Making an Ethernet Connection" on page 35 |
| Connect servers and other devices to be managed through the CS | "Connecting Servers and Other Devices to CS" on page 36 |
| Make a direct (terminal) connection to prepare CS for basic network configuration | "Making a Direct Connection to Configure the Network Parameters." on page 37 |
| Power on the CS and the connected devices | "Powering on the CS and the Connected Devices" on page 37 |
| Perform basic network configuration | "Performing Basic Network Configuration Using the wiz Command" on page 38 |
| Select a security profile using the web manager | "Selecting A Security Profile Using the Web Manager" on page 43 |

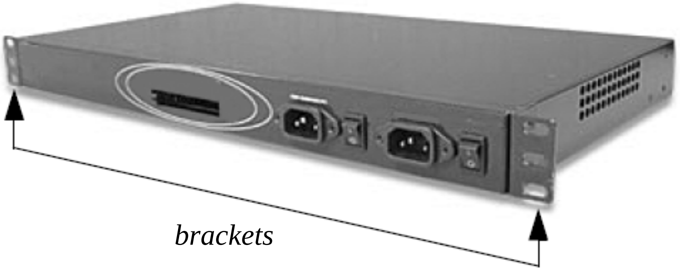
# Mounting the CS

You can mount the CS 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 CS for mounting. See item 14 in the shipping content section.

- If you are not mounting the CS, place the unit on a desk or table.
- If you are rack-mounting the CS, obtain a hex screwdriver and appropriate nuts and bolts before starting the following procedure.

### ▼ To rack-mount CS, perform the following steps:

1. Install the brackets on to the front or back edges of the box using a screw driver and the screws provided with the mounting kit.



2. Mount the CS box in a secure position.

**Note:** To ensure safety refer to Appendix B: Safety Guidelines.

# Making an Ethernet Connection

You can use the RJ-45 straight-through cable and the appropriate adapter provided in the product box to assemble a console cable. All adapters have an RJ-45 connector on one end and either a DB25 or DB9 male or female connector on the other end.

### ▼ *To Make an Ethernet Connection*

1. Connect the RJ-45 end of the cable to the port labeled “Console” on the CS.
2. Connect the adapter end of the cable to the console port of your server or device.
3. Connect a patch cable from the CS port labeled 10/100Base-T to an Ethernet hub or switch.

## *Connecting Servers and Other Devices to CS*

The following sections describes the recommended preparation for connecting servers or devices to CS.

- Make sure the configuration on servers or devices to be connected are completed.
- Work with the administrator of the servers or devices to ensure all the following prerequisites are met:
  - All devices are installed and fully configured.
  - User accounts exist for the users who need access to the server or device.
  - If a device is to use remote authentication, make sure that the authentication servers are installed and fully configured
  - You have obtained from the server’s administrator the information (IP address and other method-specific information), which you need to configure the authentication server on the CS.

### ▼ *To Connect Devices to Serial Ports*

Using patch cables with RJ-45 connectors and DB-9 console adapters assemble crossover cables to connect the CS serial ports to the device’s console port.

**Note:** After CS is installed make sure to specify the desired authentication method to CS and the serial ports that each device is connected to. See “Authentication” on page 214 for more information on configuring authentication to CS, and “Physical Ports” on page 239 for detail information on configuring the serial ports.

## Making a Direct Connection to Configure the Network Parameters.

Perform the following steps to connect a terminal or a computer to the console port of the CS. This procedure assumes you know how to use a terminal or terminal emulation program.

On a PC, ensure that HyperTerminal or another terminal emulation program is installed on the Windows operating system. On a computer 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

1. Install and launch your serial communication software on a terminal or a computer. For example, if you are using a PC, use HyperTerminal to perform the initial configuration of the CS directly through your PC's COM port.
2. Open HyperTerminal. Start > All Programs > Accessories > Communications > HyperTerminal
3. Start a New Connection session, select an available COM port, and enter the following console parameters.
   - Bits per second: 9600 bps
   - Data bits: 8 bits
   - Parity: None
   - Stop bit: 1
   - Flow control: None

## Powering on the CS and the Connected Devices

Do the following procedures in the order shown to avoid problems with components on connected devices.

### ▼ To Power on the CS

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

**Note:** If your CS model 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 Power On Connected Devices*

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

## *Configuring the Network Parameters*

In preparation to make CS available on the network, collect the following information from your system administrator and proceed with the network configuration procedure.

- Hostname
- An IP address for CS
- Domain name
- DNS IP address
- Gateway IP address
- Network mask
- NTP server’s IP address (if you are using a time/date server)

### Performing Basic Network Configuration Using the wiz Command

The following procedure assumes that a hardware connection is made between the CS’s console port and the COM port of a computer.

### ▼ *To Log Into CS Through the Console*

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

```
CS login: root
Password: bb
```

**Note:** It is strongly recommended to change the default password “**bb**” before setting up the CS for secure access to the connected servers or devices.

### ▼ *To Change the root password*

**1.** Enter the **`passwd`** command.

```
[root@CAS root]# passwd
```

**d.** Enter a new password when prompted.

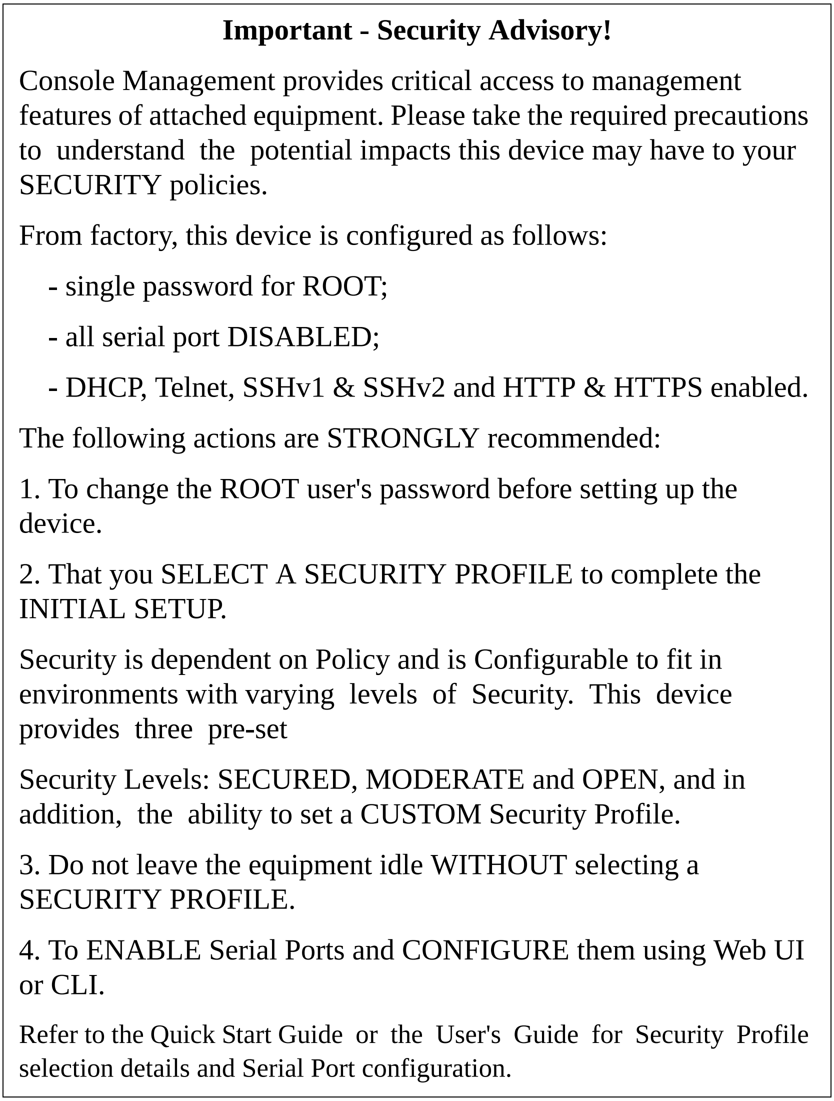
```
New password: new_password

Re-enter new password: new_password

Password changed
```

The following Security Advisory appears the first time CS is powered on, or when the unit is reset to factory default parameters.

**Figure 2-2:** Security Advisory Console Message



**Important - Security Advisory!**

Console Management provides critical access to management features of attached equipment. Please take the required precautions to understand the potential impacts this device may have to your SECURITY policies.

From factory, this device is configured as follows:

- single password for ROOT;

- all serial port DISABLED;

- DHCP, Telnet, SSHv1 & SSHv2 and HTTP & HTTPS enabled.

The following actions are STRONGLY recommended:

1. To change the ROOT user's password before setting up the device.

2. That you SELECT A SECURITY PROFILE to complete the INITIAL SETUP.

Security is dependent on Policy and is Configurable to fit in environments with varying levels of Security. This device provides three pre-set

Security Levels: SECURED, MODERATE and OPEN, and in addition, the ability to set a CUSTOM Security Profile.

3. Do not leave the equipment idle WITHOUT selecting a SECURITY PROFILE.

4. To ENABLE Serial Ports and CONFIGURE them using Web UI or CLI.

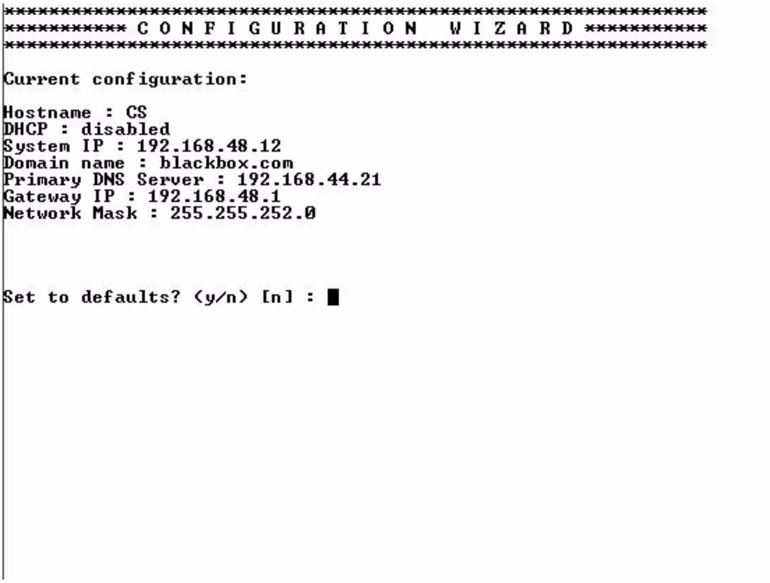
Refer to the Quick Start Guide or the User's Guide for Security Profile selection details and Serial Port configuration.

### ▼ *To Use the wiz Command to Configure Network Parameters*

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

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

As shown in the sample screen below, the system brings up 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 ***********
***************************************************************

Current configuration:

Hostname : CS
DHCP : disabled
System IP : 192.168.48.12
Domain name : blackbox.com
Primary DNS Server : 192.168.44.21
Gateway IP : 192.168.48.1
Network Mask : 255.255.252.0



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

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

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

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

```
Hostname [CAS]: fremont_branch_CS
```

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

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

5. To change the default static IP address, see your network administrator to obtain a valid IP address.

   ```
   System IP[192.168.160.10]: CS_IP_address
   ```

6. Enter the domain name.

   ```
   Domain name[blackbox.com]: domain_name
   ```

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

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

8. Enter the IP address for the gateway.

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

9. Enter the netmask for the subnetwork.

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

   The network configuration parameters appear.

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

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

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

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

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

12. After the initial configuration proceed to the Web Manager to select a security profile.

**Note:** To use the Web Manager, ask your system administrator for the CS's IP address. CS may be set up with a static IP address at your site. By default, CS uses the IP address provided by the DHCP server. If your network does not use DHCP, then CS 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 CS in a supported browser.

**Note:** Once you login to the Web Manager, a Security Profile must be selected in order to further configure CS using the Web Manager. For this reason your browser redirects to Wizard > Step1: Security Profiles.

### ▼ *To Select 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 all services, Telnet, SSHv1, SSHv2, HTTP, HTTPS, SNMP, RPC, ICMP and Telnet, SSH and Raw connections to Serial Ports.
- **Default:** Sets the profile to the same configuration as Moderate.
- **Custom:** Enable or disable individual protocols and services, and configure access to ports.

For detailed information on Security Profiles see "Security Profiles" on page 226.

The administrator can perform the following tasks using the Web Manager.

- Administer CS 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*

### Enabling Ports and Assigning Users.

**Note:** From the factory, CS 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 detailed information on managing users and ports see Appendix 9, “Security Menu & Forms" and Appendix 10, “Ports Menu & Forms".

For additional configuration and administration options, and other important related information, see the chapters in the CS user manual that are listed in the following table.

| **Topic** | **Where Documented** |
|---|---|
| Installation and Configuration Process. | Appendix 2, “Installation and Configuration" |
| For Regular Users - How to use the Web Manager to access servers and connected devices. | Appendix 3, “Web Manager for Regular Users" |
| Web Manager in Wizard Mode. | Appendix 5, “Configuring CS in Wizard Mode" |
| Web Manager in Expert Mode. | Appendix 6, “Configuring the CS in Expert Mode" |

# Other Methods of Accessing the Web Manager

You can access the Web Manager using one of the following methods.

**Note:** The following methods require additional setup and configuration, which could be specific to your site's network configuration.

- Using DHCP
- Using the default IP address

## ▼ *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 that is currently assigned to CS.

1. Mount the BLACK BOX® CS.
2. Connect computers and other devices to be managed through the CS.
3. Power on the CS and connected devices.
4. Obtain the CS's current IP address.
5. Enter the CS's IP address in the browser's Address window.
6. Login to the CS 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 CS is `192.168.160.10.` This procedure assumes that you are able to temporarily change the IP address of a computer that is on the same subnet as the CS.

1. On a computer that resides on the same subnet as the CS, change the network portion of the IP address of that computer to `192.168.160`.

   For example, you could change the computer's IP address to `192.168.160.44`. For the host portion of the IP address, you can use any number except `10`, `0`, or `255`.

2. Bring up a browser on the computer whose address you changed, enter the CS’s default IP address, `http://192.168.160.10` to bring up the Web Manager, and log in.

# Installing PCMCIA Cards

The front panel of the CS has two PCMCIA card slots as shown in the following figure. You can insert and configure one card in each of the slots. See Appendix C, “Supported PCMCIA Cards".

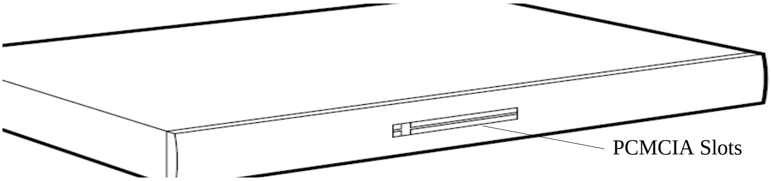


**Figure 2-3:** Front Panel PCMCIA Card Slots

## ▼ *To Install a PCMCIA Card*

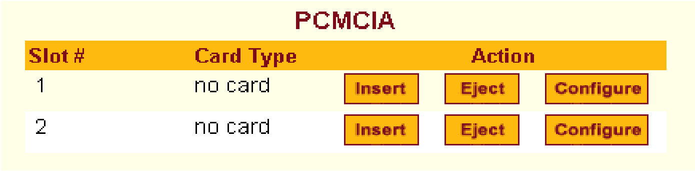
1. Insert the PCMCIA card into slot 1 or slot 2.
2. Use the Web Manager to configure the PCMCIA card.

**Note:** A hard disk PCMCIA card is automatically mounted once it is inserted, and it needs no configuration.

## ▼ *To Remove a PCMCIA Card*

**Caution:** Always use the Web Manager to eject a PCMCIA card. Any other method may cause a kernel panic.

1. Eject the card by using the Eject button on the Web Manager’s PCMCIA Management form, Expert > Network > PCMCIA Management > Eject



PCMCIA

| Slot # | Card Type | Action | | |
|---|---|---|---|---|
| 1 | no card | Insert | Eject | Configure |
| 2 | no card | Insert | Eject | Configure |

**Figure 2-4:** PCMCIA Eject Button in Web Manager

**2.** Physically remove the card from the slot.

### ▼ *To Configure a PCMCIA Card*

See Chapter 8, “To Configure a PCMCIA Card”, and the sections related to the type of card you need to configure.

## Connecting AlterPath PM IPDUs

You can connect AlterPath Power Management (PM) intelligent power distribution units (IPDUs) to the serial ports on the CS using an RJ-45 to RJ-45 UTP cable. AlterPath PM includes two RS-232 outlets for serial management and daisy-chaining. Any combination of Alter PM models up to 128 outlets can be daisy-chained into a single virtual power distribution unit.

The following figure shows an CS and two AlterPath PM8 IPDUs daisy-chained. One PM is connected to a serial port on CS configured for power management, and a second PM is daisy-chained from the first PM.

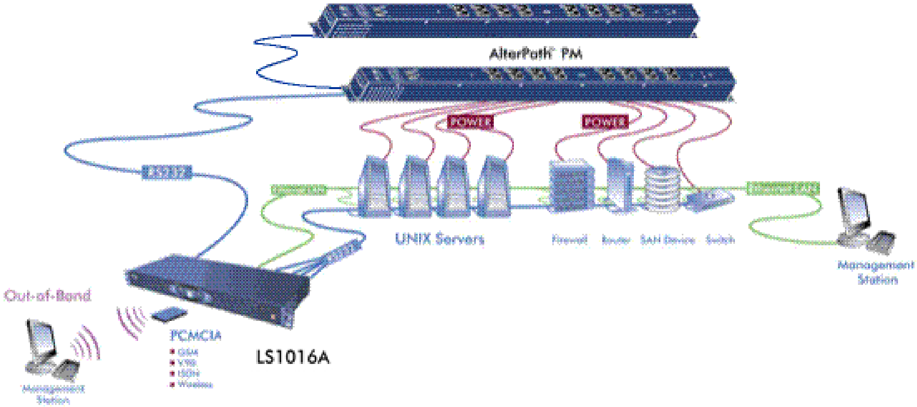


**Figure 2-5:** AlterPath PMs Connected to the CS

The following table lists the related tasks on connecting IPDU units and managing power.

**Table 2-4:** Tasks Related to Connecting AlterPath PMs

| Task | Where Documented |
|---|---|
| Configure serial ports for power management protocol. | "To Configure a Serial Port for IPDU or IPMI Power Management" on page 274 |
| How the administrators perform IPDU power management using the Web Manager | "IPDU Power Mgmt." on page 120 |
| How the regular users manager power outlets using the Web Manager | "To Close an SSH Session" on page 56 |
| Connect the AlterPath PM to the CS unit, and daisy-chain multiple PM units. | "To Daisy-Chain AlterPath PMs to the CS" on page 48 |
| Configure users for IPDU power management | "To Configure Users to Manage Power Outlets on IPDUs" on page 128 |
| Configure servers for IPMI power management while connected. | "To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management" on page 142 |

## ▼ *To Daisy-Chain AlterPath PMs to the CS*

This procedure assumes that you have one AlterPath PM connected to a serial port on the CS.

1. Connect one end of a UTP cable with RJ-45 connectors to the "OUT" port of the AlterPath PM that is connected to the serial port on CS.
2. Connect the other end of the cable to the "IN" port of the next AlterPath PM.
3. Repeat Steps 1 and 2 until you have connected the desired number of AlterPath PMs.

# Chapter 3
# Web Manager for Regular Users

This chapter describes the requirements and the procedures for “Regular Users” to use the Web Manager. Regular users are those who have configured accounts on the CS with limited access rights.

Regular users can perform the following tasks using the Web Manager.

- Access computers and devices that are connected to the serial ports on the CS.
- Perform IPDU power management.
- Change their current password.

This chapter contains the following sections.

## Using the Web Manager

CS users perform most tasks through the Web Manager. The Web Manager runs in a browser and provides a real-time view of all the equipment that is connected to the CS.

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

## ▼ *Logging in to the Web Manager*

1. Connect your web browser to CS by typing in the Console Access Server's IP address (*e.g.*, https://10.10.10.10) provided to you by your system administrator in your internet browser.

**Note:** Refer to Chapter 2, " for the requirements to start with the Web Manager.

Press **`Enter`**.

The system brings up the CS Web Manager Login form.

2. Type in your username and password as provided to you by your system administrator.

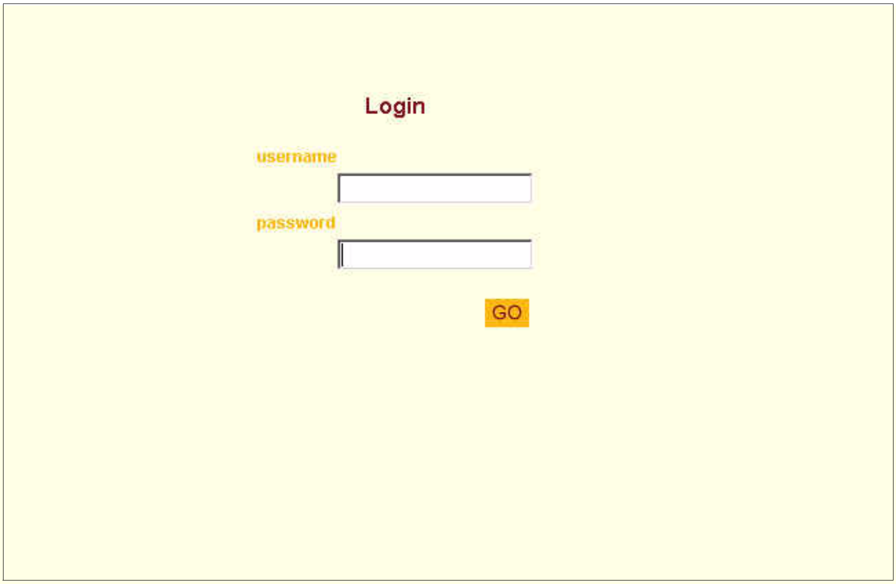
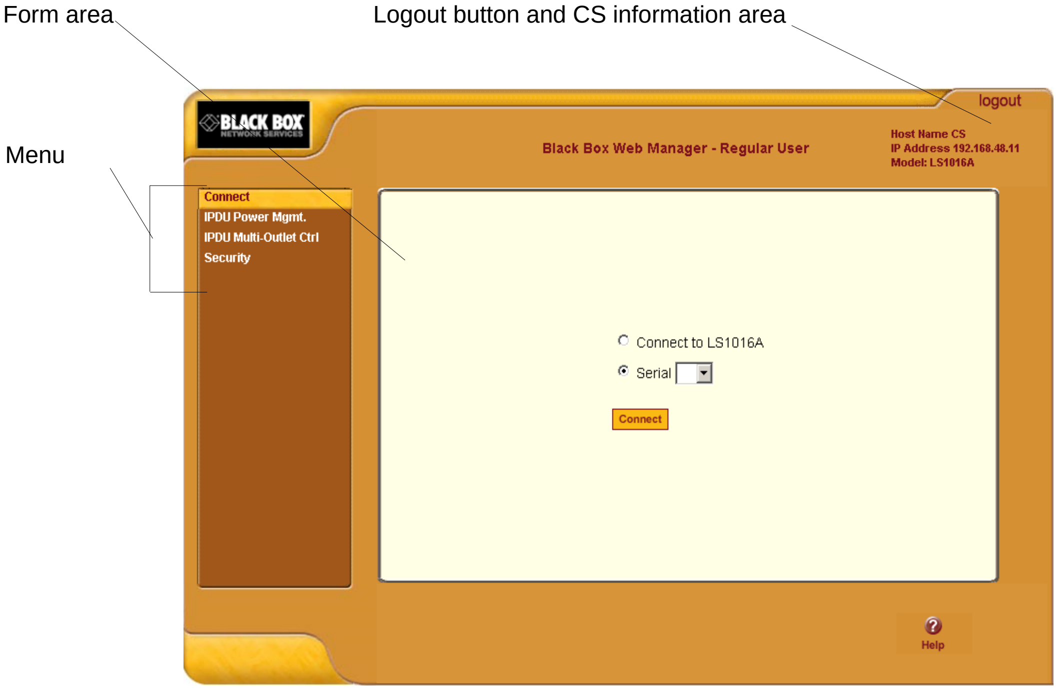


**Figure 3-1:** Regular User > Web Manager Login form

# Features of Regular User Forms

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



Black Box Web Manager - Regular User

Host Name CS
IP Address 192.168.48.11
Model: LS1016A

○ Connect to LS1016A

● Serial

**Figure 3-2:** Regular User Form

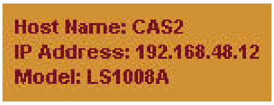
The form in the middle changes according to which menu option is selected.

The following table illustrates the functions that are common to all the forms.

**Table 3-1:** Common Screen Information

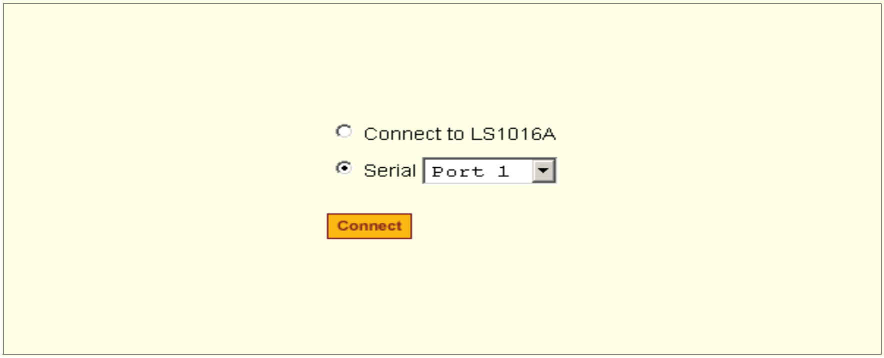
| Form Area | Purpose |
|---|---|
| logout | Click this button to log out. |

**Table 3-1:** Common Screen Information (Continued)

| Form Area | Purpose |
|---|---|
| <br>Host Name: CAS2<br>IP Address: 192.168.48.12<br>Model: LS1008A | Displays the hostname and IP address assigned during initial configuration, and the model number of the CS. |
| <br>Help | Brings up the online help. |

# Connect

When you select the “Connect” option, the following form appears.



○ Connect to LS1016A

● Serial Port 1

Connect

**Figure 3-3:** Regular User > Connect Form

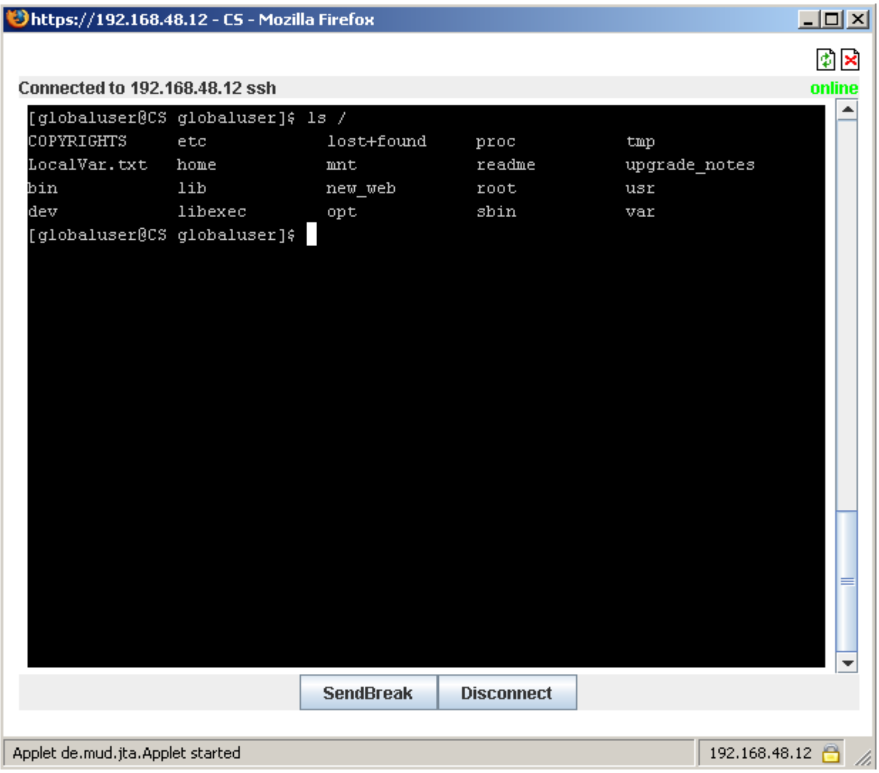
You can use this form to connect to the CS console, or to one of the serial ports as described in the following sections.

- “Connect to CS” on page 53
- “Connect to Serial Ports” on page 54

Permission to access a port or perform power management is granted by the CS administrator when your user account is created. Contact your administrator to gain authorization to access the serial port that the server or devices is connected to.

## Connect to CS

When you click the “Connect to CS” radio button on the “Connect” form, a Java applet viewer appears running an SSH session on the CS. The following figure shows the Java applet when you connect to the CS. Note in the “Connected to” message in the below figure at the top of the screen the IP address of the CS followed by the session type, in this case “SSH”.



https://192.168.48.12 - CS - Mozilla Firefox

Connected to 192.168.48.12 ssh

```
[globaluser@CS globaluser]$ ls /
COPYRIGHTS     etc            lost+found     proc           tmp
LocalVar.txt   home           mnt            readme         upgrade_notes
bin            lib            new_web        root           usr
dev            libexec        opt            sbin           var
[globaluser@CS globaluser]$
```

Applet de.mud.jta.Applet started

**Figure 3-4:** Java Applet

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 |

**Table 3-2:** (Continued)Java Applet Buttons

| Button | Purpose |
|---|---|
| Disconnect | To disconnect from the Java applet |
| 🔄 ✖ | Select the left icon to reconnect to the server or device; or select the right icon to end the session and disconnect from the Java applet. |

## Connect to Serial Ports

The list of serial ports includes the port names or administrator-defined aliases only for ports you have permission to access. If the list is empty or does not include a port you need to access, contact the CS system administrator.

### 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 CS is required. Your system administrator can help with authorization to specific CS ports that your server or device is connected to.

**Note:** If an authentication server is setup in your network, an authentication method and the related parameters should be setup to allow access to the connected devices. Consult your system administrator for configuring the authentication method.

When you select a port from the Serial pull-down list and click the Connect button, a Java applet viewer appears. A “Connected to” message in a gray area at the top of the screen shows the IP address of the CS followed by the TCP port number. See an example of the Java applet in Figure 3-4

## 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. There are a number of connection protocols for the serial ports, which your system administrator can setup depending on your requirements.   The following table shows the protocols the CS administrator can choose for the serial ports.

**Table 3-3:** Serial Ports Connection 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 increments up to the number of serial ports that your CS unit has. For example, an CS with 8 serial ports have TCP ports 7001 through 7008. The CS administrator may change the default port numbers, so if you use the defaults and they fail, check with the administrator to find which port numbers to use.

### ▼ *To Use Telnet to Connect to a Device Through a Serial Port*

For this procedure, you need the hostname of the CS 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 CS or its IP address.

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

```
ssh -l username:TCP_port_number CS_IP_address
```

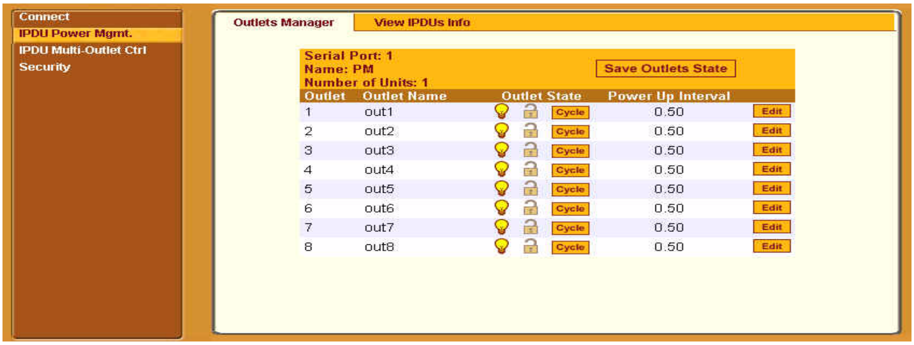
### ▼ *To Close an SSH Session*

Enter the hotkey defined for the SSH client followed by a dot “.”. The default is “~.”

**Note:** Make sure you enter the escape character followed by a “.” at the beginning of a line to close the SSH session.

## IPDU Power Mgmt.

IPDU or “Intelligent Power Distribution Units” management allows you to manage the power outlets on the AlterPath PM products. When you select the “IPDU Power Mgmt.” option, if you have permission to manage outlets on an AlterPath PM, two tabs appear at the top of the form, as shown in the following figure, “Outlets Manager” and “View IPDUs Info”.



Serial Port: 1
Name: PM
Number of Units: 1

| Outlet | Outlet Name | Outlet State | Power Up Interval | |
|---|---|---|---|---|
| 1 | out1 | 💡 🔓 Cycle | 0.50 | Edit |
| 2 | out2 | 💡 🔓 Cycle | 0.50 | Edit |
| 3 | out3 | 💡 🔓 Cycle | 0.50 | Edit |
| 4 | out4 | 💡 🔓 Cycle | 0.50 | Edit |
| 5 | out5 | 💡 🔓 Cycle | 0.50 | Edit |
| 6 | out6 | 💡 🔓 Cycle | 0.50 | Edit |
| 7 | out7 | 💡 🔓 Cycle | 0.50 | Edit |
| 8 | out8 | 💡 🔓 Cycle | 0.50 | Edit |

**Figure 3-5:** Regular User > IPDU Power Mgmt. Forms

You can access the forms under IPDU Power Mgmt. menu to manage outlets, or view IPDUs information:

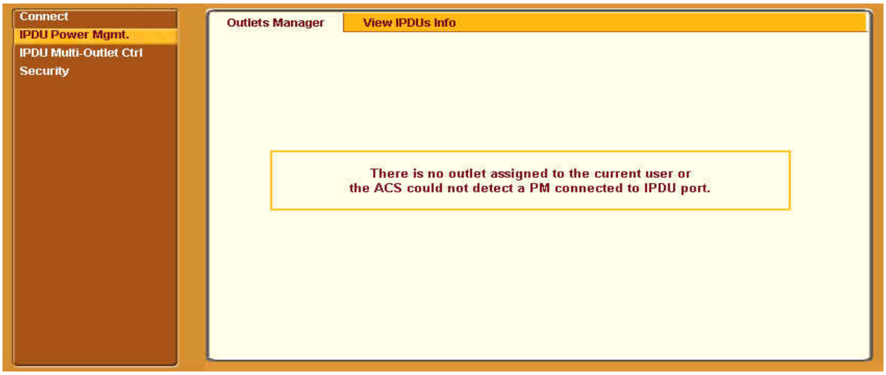
## Outlets Manager

When you go to IPDU Power Mgmt.>Outlets Manager tab, the message shown in the following figure appears if,

1- You do not have permission to manage power on any of the AlterPath PM outlets or,

2- CS cannot detect an AlterPath PM that has been configured for power management.

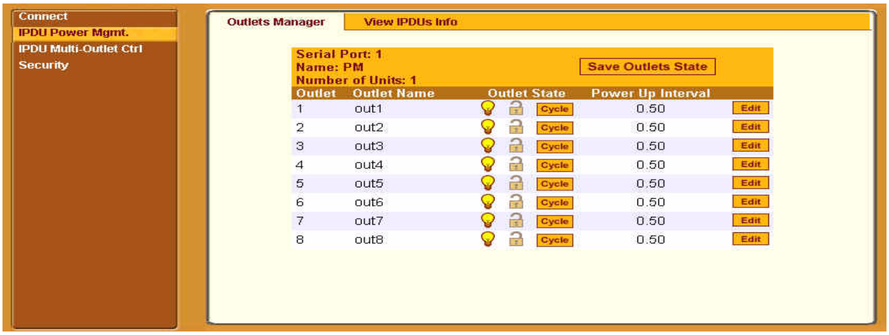
Contact the CS administrator for help, if you see this message.



There is no outlet assigned to the current user or
the ACS could not detect a PM connected to IPDU port.

**Figure 3-6:** Regular User > Outlets Manager (no permissions)

The following form appears if you have permission to manage power on one or more outlets of the AlterPath PM.



Serial Port: 1
Name: PM
Number of Units: 1

| Outlet | Outlet Name | Outlet State | Power Up Interval | |
|---|---|---|---|---|
| 1 | out1 | Cycle | 0.50 | Edit |
| 2 | out2 | Cycle | 0.50 | Edit |
| 3 | out3 | Cycle | 0.50 | Edit |
| 4 | out4 | Cycle | 0.50 | Edit |
| 5 | out5 | Cycle | 0.50 | Edit |
| 6 | out6 | Cycle | 0.50 | Edit |
| 7 | out7 | Cycle | 0.50 | Edit |
| 8 | out8 | Cycle | 0.50 | Edit |

**Figure 3-7:** Regular User > Outlets Manager (with permissions)

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 do the following for any listed outlet:

- Edit the outlet name.

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

- Edit the power up interval.

  The power up interval is the time interval (in seconds) that the system waits between turning on the currently-selected outlet and the next outlet. The default is set at 30 seconds.

- 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.

The following table describe the corresponding buttons to do the above operations:

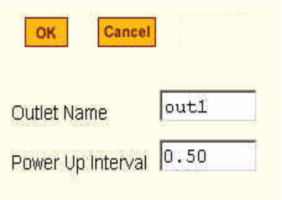
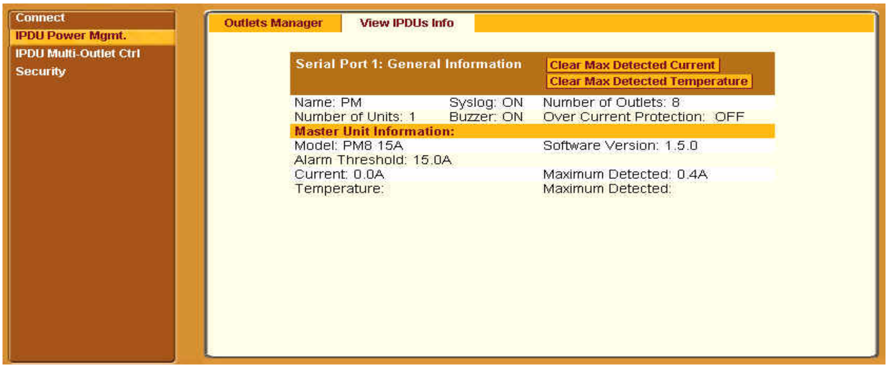
| Button | Purpose |
|---|---|
| Edit | Opens a dialog box to<br>Edit an Outlet name, and the Power Up Interval.<br><br>OK Cancel<br>Outlet Name: out1<br>Power Up Interval: 0.50 |
| Cycle | Turn power briefly off and then on again. |
| 💡 💡 | Turn power On/Off. |
| 🔒 🔓 | Lock or unlock the outlet. |

**Table 3-4:** Regular User > Outlet Management Buttons

## View IPDUs Info

When you go to IPDU Power Mgmt.>View IPDUs Info, the form appears as shown in the following figure.



Serial Port 1: General Information

Name: PM    Syslog: ON    Number of Outlets: 8
Number of Units: 1    Buzzer: ON    Over Current Protection: OFF

Master Unit Information:

Model: PM8 15A    Software Version: 1.5.0
Alarm Threshold: 15.0A
Current: 0.0A    Maximum Detected: 0.4A
Temperature:    Maximum Detected:

**Figure 3-8:** Regular User > View IPDUs Info

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

**Table 3-5:** Regular User > Information on the View IPDUs Info Form

| | Description | Example |
|---|---|---|
| **Name** | Either a default name or administrator-configured name. | PM |
| **Number of Units** | The number of IPDUs connected to the port. The first IPDU is referred to as the master. Any other IPDUs daisy-chained off the first IPDU are referred to as slaves. | 1 |
| **Syslog** | Whether syslogging has been configured for messages from this IPDU. | ON |
| **Buzzer** | Whether a buzzer has been configured to sound when a specified alarm threshold is exceeded. | ON |
| **Number of Outlets** | Total number of outlets on all connected IPDUs. | 8 |

**Table 3-5:** Regular User > Information on the View IPDUs Info Form

| | **Description** | **Example** |
|---|---|---|
| **Over Current Protection** | Whether over current protection is enabled (to prevent outlets from being turned on if the current on the IPDU exceeds the specified threshold). | OFF |

| | **Description** | **Example** |
|---|---|---|
| **Model** | AlterPath PM model number | PM8 15A |
| **Software Version** | PM firmware version | 1.5.0 |
| **Alarm Threshold** | Number of amperes that triggers an alarm or syslog message if it is reached | 15.0A |
| **Current** | Current level on the IPDU | 0.0A |
| **Maximum Detected** | Maximum current detected | 0.4A |
| Clear Max Detected Temperature | Use this button to refresh the currently displayed maximum detected temperature. | |
| **Temperature** | Temperature on the AlterPath PM *(Available only on selected models that have temperature sensors)* | |
| **Maximum Detected** | Maximum temperature detected *(Available only on selected models that have temperature sensors)* | |
| Clear Max Detected Current | Use this button to refresh the currently displayed maximum detected current. | |

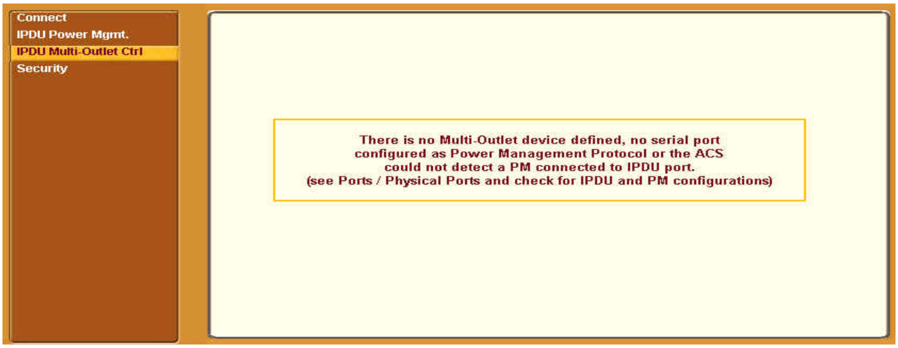
# IPDU Multi-Outlet Ctrl

Selecting IPDU Multi-Outlet Control form allows you to view and manage the power on a group of outlets that provide power to a multi power supply server or device connected to a serial port. Whether the outlets that the multi power supply device is connected to are on the same PM or not, the outlets can be grouped together and managed simultaneously from this form.

When you select IPDU Multi-Outlet Ctrl form, the following figure appears if,

1. There is no multi-outlet device defined.
2. Power Management is not enabled for the serial port the device is connected to.
3. CS cannot detect an AlterPath PM that has been configured for power management.

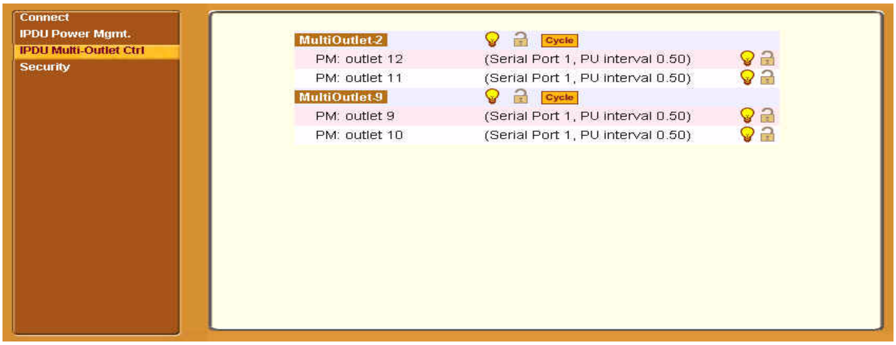
Contact the CS administrator for help, if you see this message.



There is no Multi-Outlet device defined, no serial port configured as Power Management Protocol or the ACS could not detect a PM connected to IPDU port.
(see Ports / Physical Ports and check for IPDU and PM configurations)

**Figure 3-9:** Regular User > IPDU Multi-Outlet (no permissions)

The following form appears if you have permission to view and control the outlets that a multi power supply server or device is connected to.



| | |
|---|---|
| MultiOutlet-2 | |
| PM: outlet 12 | (Serial Port 1, PU interval 0.50) |
| PM: outlet 11 | (Serial Port 1, PU interval 0.50) |
| MultiOutlet-9 | |
| PM: outlet 9 | (Serial Port 1, PU interval 0.50) |
| PM: outlet 10 | (Serial Port 1, PU interval 0.50) |

**Figure 3-10:** Regular User > IPDU Multi-Outlet (with permissions)

Notice in the above figure that the first line of each group, the light bulb, the lock icon, and the Cycle button operate over the entire group. The light bulb and lock icons next to the individual outlets are used to display the status of each outlet but cannot be used to control the individual outlets.

The following table describes the icons in the first line of each group.

**Table 3-6:** Regular User > IPDU Multi-Outlet Ctrl. Form Icons

| Button | Purpose |
|---|---|
| 💡 💡 | A grey light bulb icon indicates that the group is off.<br>A yellow light bulb indicates that the group is on.<br>Clicking the light bulb icon changes the power status of all of the outlets in the group. |
| 🔒 🔓 | A grey and open lock icon indicates that the outlets are unlocked and can be powered on or off.<br>A full-color and closed lock icon indicates that the outlet is locked and cannot be turned on or off.<br>Clicking the lock icon changes the lock status of all of the icons in the group. |
| Cycle | Turn power briefly off and on again |

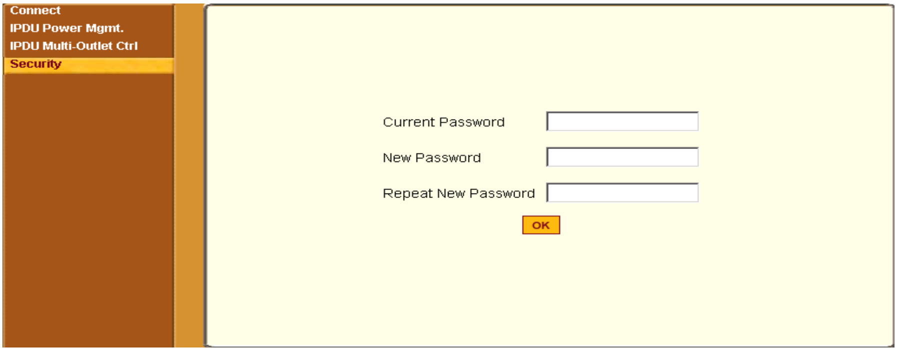
**Note:** Only one outlet needs to be powered on or unlocked in order for the entire group to be considered on or unlocked respectively. In this case, it takes two clicks to turn the power off or to lock the entire group instead of the one click, when all of the outlets are in the same state. The first click turns the other outlets on or unlocks them so that all the outlets are in the same state; the second click turns all of the outlets off or locks them.

The Cycle button operates only if all outlets of a group are turned on.

**Note:** The “PU (Power Up) interval" parameter configured for each outlet plays an important role in the power up sequence of multi-outlet devices. The next outlet in the group turns on only after the power up interval specified for the current outlet has elapsed. This parameter can be configured through the IPDU Power Mgmt. form. See “To Close an SSH Session” on page 56.

# Security

When you select the “Security” menu option, the following form appears.



Current Password

New Password

Repeat New Password

.

**Table 3-7:** Regular User > Password Management Form

### ▼ *To Change Your Password*

1. Select the “Security” option from the menu panel.

   The “Security” form appears.

2. Enter your current password in the “Current Password” field.
3. Enter the new password in the “New Password” and the “Repeat New Password” fields.
4. Click OK.
5. Log out and log in using your new password to verify your password change.

# Chapter 4
# Web Manager for Administrators

## Overview

This chapter is for system administrators who use the Web Manager to configure the CS and its users. For information on how to configure CS using vi or Command Line Interface (CLI), please consult the *BLACK BOX® CS Installation, Administration, and User's Guide*.

The CS Web Manager for administrators describes two modes of operation, Wizard and Expert.

This chapter provides an overview of the Web Manager forms. The subsequent chapters describe the menus, forms, and the configuration procedures of the Web Manager in Wizard and Expert modes. If you are a regular user see Chapter 3, “Web Manager for Regular Users”.

The sections listed in the following table provides background information related to CS administrators’ use of the Web Manager, including explanations of the types of information to be entered in each of the forms, and links to all the procedures performed in each mode.

# BLACK BOX® Web Manager

CS administrators perform most tasks through the BLACK BOX® Web Manager either locally or from a remote location. The Web Manager provides a real-time view of the equipment that is connected to the CS.

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

Access to the Web Manager can be through any of the following methods:

- Through an Ethernet protocol network.
- Through a dial-up protocol such as:
  - An optional modem connected to one of the serial ports.
  - An optional modem card inserted into one of the PCMCIA slots.
  - An optional CDMA wireless, GSM, or ISDN card.

## *Prerequisites for Using the Web Manager*

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

- Basic network parameters must be defined on the CS so the Web Manager can be launched over the network.
- The IP address of the CS must be known.

**Note:** If DHCP is enabled on CS, the IP address is not fixed. Anyone wanting to access the CS must find out the currently-assigned IP address each time. If DHCP is enabled and you do not know how to find out the current IP address of the CS, contact your system administrator for help.

- A user account must be defined on the Web Manager.

  By default, the “root” has an account on the Web Manager. An administrator with “root” access can add regular user accounts to access connected devices.

# Common Tasks for CS Administrators

The following table shows some of the common tasks that are performed by an administrator and links to the process and procedure for performing the task.

**Table 4-1:** Administrator > Common Administrative Tasks

| **Task** | **Where Documented** |
|---|---|
| Set up users and groups to access connected devices. | "Users and Groups" on page 208 |
| Set up user authentication to access serial ports. | "Access" on page 259 |
| Configure serial ports for power management. | "To Configure a Power Management Protocol for an IPDU" on page 254 |
| Assign users permissions to manage outlets on connected AlterPath PMs. | "To Configure Users to Manage Power Outlets on IPDUs" on page 128 |
| Set up local or remote data buffering, and specify alarms for one or more serial ports. | "To Configure Data Buffering for Serial Ports" on page 267<br>"To Choose a Method for Sending Notifications for Serial Port Data Buffering Events" on page 297 |
| Set up logging of system messages to a syslog server. | "To Specify Names, Alarms, Syslogging, and Over Current Protection for IPDUs" on page 130<br>"To Configure Syslogging for Serial Ports and Specify Message Filtering" on page 158" |
| Configure devices for IPMI power management. | "IPMI Power Management" on page 139 |
| Select an authentication method for accessing connected devices. | "Authentication" on page 214 |
| Configure packet filtering. | "Firewall Configuration" on page 186 |

# Common Features of Administrator Forms

The common features of all Web Manager forms for CS administrators are described in the following sections.

- Buttons and CS Information
- Getting more information

## *Buttons and CS Information*

The following figure shows the control buttons that display at the bottom of the form when the logged in user is an administrator.

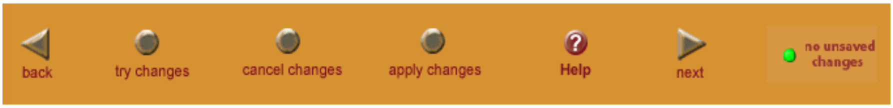


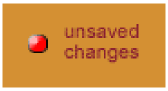
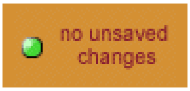
**Figure 4-1:** Administrator > Web Manager Buttons

The following table describes the uses for each control button.

**Table 4-2:** 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 all unsaved changes. |
| reload page | Reloads the page. |
| Help | Brings up the online help. |
| next | Only appears in Wizard mode. Goes to the next form. |

**Table 4-2:** Administrator > Web Manager Buttons

| Button Name | Use |
|---|---|
|  | 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. |
|  | The no unsaved changes button appears and a graphical LED appears in green when no changes have been made that need to be saved. |

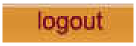
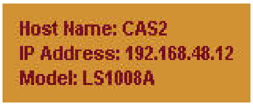
The various Web Manager actions for trying, saving, and restoring configuration changes are summarized in the following table.

**Table 4-3:** Administrator > Options for Trying, Saving, and Restoring Configuration Changes

| 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 4-4:** Administrator > Logout Button and Other Information in the Upper Right

| Form Area | Purpose |
|---|---|
| <br>logout | Click this button to log out. |
| <br>Host Name: CAS2<br>IP Address: 192.168.48.12<br>Model: LS1008A | Displays the hostname, IP address assigned during initial configuration, and the model number of the Advanced Console Server. |

# Logging Into the Web Manager

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

## ▼*To Log Into the Web Manager*

**1** To bring up the Web Manager, enter the IP address of the CS in the address field of your browser. For example, http://192.168.48.11

**Note:** Devices such as CS are usually assigned a static IP addresses. If DHCP is enabled, you must find out the dynamically-assigned IP address each time you need to run the Web Manager. Finding a dynamically-assigned IP address requires making an inquiry to the DHCP server using the MAC address (a 12-digit hexadecimal number, which is on a label on CS). Check with the system administrator who configured the basic network parameters on the assigned IP address. If there is no DHCP server, use the default static IP address 192.168.160.10 that is pre-configured in the CS.

a. If DHCP is disabled, use a static IP address assigned by the administrator.

b. If DHCP is enabled, enter the dynamically-assigned IP address.

The Login page appears.

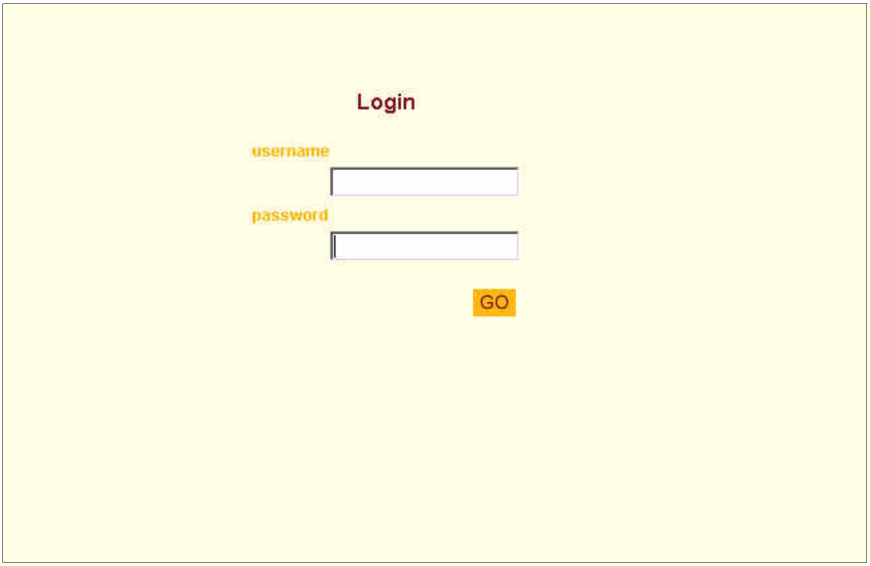
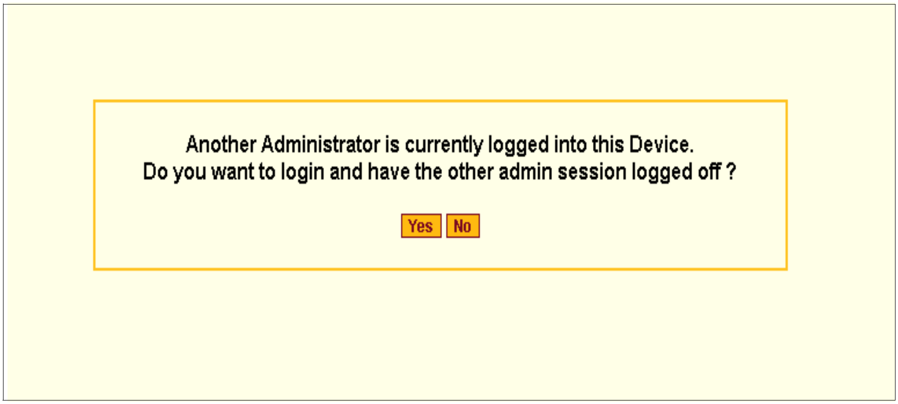


**Figure 4-2:** Administrator > Web Manager Login Form

2. Log in as “**root”** and type in the root password. The default password is “**bb”.**

**Caution:** It is important to change the “root” password as soon as possible to avoid security breaches.

If another administrator is already logged in, the dialog box shown in the following screen example appears.

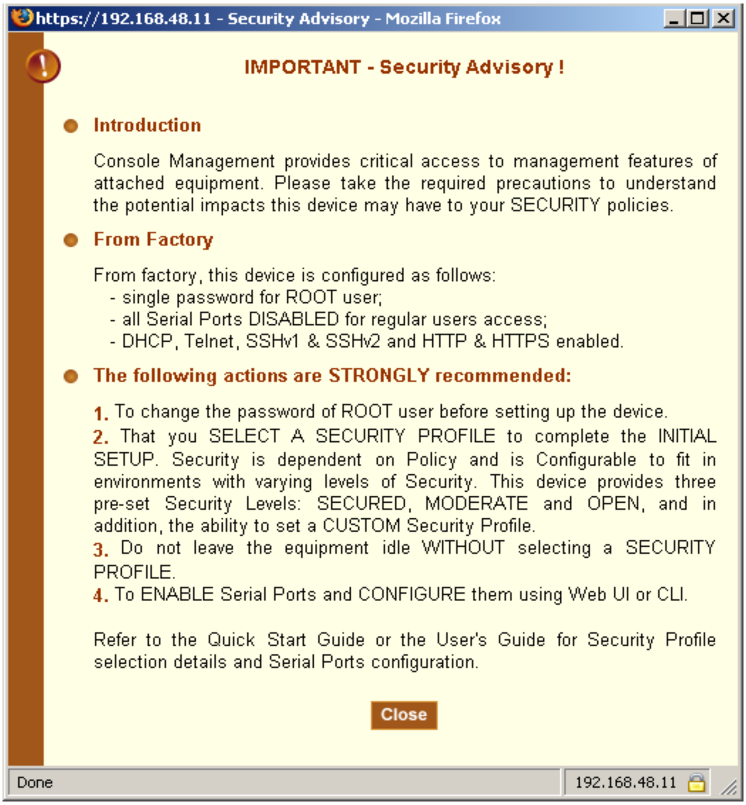


Another Administrator is currently logged into this Device.
Do you want to login and have the other admin session logged off ?

**Figure 4-3:** Administrator > Multi Administrator Login Message

**3** Click the appropriate radio button and then click Apply.

**Note:** The following Security Advisory appears the first time CS is accessed. Browser’s pop-up blocker should be disabled for this dialog box to appear.



IMPORTANT - Security Advisory !

- Introduction

Console Management provides critical access to management features of attached equipment. Please take the required precautions to understand the potential impacts this device may have to your SECURITY policies.

- From Factory

From factory, this device is configured as follows:
- single password for ROOT user;
- all Serial Ports DISABLED for regular users access;
- DHCP, Telnet, SSHv1 & SSHv2 and HTTP & HTTPS enabled.

- The following actions are STRONGLY recommended:

1. To change the password of ROOT user before setting up the device.
2. That you SELECT A SECURITY PROFILE to complete the INITIAL SETUP. Security is dependent on Policy and is Configurable to fit in environments with varying levels of Security. This device provides three pre-set Security Levels: SECURED, MODERATE and OPEN, and in addition, the ability to set a CUSTOM Security Profile.
3. Do not leave the equipment idle WITHOUT selecting a SECURITY PROFILE.
4. To ENABLE Serial Ports and CONFIGURE them using Web UI or CLI.

Refer to the Quick Start Guide or the User's Guide for Security Profile selection details and Serial Ports configuration.

**Figure 4-4:** Administrator > Security Advisory Message

# Overview of Administrative Modes

The CS Web Manager operates in two modes:

1. Wizard
2. Expert

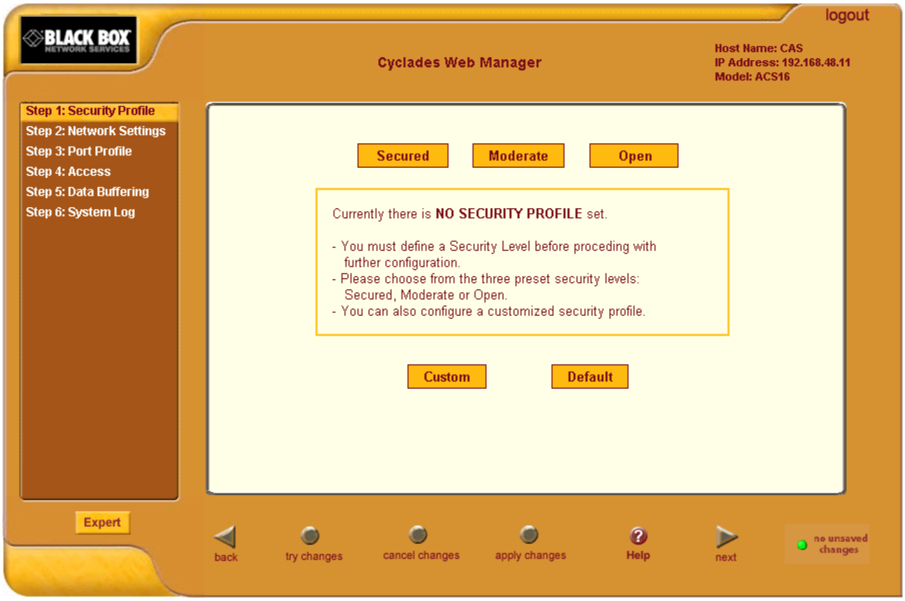
| | |
|---|---|
| | In Wizard mode, the Expert button displays. In Expert mode, the Wizard button displays. Clicking these buttons toggles between Wizard and Expert mode. Expert is the default mode. |

## 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 CS as an administrator or as a user with administrative privileges, by default the system point to Expert Mode>Ports>Ports Status form. To change to the Wizard Mode, click on the “Wizard” button located in the left bottom corner of the menu panel.

Shown below is a typical form of the CS web interface in Wizard Mode. The user entry form varies depending on the selected menu item.



Host Name: CAS
IP Address: 192.168.48.11
Model: ACS16

Currently there is NO SECURITY PROFILE set.

- You must define a Security Level before proceding with further configuration.
- Please choose from the three preset security levels: Secured, Moderate or Open.
- You can also configure a customized security profile.

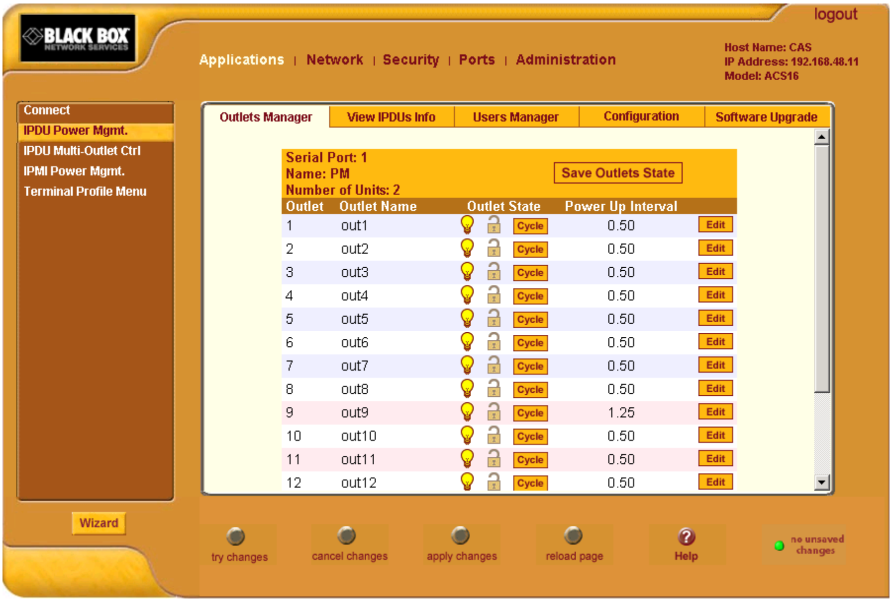
**Figure 4-5:** Example of Web Manager Form in Wizard Mode

## Expert Mode

Designed for advanced users, this is the default mode when you log in to the CS. If you are in the “Wizard” mode, you can change to “Expert” mode by clicking on the “Expert' button at the left bottom corner of the menu panel.

Shown below is a typical CS 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, which are identified by tabs such as the one shown in Figure 4-6.



Host Name: CAS
IP Address: 192.168.48.11
Model: ACS16

Serial Port: 1
Name: PM
Number of Units: 2

| Outlet | Outlet Name | Outlet State | | | Power Up Interval | |
|---|---|---|---|---|---|---|
| 1 | out1 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 2 | out2 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 3 | out3 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 4 | out4 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 5 | out5 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 6 | out6 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 7 | out7 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 8 | out8 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 9 | out9 | 💡 | 🔓 | Cycle | 1.25 | Edit |
| 10 | out10 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 11 | out11 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 12 | out12 | 💡 | 🔓 | Cycle | 0.50 | Edit |

**Figure 4-6:** Example of Web Manager Form in Expert Mode

The subsequent chapters shown below describe the Wizard and Expert configuration modes in detail, introduces the menu elements in the "Expert" mode, and describe the underlying procedures.

**Table 4-5:** Administrator > CS Configuration and Expert Menus Chapters

| | |
|---|---|
| Configuring the CS in Wizard Mode | Chapter 5 |
| Configuring the CS in Expert Mode | Chapter 6 |
| Applications Menu [Expert] | Chapter 7 |
| Network Menu [Expert] | Chapter 8 |

**Table 4-5:** Administrator > CS Configuration and Expert Menus Chapters

| | |
|---|---|
| Security Menu [Expert] | Chapter 9 |
| Ports Menu [Expert] | Chapter 10 |
| Administration Menu [Expert] | Chapter 11 |

# Chapter 5
# Configuring CS in Wizard Mode

There are six configuration steps displayed in the menu panel of the Web Manager in Wizard mode. The following table lists the sections where the steps are described.

| | |
|---|---|
| Step 1: Security Profile | Page 77 |
| Step 2: Network Settings | Page 85 |
| Step 3: Port Profile | Page 88 |
| Step 4: Access | Page 91 |
| Step 5: Data Buffering | Page 96 |
| Step 6: System Log | Page 101 |

## *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 that are active at any time.

### Pre-defined Security Profiles

There are three pre-defined security profiles:

1. 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 “allow root access” option.

2. 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.
3. 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 sets the parameters to same as *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 user’s custom requirements

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

**Table 5-1:** Wizard > Enabled services to access the CS under each security profile.

| Access to CS | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| Telnet | | | ✓ | | User Configurable |
| SSHv1 | | ✓ | ✓ | ✓ | |
| SSHv2 | ✓ | ✓ | ✓ | ✓ | |
| Allow SSH root access | | ✓ | ✓ | ✓ | |
| HTTP | | ✓ | ✓ | ✓ | |
| HTTPS | ✓ | ✓ | ✓ | ✓ | |
| HTTP redirection to HTTPS | | ✓ | | ✓ | |

1-The *Default* security profile parameters are the same as Moderate profile.

**Table 5-2:** Wizard > Enabled services to access the serial ports under each security profile.

| Access to Serial Ports | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| Console (Telnet) | | ✓ | ✓ | ✓ | User Configurable |
| Console (SSH) | ✓ | ✓ | ✓ | ✓ | |
| Console (Raw) | | ✓ | ✓ | ✓ | |
| Serial Port Authentication | ✓ | | | | |
| Bidirect (Dynamic Mode Support) | | ✓ | ✓ | ✓ | |

1-The *Default* security profile parameters are the same as Moderate profile.

**Table 5-3:** Wizard > Enabled protocols for each security profile shown with a check mark.

| Other Services | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| SNMP | | | ✓ | | **User Configurable** |
| RPC | | | ✓ | | |
| ICMP | | ✓ | ✓ | ✓ | |
| FTP | | | | | |
| IPSec | | | | | |

[1] -The *Default* security profile parameters are the same as Moderate profile.

The first step in configuring your Advanced Console Server is to select a Security Profile. One of the following situations is applicable when you boot the CS unit.

1. CS is starting for the first time, or after a reset to factory default.

   In this situation when you boot CS and login 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 apply the changes, CS Web Manager restarts for the security configuration to take effect.

2. CS firmware is upgraded and the system is restarting with the new firmware.

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

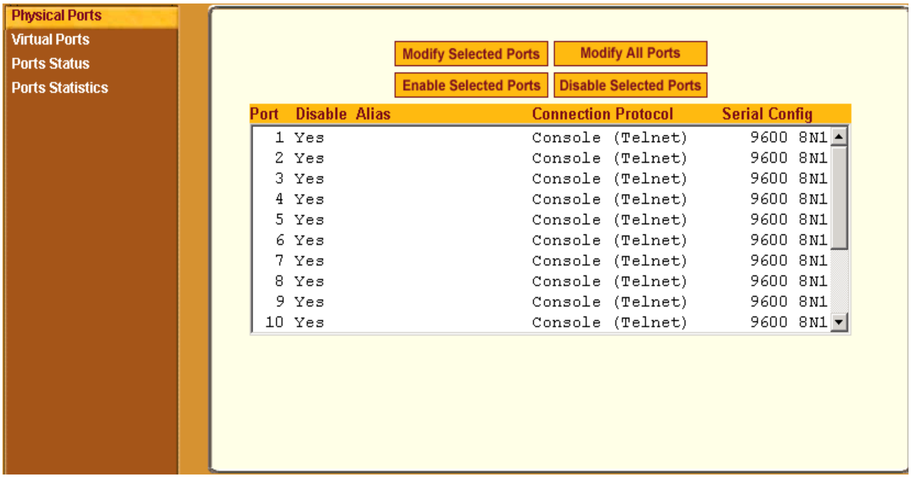
3. CS is restarting normally.

   In this situation CS detects the pre-defined security profile. You can continue working in the Web Manager.

## Serial Port Settings and Security Profiles

All serial ports on CS units 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 figure shows the default factory settings of serial ports.

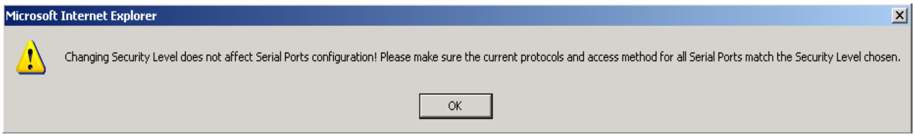


| Port | Disable | Alias | Connection Protocol | Serial Config |
|---|---|---|---|---|
| 1 | Yes | | Console (Telnet) | 9600 8N1 |
| 2 | Yes | | Console (Telnet) | 9600 8N1 |
| 3 | Yes | | Console (Telnet) | 9600 8N1 |
| 4 | Yes | | Console (Telnet) | 9600 8N1 |
| 5 | Yes | | Console (Telnet) | 9600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

**Figure 5-1:** Administrator > Physical Ports Factory Settings

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.

The following reminder dialog box appears before you proceed to Step2: Network Setting.



Changing Security Level does not affect Serial Ports configuration! Please make sure the current protocols and access method for all Serial Ports match the Security Level chosen.

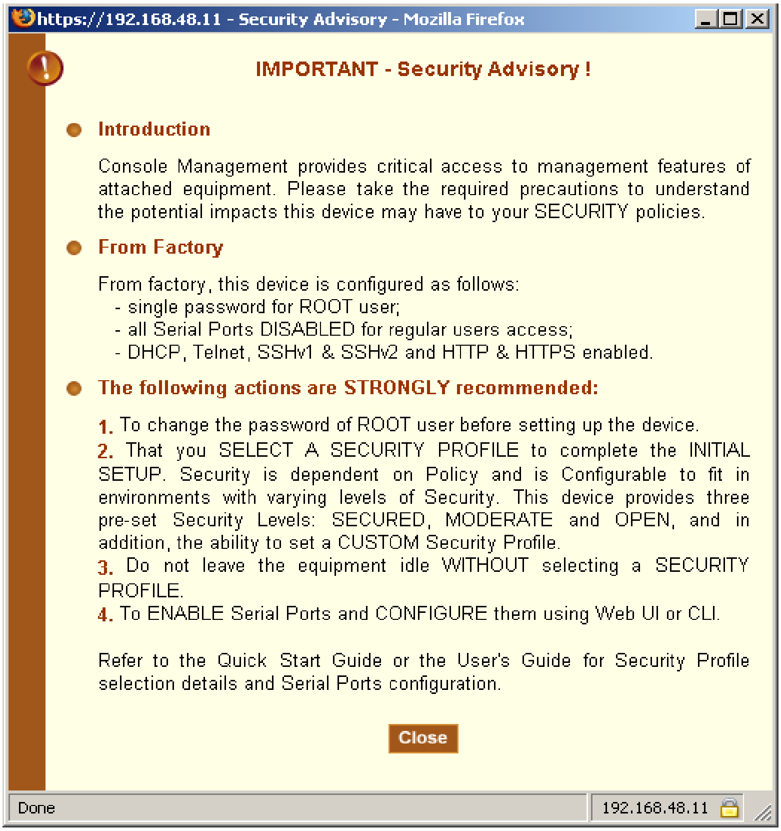
**Figure 5-2:** Security and Serial Ports Configuration Alert

## ▼ *To Select or Configure a Security Profile*

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

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

   The following security warning dialog box appears.



IMPORTANT - Security Advisory !

- Introduction

  Console Management provides critical access to management features of attached equipment. Please take the required precautions to understand the potential impacts this device may have to your SECURITY policies.

- From Factory

  From factory, this device is configured as follows:
   - single password for ROOT user;
   - all Serial Ports DISABLED for regular users access;
   - DHCP, Telnet, SSHv1 & SSHv2 and HTTP & HTTPS enabled.

- The following actions are STRONGLY recommended:

  1. To change the password of ROOT user before setting up the device.
  2. That you SELECT A SECURITY PROFILE to complete the INITIAL SETUP. Security is dependent on Policy and is Configurable to fit in environments with varying levels of Security. This device provides three pre-set Security Levels: SECURED, MODERATE and OPEN, and in addition, the ability to set a CUSTOM Security Profile.
  3. Do not leave the equipment idle WITHOUT selecting a SECURITY PROFILE.
  4. To ENABLE Serial Ports and CONFIGURE them using Web UI or CLI.

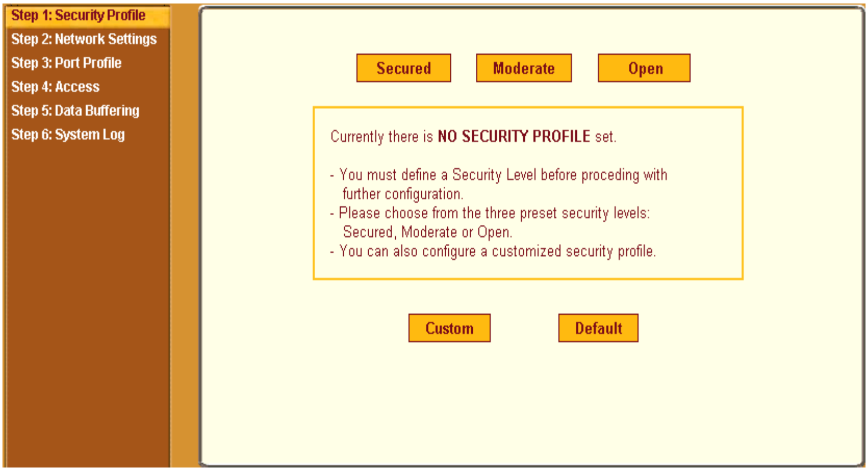
  Refer to the Quick Start Guide or the User's Guide for Security Profile selection details and Serial Ports configuration.

**Figure 5-3:** Security Advisory Dialog Box

**Note:** Your browser's pop-up blocker should be disabled for this dialog box to appear.

2. Review the Security Advisory and click the "Close" button.
3. The Web Manager is redirected to Wizard > Step 1: Security Profile.

   The following form is displayed.



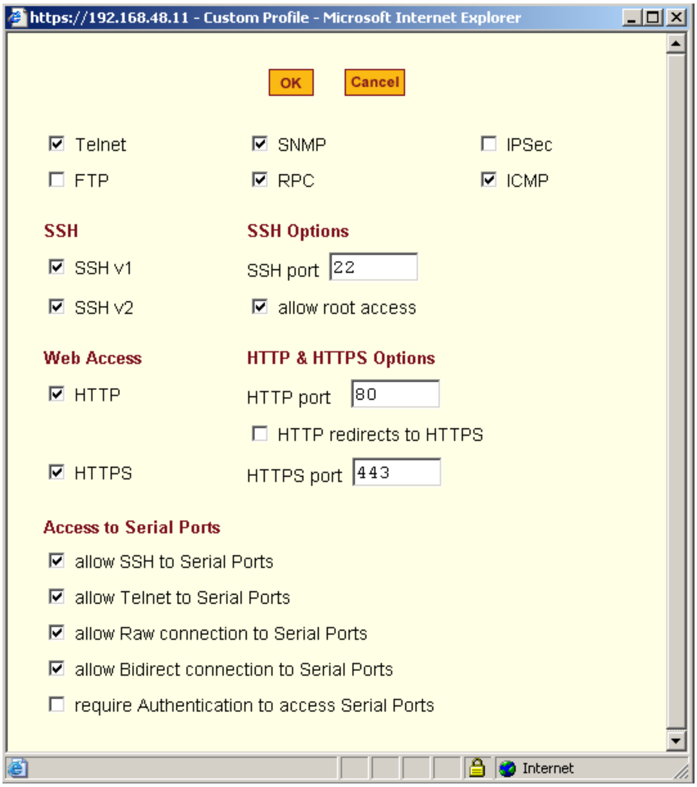
Currently there is **NO SECURITY PROFILE** set.

- You must define a Security Level before proceding with further configuration.
- Please choose from the three preset security levels: Secured, Moderate or Open.
- You can also configure a customized security profile.

**Figure 5-4:** Wizard > Step 1: Security Profile Form

4. Select a pre-defined Security Profile by pressing one of the "Secured", "Moderate", "Open", or "Default" profiles, or create a "Custom" profile.

   The following dialog box appears when you select the "Custom" profile.



https://192.168.48.11 - Custom Profile - Microsoft Internet Explorer
OK
Cancel
Internet

☑ Telnet    ☑ SNMP    □ IPSec

□ FTP    ☑ RPC    ☑ ICMP

**SSH**

☑ SSH v1

☑ SSH v2

**SSH Options**

SSH port 22

☑ allow root access

**Web Access**

☑ HTTP

☑ HTTPS

**HTTP & HTTPS Options**

HTTP port 80

□ HTTP redirects to HTTPS

HTTPS port 443

**Access to Serial Ports**

☑ allow SSH to Serial Ports

☑ allow Telnet to Serial Ports

☑ allow Raw connection to Serial Ports

☑ allow Bidirect connection to Serial Ports

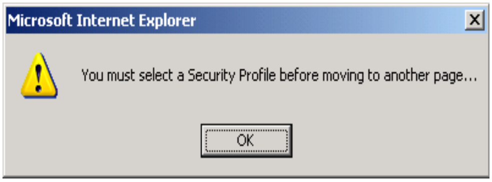
□ require Authentication to access Serial Ports

**Figure 5-5:** Custom Security Profile Dialog Box

**Caution:** Take the required precautions to understand the potential impacts of each individual service configured under the "Custom" profile

Refer to Table 5-1 on page 79, and the subsequent tables for a comparison of the available services in each security profile. Refer to the Glossary for a definition of the available services.

**Note:** It is not possible to continue working in the Web Manager without selecting a Security Profile. The following dialog box appears if you try to navigate to other sections of the Web Manager.

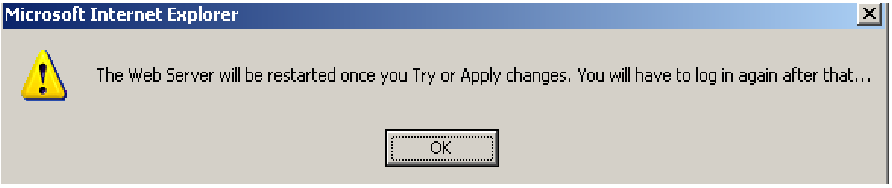


Microsoft Internet Explorer

You must select a Security Profile before moving to another page...

5. Once you select a security profile or configure a custom profile and apply the changes, the CS Web Manager restarts in order for the changes to take effect.

   The following dialog box appears.



Microsoft Internet Explorer

The Web Server will be restarted once you Try or Apply changes. You will have to log in again after that...

6. Select “apply changes” to save the configuration to Flash.

   CS Web Manager restarts.

7. Login 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

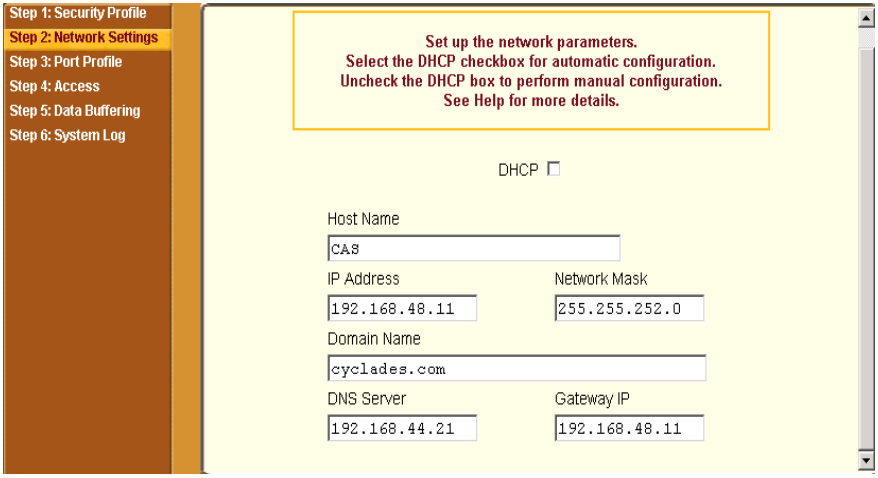
Selecting "Step 2: Network Settings” brings up a form for reconfiguring existing network settings. During initial setup of the CS, the administrator configures the basic network settings that were required to enable logins through the Web Manager. You can skip this step if the current settings are correct.

In preparation to configure network settings collect the following information and proceed with the network configuration procedure.

- Hostname
- An IP address for CS
- Domain name
- DNS server’s IP address
- Gateway IP address
- Network mask
- NTP server’s IP address (if you are using a time/date server)

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

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



Set up the network parameters.
Select the DHCP checkbox for automatic configuration.
Uncheck the DHCP box to perform manual configuration.
See Help for more details.

DHCP □

Host Name: CAS

IP Address: 192.168.48.11

Network Mask: 255.255.252.0

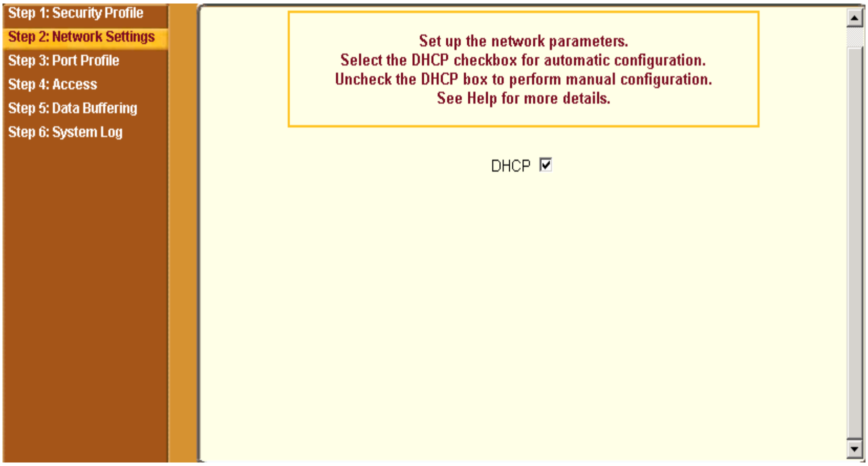
Domain Name: cyclades.com

DNS Server: 192.168.44.21

Gateway IP: 192.168.48.11

**Figure 5-6:** Wizard > Step 2: Network Settings - DHCP disabled.

If the “DHCP” is enabled, the form appears as shown in the following figure.



Set up the network parameters.
Select the DHCP checkbox for automatic configuration.
Uncheck the DHCP box to perform manual configuration.
See Help for more details.

DHCP ☑

**Figure 5-7:** Wizard > Step 2: Network Settings - DHCP enabled.

## ▼ *To configure the Network Settings*

**1.** Select “Step 2: Network Settings.”

The system brings up the DHCP form. By default DHCP is active.

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

**2.** If you are using DHCP, proceed to “Step 3: Port Profile”, if not, click on the checkbox to deselect DHCP and enter your network settings manually.

**3.** Enter the following network information:

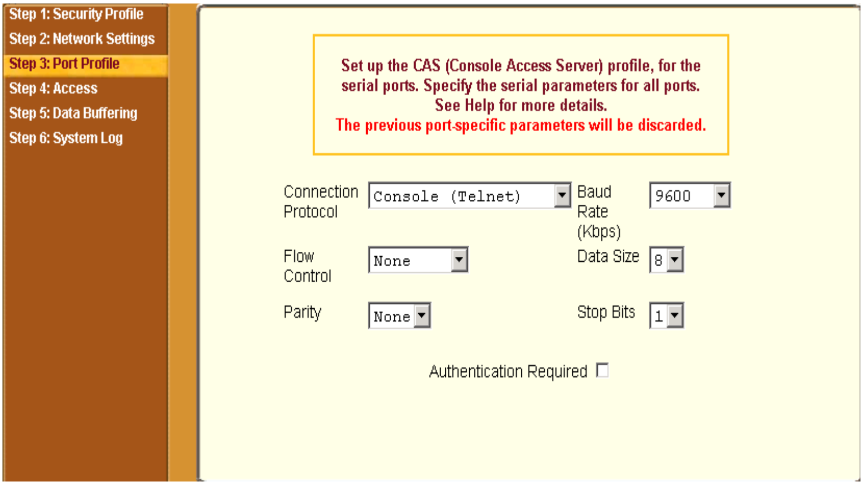
- Host Name
- IP addresses
- Network Mask
- Domain Name
- DNS Server
- Gateway IP

**4.** Select “apply changes” to save configuration to flash.

5. Select the “Next” button, or proceed to “Step 3: Port Profile”.

## Step 3: Port Profile

Selecting “Step 3: Port Profile” brings up a form for configuring the Console Access Profile (CAS). The protocol used to access the serial ports can be configured in this form.



Set up the CAS (Console Access Server) profile, for the serial ports. Specify the serial parameters for all ports. See Help for more details.
The previous port-specific parameters will be discarded.

| | | | |
|---|---|---|---|
| Connection Protocol | Console (Telnet) | Baud Rate (Kbps) | 9600 |
| Flow Control | None | Data Size | 8 |
| Parity | None | Stop Bits | 1 |

Authentication Required ☐

**Figure 5-8:** Wizard > Step 3: Port Profile

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

**Note:** From the factory by default, all Serial Ports are disabled. 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:** Wizard > Serial Port Profile Parameters and Usage

| Parameter | Options | Description |
|---|---|---|
| **Connection Protocol** | Console (Telnet) [Default]<br>Console (SSH)<br>Console (TelnetSSH)<br>Console (Raw) | Sets the protocol to be used to connect to devices that are connected to serial ports.<br>Console (SSH) encrypts data and authentication information.<br>Console (TelnetSSH) allows users to connect using either protocol.<br>Console (Raw) is for unnegotiated plain socket connections.<br>Use Expert mode if you want to specify any of several other connection protocols that are listed under Ports>Physical Ports>Modify>General. |
| **Flow Control** | None [Default]<br>Hardware<br>Software | Must match the flow control method of the devices connected to all serial ports. |
| **Parity** | None [Default]<br>Odd<br>Even | Must match the parity used by the devices connected to all serial ports. |
| **Baud Rate (Kbps)** | 9600 [Default]<br>Options range from 2400–921600 Kbps | Must match the baud rates of the devices connected to all serial ports. |
| **Data Size** | 8 [Default]<br>Options range from 5–8 | Must match the number of data bits used by the devices connected to all ports. |
| **Stop Bits** | 1 [Default]<br>Options are either 1 or 2 | Must match the number of stop bits used by the devices connected to all ports. |

**Table 5-4:** Wizard > Serial Port Profile Parameters and Usage (Continued)

| Parameter | Options | Description |
|---|---|---|
| **Authentication Required** | Check for enabled.<br>Unchecked for disabled. [Default] | If the “Authentication Required” is enabled, user authentication is enforced using the local `passwd` database.<br>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. For example, to assign an alias to a serial port, to specify individual parameters to the serial ports or groups of serial ports, or to utilize any of several other connection protocols.

For information on configuring serial ports in expert mode see Chapter 10, “Ports Menu & Forms.”

## ▼ *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 CS can run using the same connection protocol with the same speed. In addition you need to 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. See Chapter 10, “Ports Menu & Forms” for more detail.

1. Select a protocol, “Console (Telnet)”, “Console (SSH)” “Console (TelnetSSH)”, or “Console (Raw)” from the “Connection Protocol” pull-down menu.

   The default is “Console (Telnet).”

2. To change the flow control, select “None,” “Hardware,” or “Software” from the “Flow Control” pull-down menu.

   The default is None.

3. To change the parity, select “None,” “Odd” or “Even” from the “Parity” pull-down menu.

   The default is “None.”

4. To change the baud rate, select an option from 2400 to 921600 Kbps from the “Baud Rate” pull-down menu.

   The default is 9600, which is the most common baud rate for devices.

5. To change the data size, select an option from 5 to 8 from the “Data Size” 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 authentication is required, check the “Authentication Required” checkbox for enabled or leave it unchecked for disabled.

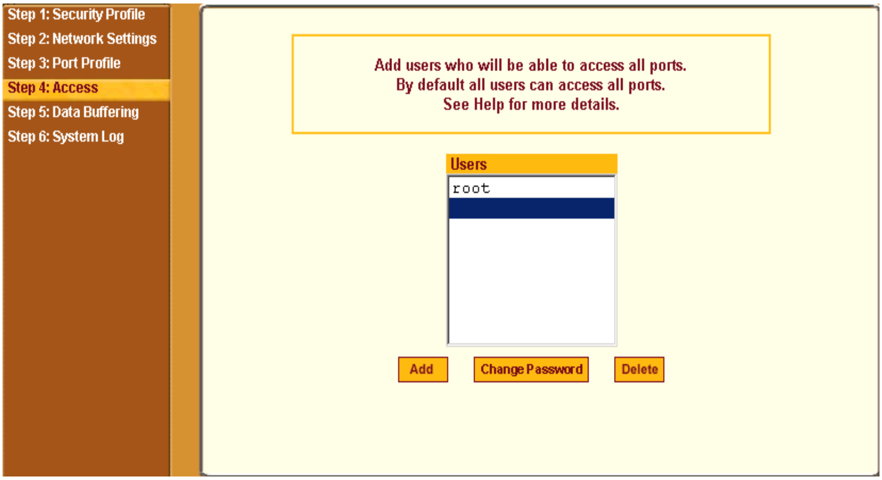
8. Select “apply changes' to save configuration to Flash.

9. Select the “Next” button or proceed to the next section, “Step 4: Access.”

## Step 4: Access

Selecting “Step 4: Access” brings up a form shown in the following figure, which allows 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 CS. By default any user can access any port as long as they have a valid user ID and password.



Add users who will be able to access all ports.
By default all users can access all ports.
See Help for more details.

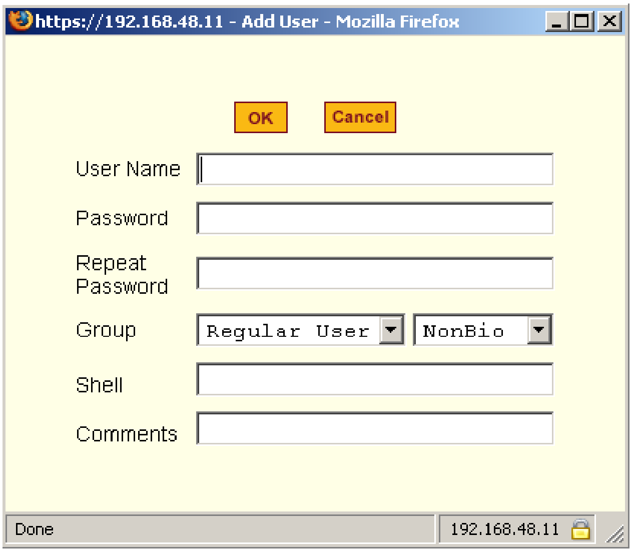
root

**Figure 5-9:** Wizard > Step 4:Access

The Access form lists the currently defined Users and has “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 CS.

Clicking the “Add” button, brings up the following form.



https://192.168.48.11 - Add User - Mozilla Firefox

| | |
|---|---|
| User Name | |
| Password | |
| Repeat Password | |
| Group | Regular User / NonBio |
| Shell | |
| Comments | |

**Figure 5-10:** Wizard > Step 4: Access Add User Dialog Box

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. To define a new group, go to the "Expert" mode and select Security > Users and Groups. |
| **[*dropdown list*]** | Select whether the user of this group is a "NonBio" [Default] or a "BioUser." The "BioUser" group should only be selected if authentication will be made through the AlterPath Bio (biometric authentication). |

**Table 5-5:** Wizard > Add User Dialog: Field Names and Definitions

| Field Name | Definition |
|---|---|
| **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. |

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

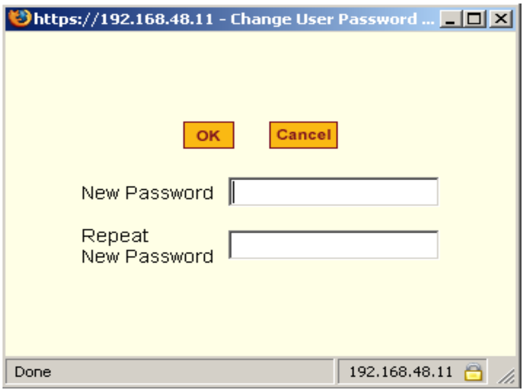


**Figure 5-11:** Wizard > Step 4: Change Password Dialog Box

## ▼ *To Add a User*

1. Select "Step 3: Access"

   The Access form displays.

1. Click Add.

   The "Add User" dialog box appears.

2. Enter the username and password in the "User Name" and "Password" fields, and enter the password again in the "Repeat Password" field.

3. Select from the "Group" menu options.

   a. To create a regular user account without administrator privileges, select "Regular User" [Default] from the "Group" pull-down menu.

b. To create an account with administrator privileges, select “Admin” from the “Group” pull-down menus.

**Note:** To define a new group, switch to ”Expert” mode, and select Security > Users and Groups.

4. Select whether the user of this group is a NonBio or a BioUser. The BioUser group should only be selected if authentication is made through the AlterPath Bio (biometric authentication).
5. Enter the default shell in the “Shell” field (optional).
6. Enter comments to identify the user’s role or configuration in the “Comments” field (optional).
7. Click OK.
8. Click the “apply changes” button.

## ▼ *To Delete a User*

1. Select “Step 3: Access.”

   The “Access” form displays.
2. Select the user name to delete.
3. Click “Delete.”
4. Click “apply changes.”

## ▼ *To Change a Password*

**Caution:** Leaving the default “root” password unchanged leaves the CS and connected devices open to anyone who knows the default password and the CS’s IP address. For security reasons, change the “root” password from the default “bb” as soon as possible.

1. Select “Step 3: Access.”

   The “Access” form displays.
2. Select the name of the user whose password you want to change.

3. Click “Change Password.”

   The “Change User Password” dialog box displays.

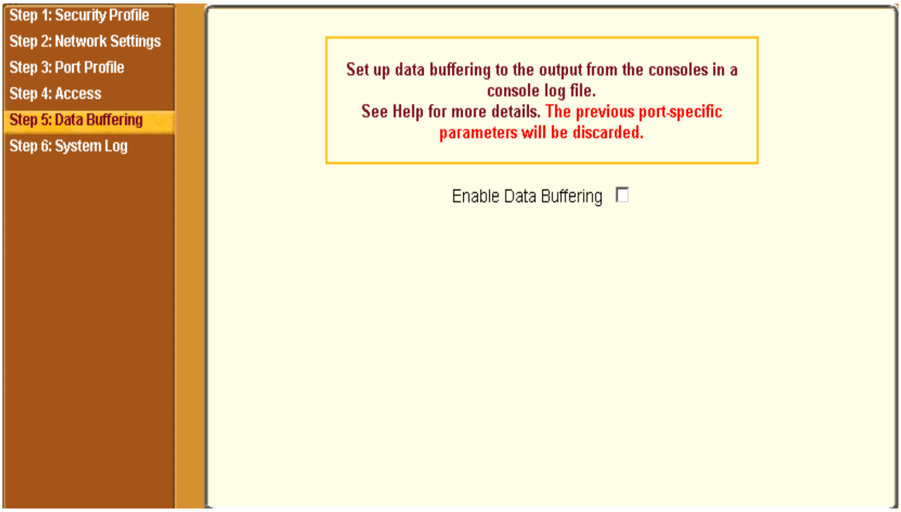
4. Enter the new password in both fields, and click OK.

5. Click “apply changes.”

## Step 5: Data Buffering

Selecting “Step 5: Data Buffering” brings up a form to allow logging the console data to a data buffer file either locally in CS or remotely to an external storage source such as an NFS server or Syslog server.

The following figure shows the form when “Enable Data Buffering” is inactive.



Set up data buffering to the output from the consoles in a console log file.
See Help for more details. The previous port-specific parameters will be discarded.

Enable Data Buffering □

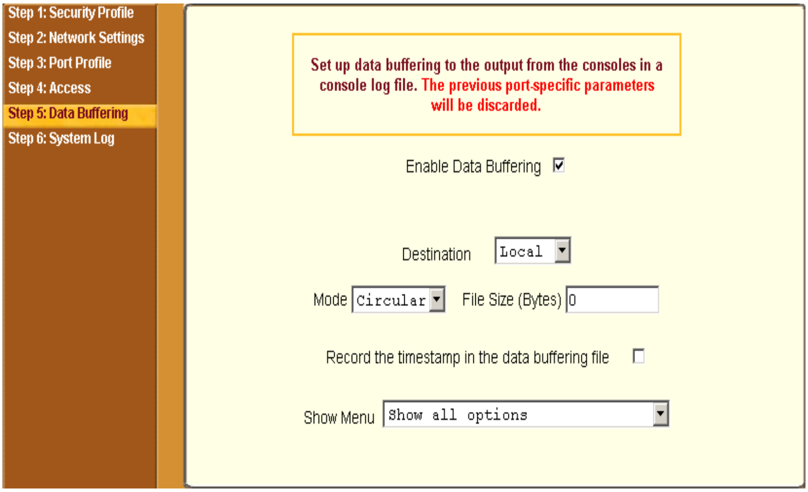
**Figure 5-12:** Wizard > Step 5: Data Buffering [Inactive]

Once data buffering is enabled 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

CS's flash memory or on the hard disk of an external server, such as an NFS or Syslog server.

The following figure shows the form when Data Buffering is set to enabled, and the "Destination" is set to "Local".



Set up data buffering to the output from the consoles in a console log file. The previous port-specific parameters will be discarded.

Enable Data Buffering ☑

Destination: Local

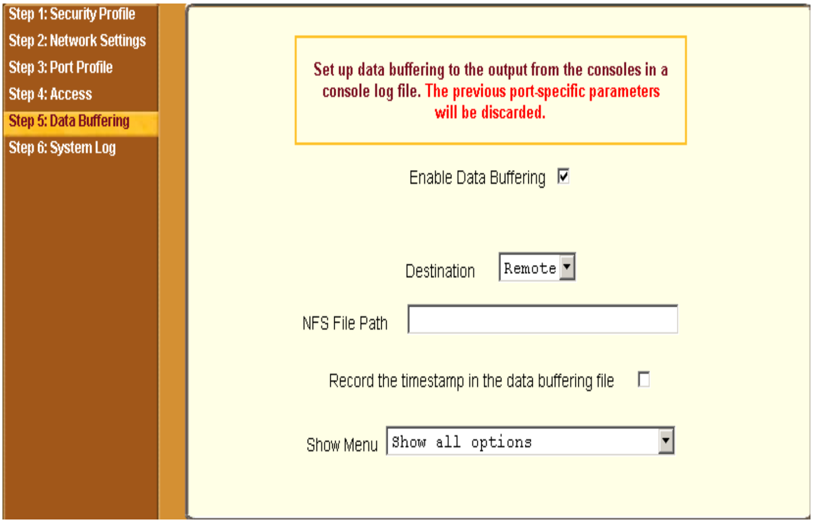
Mode: Circular  File Size (Bytes): 0

Record the timestamp in the data buffering file □

Show Menu: Show all options

**Figure 5-13:** Wizard > Step 5: Data Buffering [Local]

The following figure shows the form when data buffering is set to "Destination Remote"



Set up data buffering to the output from the consoles in a console log file. The previous port-specific parameters will be discarded.

Enable Data Buffering ☑

Destination Remote

NFS File Path

Record the timestamp in the data buffering file □

Show Menu Show all options

**Figure 5-14:** Wizard > Step 5: Data Buffering [Remote]

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 sequential files, or Circular for non-sequential format.<br>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. |

| Field Name | Definition |
|---|---|
| **File Size (Bytes)** | For Local Destination - Sets the value for this field to be greater than zero. |
| **Record the timestamp...** | If enabled, the system inserts a timestamp in the buffer. |
| **NFS File Path** | For Remote Destination - Includes the path where the data buffer file should be stored. |
| **Show Menu** | Defines the options you want to show in the menu of the buffer file. |

**Note:** Make sure that enough disk space is available to store the files in the location you select. Sequentially-written files can quickly grow to exceed the storage capacity of the local flash memory or remote hard drive. Data buffering should only be done if processes are in place to monitor the stored data.

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

**Table 5-7:** Wizard > Differences Between Remote and Local Buffering

| Option | Description |
|---|---|
| **Remote server** | Data is stored in files sequentially. The NFS server must be configured with the mount point shared (exported). In linear mode, data is written into a continuous sequence of files, and the file spaces is not reused. The administrator needs to allow enough space for the expected amount of data, and take measures such as moving unneeded data files off line, to ensure data does not outgrow the available space. |
| **Local files** | Set a file size greater than zero. Make sure the file size does not exceed the space available on the CS’s flash memory. If needed, you can supplement the flash memory module by installing a flash memory card (with an adapter) or other storage device in a PCMCIA slot. For a list of supported PCMCIA cards see Appendix C. |

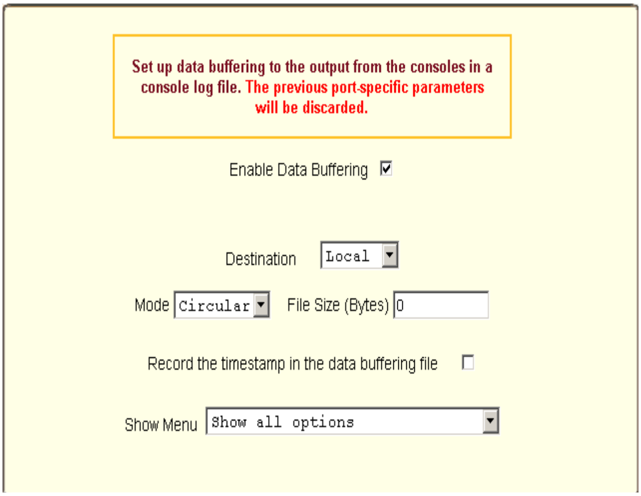
**Note:** You can perform advanced configuration in Expert mode including the option of setting up data buffering separately for individual or groups of serial ports.

## ▼ *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.



Set up data buffering to the output from the consoles in a console log file. The previous port-specific parameters will be discarded.

Enable Data Buffering ☑

Destination: Local

Mode: Circular

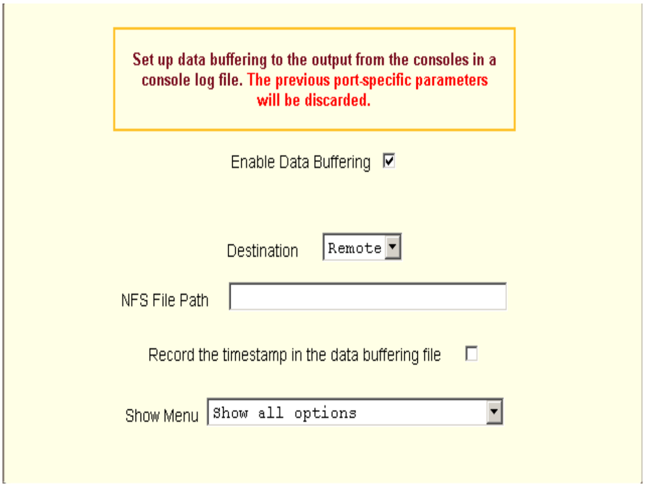
File Size (Bytes): 0

Record the timestamp in the data buffering file ☐

Show Menu: Show all options

   a. From the "Mode" pull-down menu, select "Circular" or "Linear" data buffering.
   b. Type a file size in bytes into the "File Size (Bytes)" field.

      The file size should be greater than zero.
5. When the destination is remote, perform the following steps.



Set up data buffering to the output from the consoles in a console log file. The previous port-specific parameters will be discarded.

Enable Data Buffering ☑

Destination: Remote

NFS File Path:

Record the timestamp in the data buffering file ☐

Show Menu: Show all options

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/cslogs`, enter `/var/adm/cslogs` 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 CS.

---

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

c. Select an option from the “Show Menu” pull-down menu.

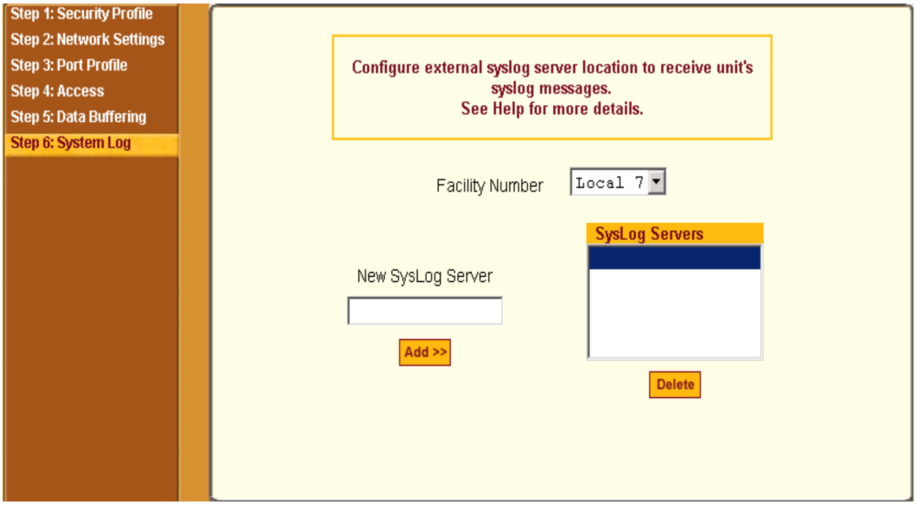
   The choices are: “show all options”, “No”, “Show data buffering file only”, and “Show without the erase options.”

6. Click “apply changes.”

## Step 6: System Log

Selecting “Step 6: System Log” brings up a form for identifying one or more syslog servers to receive syslog messages generated by the CS’ serial ports. Syslogging for IPDUs is also possible, if IPDU power management is configured. See Chapter 7, “IPDU Power Mgmt.

The form appears as shown in the following figure.



Configure external syslog server location to receive unit's syslog messages.
See Help for more details.

Facility Number: Local 7

New SysLog Server

SysLog Servers

**Figure 5-15:** Wizard > Step 6: System Log

**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 an pre-configured syslog server is available on the same network as the CS. Obtain the following information from the syslog server's administrator.

- The IP address of the syslog server.
- The facility number for messages coming from the CS.

  See Chapter 1, "Syslog Servers" on how facility numbers are used.

## ▼ *To Add a Syslog Server*

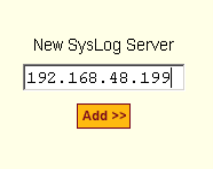
This procedure assumes you have the following information:

- The IP address of the syslog server
- The facility number for messages coming from the CS

**1.** Select "Step 6: System Log."

The System Log form displays.

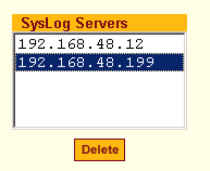
2. From the Facility Number drop-down menu, select the facility number.
3. In the “New Syslog Server” field, enter the IP address of a syslog server, and then click the “Add” button. (Repeat this step until all syslog servers are listed.)



New SysLog Server

192.168.48.199

4. The new server(s) appear in the Syslog Servers list.



SysLog Servers

192.168.48.12

192.168.48.199

5. Click “apply changes.”

## ▼ *To Delete a Syslog Server*

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

The subsequent chapters shown below describe the Expert configuration mode in detail, introduces the menu elements in the “Expert” mode, and describe the underlying procedures.

**Table 5-8:** CS Configuration and Expert Menus Chapters

| | |
|---|---|
| Configuring the CS in Expert Mode | Chapter 6, “Configuring the CS in Expert Mode |
| Applications Menu [Expert] | Chapter 7, “Applications Menu & Forms |

**Table 5-8:** CS Configuration and Expert Menus Chapters

| | |
|---|---|
| Network Menu [Expert] | Chapter 8, “Network Menu & Forms |
| Security Menu [Expert] | Chapter 9, “Security Menu & Forms |
| Ports Menu [Expert] | Chapter 10, “Ports Menu & Forms |
| Administration Menu [Expert] | Chapter 11, “Administration Menu & Forms |

# Chapter 6
# Configuring the CS in Expert Mode

This chapter provides an overview of configuring the CS Web Manager in Expert Mode. The following chapters in this manual introduces the Expert mode forms and functionality.

The Expert mode is designed for the advanced user administrator who needs to configure the CS beyond the capabilities of the basic wizard mode.

This chapter includes the following sections:.

## Overview of Menus and Forms

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.

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. Occasionally, a menu selection comprise of multiple forms as shown in the following figure.

These forms are identified by their tabs. Select the tab to access the desired form.

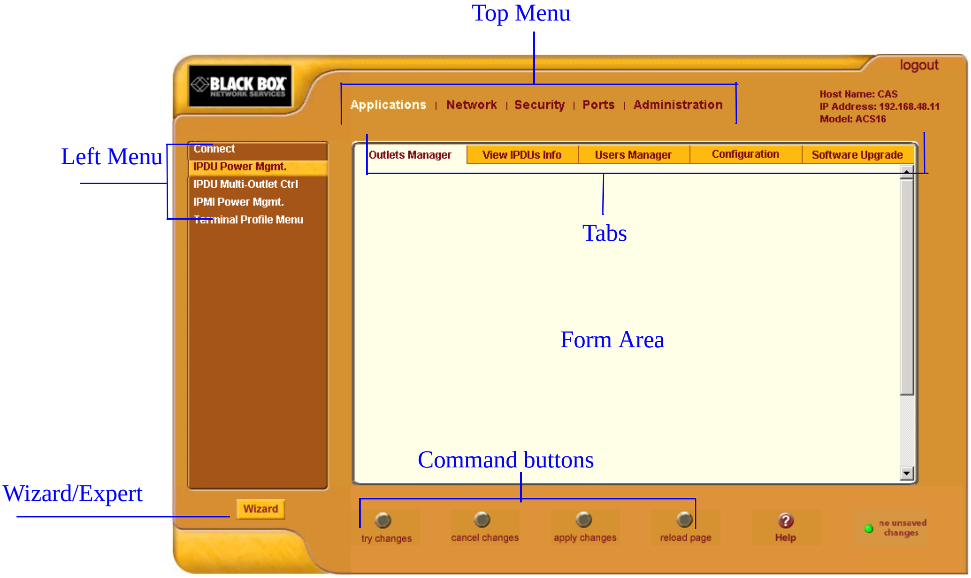


**Figure 6-1:** Expert Mode Screen Elements

**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 use this convention, “In Expert mode, go to Applications> IPDU Power Mgmt.>Outlets Manager”

# Mapping of the Expert Mode Menus and Forms

The following table illustrates a mapping of the menus and forms available in Expert mode. If you are viewing this document online, click any term to go to the section where the form is described.

**Table 6-1:** Expert Mode Menu and Forms

**Applications**

- Connect
  - IPDU Power Mgmt.
    - Outlets Manager
    - View IPDUs Info
    - Users Manager
    - Configuration
    - Software Upgrade [for the AlterPath PM]
- IPDU Power Mgmt.
- IPMI Power Management
- Terminal Profile Menu

**Network**

- Host Settings
- Syslog
- PCMCIA Management
- VPN Connections
- SNMP
- Firewall Configuration
- Host Table
- Static Routes

**Security**

- Users and Groups
- Active Ports Sessions
- Authentication
  - Auth Type
  - Radius
  - Tacacs+
  - Ldap
  - Kerberos
  - NIS
- Security Profiles

**Ports**

- Physical Ports
  - Modify Selected/All Ports
    - General
    - Access
    - Data Buffering
    - Multi User
    - Power Management
    - Other
- Virtual Ports
- Ports Status
- Ports Statistics

**Administration**

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

# Description of Forms in Expert Mode

The following table briefly describes the functionality of each menu and the related forms. For detailed procedures refer to the page where documented for each section.

**Table 6-2:** Expert > Applications

| Form | Use This Form To: | Where Documented |
|---|---|---|
| **Connect** | Connect to the CS shell through a secure SSH session, or connect to a specific serial port. | Chapter 7, Page 116 |
| **IPDU Power Mgmt.** | Manage power outlets on the AlterPath PM family of Intelligent Power Distribution Units. From here you may power remote machines on and off, check the status and lock the power outlet in the on or off state to prevent accidental changes. | Chapter 7, Page 120 |
| **IPDU Multi-Outlet Ctrl** | Manage all power outlets of a multi-outlet device connected to the AlterPath PM family of Intelligent Power Distribution Units in one single operation. | Chapter 7, Page 133 |
| **IPMI Power Mgmt.** | Manage IPMI devices. Power on and off remote machines, and check their current status. | Chapter 7, Page 139 |
| **Terminal Profile Menu** | Configure a menu of commands that will be presented to the user when they power on their computer terminal and login to the CS. This is a special application used only when the CS is being used as a server with terminals attached. | Chapter 7, Page 146 |

**Table 6-3:** Expert > Network

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Host Settings** | Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access. | Chapter 8, Page 152 |
| **Syslog** | Configure how CS will handle its syslog messages. CS generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit and control purposes. | Chapter 8, Page 157 |
| **PCMCIA Management** | Configure the optional PCMCIA cards. BLACK BOX® CS supports several PCMCIA cards including modem, ISDN, wireless and wired NICs, Compact Flash and IDE drives for data buffer storage. | Chapter 8, Page 158 |
| **VPN Connections** | Configure one or more VPN connections to other systems or CS attached devices. | Chapter 8, Page 176 |
| **SNMP** | Configure Simple Network Management Protocol (SNMP) with community names, OID and user names. SNMPv1, v2 and v3 are supported. This section and the dialog boxes guide you to configure the required parameters. | Chapter 8, Page 181 |
| **Firewall Configuration** | Configure static IP tables, and how packets should be filtered. | Chapter 8, Page 186 |
| **Host Table** | View information about the local network environment. View table of hosts; create, edit, and delete hosts. | Chapter 8, Page 201 |

**Table 6-3:** Expert > Network

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Static Routes** | To manually add routes. Static routes are a very quick and effective way to route data from one subnet to different subnets. | Chapter 8, Page 202 |

**Table 6-4:** Expert > Security

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Users and Groups** | Create or edit users and groups, establish or change their passwords, access rights and privileges. | Chapter 9, Page 208 |
| **Active Port Sessions** | Show the active sessions, as well as their identifications, features and usage statistics. | Chapter 9, Page 212 |
| **Authentication** | Enter the authentication method used to access CS. | Chapter 9, Page 214 |
| **Security Profiles** | Select a pre-defined Security Profile, or choose Custom Profile to configure individual settings. | Chapter 9, Page 226 |

**Table 6-5:** Expert > Ports

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Physical Ports** | Activates or deactivates serial ports. Set the parameters for each or all ports. Configure specific parameters for the serial ports where IPDU devices are connected. | Chapter 10, Page 239 |

**Table 6-5:** Expert > Ports

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Virtual Ports** | Perform Clustering. One CS can be used as a Master to control other CS (slaves) units. All ports of the slave unit appear as if they are in the master unit. This section shows how to define and configure the slaves. | Chapter 10, Page 281 |
| **Port Status** | View the current status of each port. The information provided here are: RS232 Signal Status and user connected to each port. | Chapter 10, Page 287 |
| **Ports Statistics** | View information on the data reception Rx bytes and transmission Tx bytes on each physical port. View current CAS user(s), Baud rate, frame, parity, break and overruns. | Chapter 10, Page 288 |

**Table 6-6:** Administration

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **System Information** | View information on the system hardware, version, file system and PCMCIA cards loaded | Chapter 11, Page 292 |
| **Notifications** | Configure the alarm strings and the destination of the notification. CS can send notification by email, pager or SNMP trap in the occurrence of any system warnings and alarms. | Chapter 11, Page 295 |

**Table 6-6:** Administration

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Time/Date** | Set the timezone and configure the system's Date and Time.<br>Network Time Protocol (NTP) can also be used. | Chapter 11, Page 305 |
| **Boot Configuration** | Configure CS to boot from its internal firmware or from the network.<br>Defines the settings for loading the operating system in the event that the CS fails to boot successfully.<br>The BLACK BOX® CS can boot from its internal firmware or from the network. This section configures the required parameters. | Chapter 11, Page 307 |
| **Backup Configuration** | Use a FTP server to save and retrieve your CS configuration; use a storage device to store your configuration. | Chapter 11, Page 310 |
| **Upgrade Firmware** | Upload/upgrade new firmware. | Chapter 11, Page 313 |
| **Reboot** | Reboot the CS system. | Chapter 11, Page 316 |
| **Online Help** | Configure a path to a local server for storing the online help files. | Chapter 11, Page 317 |

# Chapter 7
# Applications Menu & Forms

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 procedures.

**Table 7-1:** Expert > Applications Menu

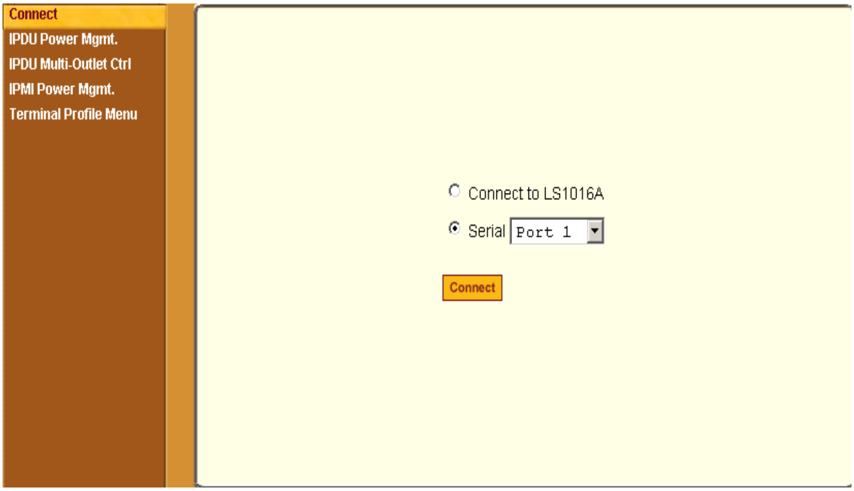
| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Connect** | Connect to the CS shell via a secure SSH session or connect to the serial ports. | Page 116 |
| **IPDU Power Mgmt.** | Manage power outlets on the AlterPath PM family of Intelligent Power Distribution Units. From here you may power remote machines on and off, check the status, and lock the power outlet in the on or off state to prevent accidental changes. | Page 120 |
| **IPDU Multi-Outlet Ctrl** | Manage all power outlets of a multi-outlet server or device connected to the AlterPath PM in one single operation. | Page 133 |
| **IPMI Power Mgmt.** | Manage IPMI (Intelligent Platform Management Interface) devices. Power on/off remote machines and check their current status. | Page 139 |

**Table 7-1:** Expert > Applications Menu

| **Menu Selection** | **Use this menu to:** | **Where Documented** |
|---|---|---|
| **Terminal Profile Menu** | Configure a menu of commands that will be presented to the user when they power on their computer terminal and login to the CS. This is a special application used only when the CS is being used as server with terminals attached. | Page 146 |

# Applications

Under “Applications” in Expert mode, five options appear in the left menu panel as shown in the following figure.



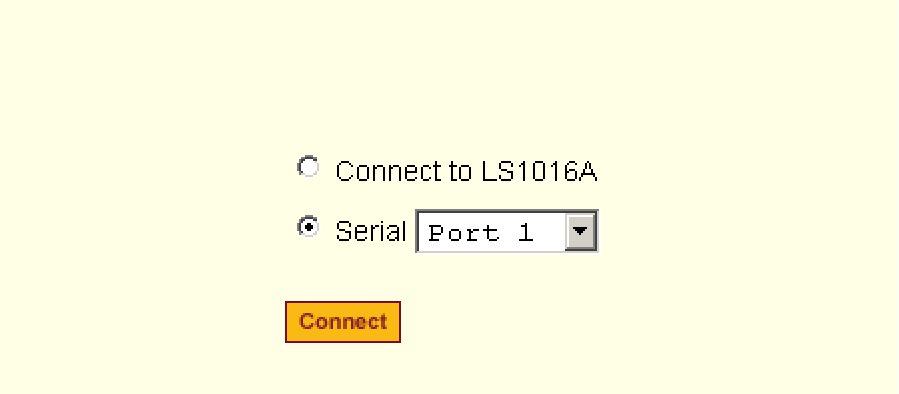
○ Connect to LS1016A

● Serial Port 1

**Figure 7-1:** Expert > Applications Menu Options

## *Connect*

Selecting the “Connect” form under “Applications” brings up the form shown in the following figure.



○ Connect to LS1016A

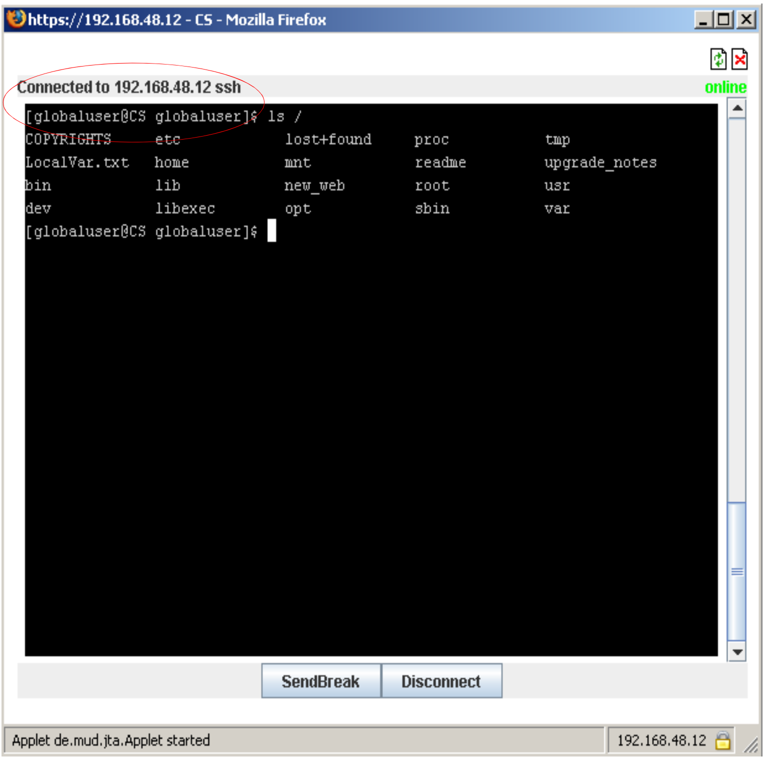
● Serial Port 1

**Figure 7-2:** Expert > Applications > Connect Form

Using the “Connect” form, you can connect directly to CS, or to the devices that are connected to the serial ports.

- Connect to CS

  Clicking the “Connect to CS” radio button and clicking the “Connect” button, brings up a Java applet running an SSH session similar to the following figure.



https://192.168.48.12 - CS - Mozilla Firefox
Connected to 192.168.48.12 ssh
online

```
[globaluser@CS globaluser]$ ls /
COPYRIGHTS    etc          lost+found    proc         tmp
LocalVar.txt  home         mnt           readme       upgrade_notes
bin           lib          new_web       root         usr
dev           libexec      opt           sbin         var
[globaluser@CS globaluser]$
```

SendBreak
Disconnect
Applet de.mud.jta.Applet started
192.168.48.12

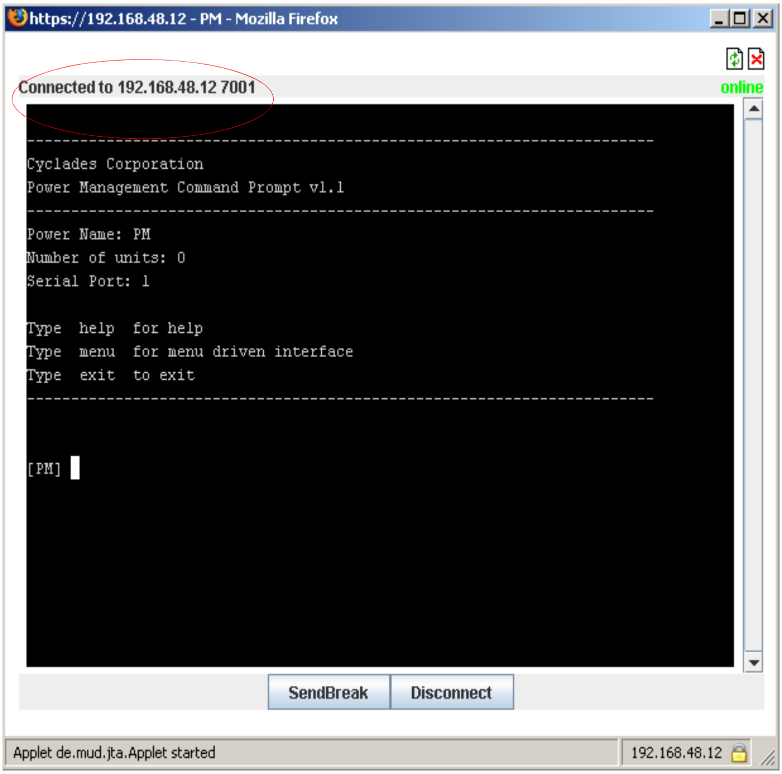
**Figure 7-3:** Expert > SSH session Java Applet

**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. For more information see Chapter 9, “Security Menu & Forms.

- Serial

  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” brings up a Java applet with a connection protocol that the serial port is configured for.

  For example, if the serial port is named “PM” and configured for power management, when you press the “Connect” button a form similar to the following figure appears.



Connected to 192.168.48.12 7001

```
----------------------------------------------------------------------
Cyclades Corporation
Power Management Command Prompt v1.1
----------------------------------------------------------------------
Power Name: PM
Number of units: 0
Serial Port: 1

Type  help  for help
Type  menu  for menu driven interface
Type  exit  to exit
----------------------------------------------------------------------


[PM]
```

Applet de.mud.jta.Applet started

**Figure 7-4:** Expert > Serial Port Java Applet

Note the difference between “Connect to CS” and “Serial” connections in the “Connected to” grey bar circled in red in the above two figures.

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 CS*

This procedure logs you into the CS as a “Regular User” in a SSH session.

1. Go to Applications > Connect in Expert mode.
2. Click the “Connect to CS” radio button.
3. Click the “Connect” button.

A Java applet viewer appears. If your security profile is set to “Moderate” or “Open” you receive a “root” prompt, otherwise, an authentication form appears. You cannot authenticate unless you change the security profile to “Custom” and enable “allow root access”.

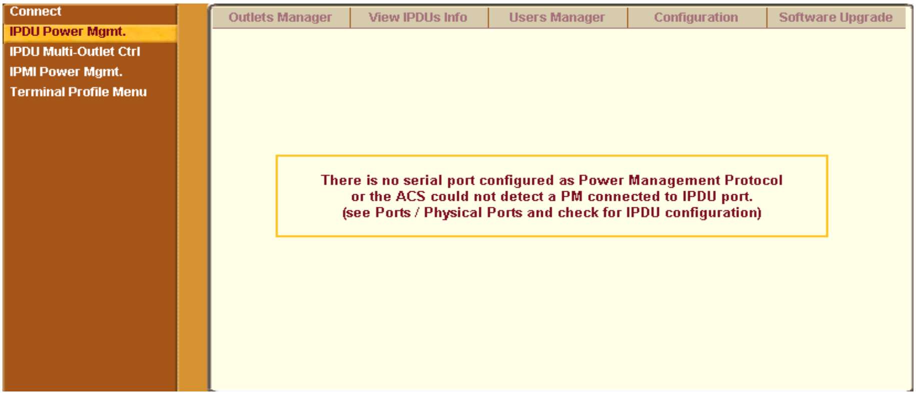
### ▼ To Connect to a Device Through a Serial Port

1. Go to Applications > Connect in Expert mode.
2. Click the “Serial” radio button.
3. Select a port number or alias from the “Serial” pull-down menu.
4. Click “Connect.”

   A Java applet viewer appears. If authentication is specified for the selected port you are prompted to log in. If not, you are automatically logged in.

## IPDU Power Mgmt.

Selecting the “IPDU Power Mgmt.” brings up the five tabs shown in the following figure. Using the IPDU power management forms you can manage the power to the connected devices only if a serial port is configured for power management.



There is no serial port configured as Power Management Protocol
or the ACS could not detect a PM connected to IPDU port.
(see Ports / Physical Ports and check for IPDU configuration)

**Figure 7-5:** Expert > IPDU Power Mgmt. Tab Options

For the procedure, see “To Configure a Serial Port for IPDU or IPMI Power Management” on page 143.”

The following table provides links to description and procedures for the forms of the IPDU Power Mgmt. tabs.

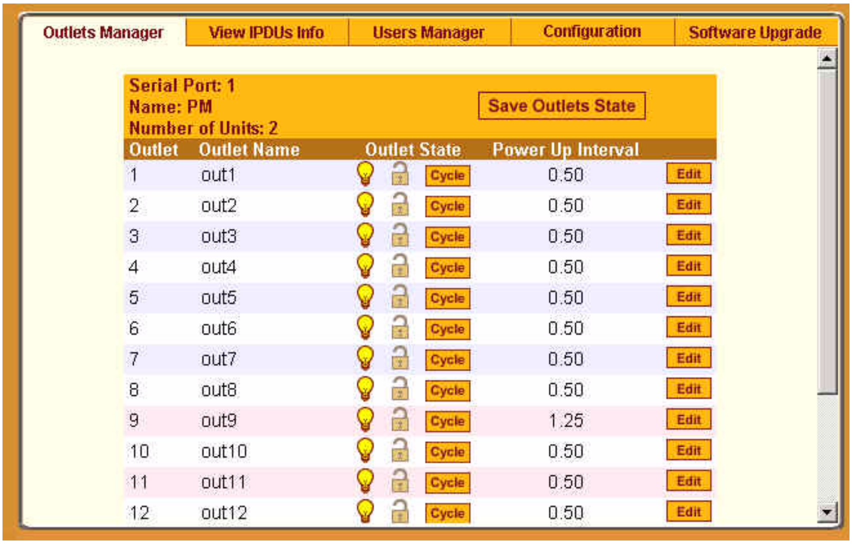
| | |
|---|---|
| Outlets Manager | Page 121 |
| View IPDUs Info | Page 124 |
| Users Manager | Page 127 |
| Configuration | Page 129 |
| Software Upgrade [for AlterPath PM] | Page 131 |

## Outlets Manager

On the “Outlets Manager” form under Applications>IPDU Power Mgmt., you can do the following tasks for all outlets on all connected IPDUs.

- Check the status of outlets
- Turn outlets on and off
- Cycle (Briefly switching the outlet off and on)
- Lock outlets in the on or off state to prevent accidental changes
- Unlock the outlets
- Assign an alias to the outlet (to identify the device for which it provides power)
- Change the power up interval. The power up interval is the time interval (in seconds) that the system waits between turning on the currently-selected outlet and the next outlet.
- Save the current configuration to Flash memory.

The following figure shows an Outlets Manager form.



Serial Port: 1
Name: PM
Number of Units: 2

| Outlet | Outlet Name | Outlet State | | | Power Up Interval | |
|---|---|---|---|---|---|---|
| 1 | out1 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 2 | out2 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 3 | out3 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 4 | out4 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 5 | out5 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 6 | out6 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 7 | out7 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 8 | out8 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 9 | out9 | 💡 | 🔓 | Cycle | 1.25 | Edit |
| 10 | out10 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 11 | out11 | 💡 | 🔓 | Cycle | 0.50 | Edit |
| 12 | out12 | 💡 | 🔓 | Cycle | 0.50 | Edit |

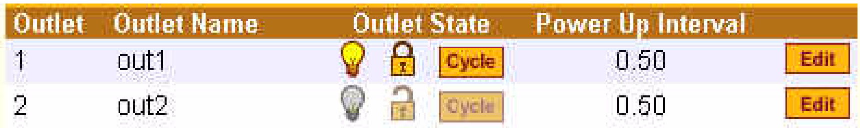
**Figure 7-6:** Expert > Applications > IPDU Power Mgmt. > Outlets Manager

The following table illustrates what each icon indicates

**Table 7-2:** Expert > Outlets Manager Icons Description

| Button | Purpose |
|---|---|
| 💡 💡 | Yellow bulbs indicate an outlet is switched on.Gray indicates 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. |

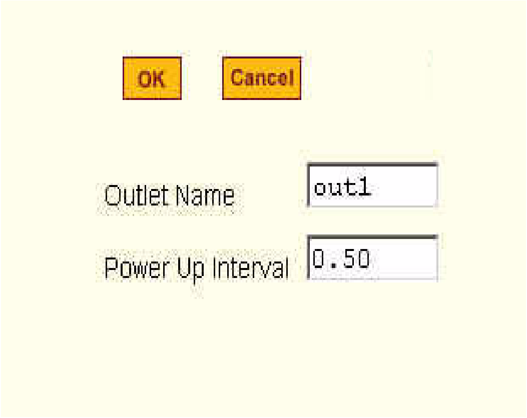
In the example below, outlet 1 is switched on and locked and outlet 2 is switched off and unlocked.



| Outlet | Outlet Name | Outlet State | Power Up Interval | |
|---|---|---|---|---|
| 1 | out1 | Cycle | 0.50 | Edit |
| 2 | out2 | Cycle | 0.50 | Edit |

**Figure 7-7:** Expert > Outlets Manager Icons

Clicking the Edit button brings up the following dialog box.



Outlet Name: out1

Power Up Interval: 0.50

**Figure 7-8:** Expert > Edit Outlets Dialog Box

You can specify a name for the outlet, for example, the server or device name, and change the power up interval.

**Note:** The power up interval is the amount of time (in seconds) that elapses after the selected outlet is turned on before another outlet can be turned on.

### ▼ *To View Status, Lock, Unlock, Rename, or Cycle Power Outlets*

1. Go to Applications > IPDU Power Mgmt. > Outlets Manager

   The “Outlets Manager” form appears.

2. To switch an outlet on or off, click the adjacent light bulb.
3. To lock or unlock an outlet, click the adjacent padlock.

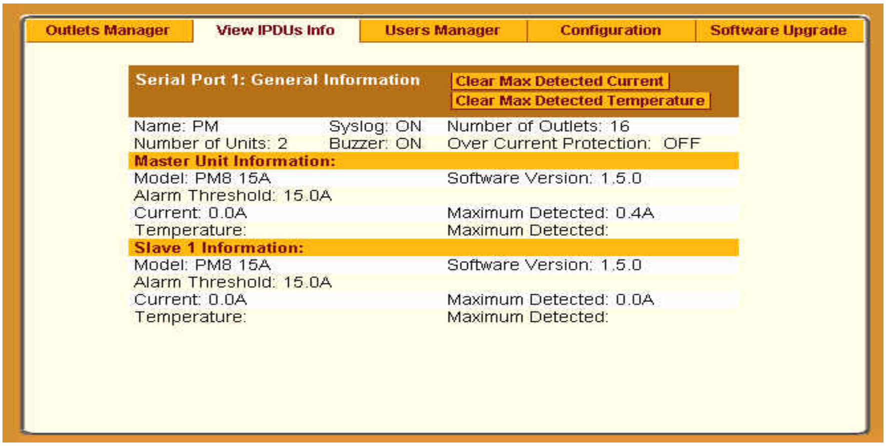
4. To momentarily power an outlet off and then on again, click the adjacent “Cycle” button.
5. To change the outlet’s name or the power up interval, click the adjacent “Edit” button.

   The Edit Outlet dialog box appears.

   a. To change the name assigned to the outlet, enter a new name in the “Outlet Name” field.
   b. To change the time between when this outlet is turned on and another can be turned on, change the default 0.50 number of seconds in the “Power Up Interval” field.
6. Click OK.
7. Click the “Save Outlets State” button.
8.  Click “apply changes.”

## View IPDUs Info

Selecting Applications > IPDU Power Mgmt. > View IPDUs Info tab, the form in the following figure appears.



Serial Port 1: General Information

Name: PM    Syslog: ON    Number of Outlets: 16

Number of Units: 2    Buzzer: ON    Over Current Protection: OFF

Master Unit Information:

Model: PM8 15A    Software Version: 1.5.0

Alarm Threshold: 15.0A

Current: 0.0A    Maximum Detected: 0.4A

Temperature:    Maximum Detected:

Slave 1 Information:

Model: PM8 15A    Software Version: 1.5.0

Alarm Threshold: 15.0A

Current: 0.0A    Maximum Detected: 0.0A

Temperature:    Maximum Detected:

**Figure 7-9:** IPDU Power Mgmt. > View IPDUs Info

The figure shows the information displayed when two eight-outlet AlterPath PM model PM8 15A is cascaded through Serial Port 1. The IPDU is configured for syslogging, an alarm buzzer, and over current protection. The configuration is done through the IPDU Power Mgmt Configuration form.

The following table describes the information viewable on the “View IPDUs Info” form. The information shown in the table appears for each serial port that is configured for power management. For example, Figure 7-9 displays “Serial Port 1: General Information” configured for power management.

**Table 7-3:** Expert > View IPDUs General Information

| | Description | Example |
|---|---|---|
| **Name** | Either a default name or administrator-configured name appears. | PM |
| **Number of Units** | The number of IPDUs connected to the port. The first IPDU is referred to as the master. Any other IPDUs daisy-chained off the first IPDU are referred to as slaves. | 2 IPDUs daisy-chained through the Serial Port 1 |
| **Number of Outlets** | Total number of outlets on all connected IPDUs. | Sixteen for two AlterPath PM8 15A daisy-chained through Serial Port 1 |
| **Buzzer** | Whether a buzzer has been configured to sound when a specified alarm threshold has reached. | ON when the buzzer is configured |
| **Syslog** | Whether syslogging has been configured for messages from this IPDU. | ON when syslogging is configured |
| **Over Current Protection** | Whether over current protection is enabled. “Over Current Protection” is to prevent outlets from being turned on, if the current on the IPDU exceeds the specified threshold. | OFF when over current protection is not enabled |

You can view the following information about each IPDU that is configured through a serial port. For example, the configuration illustrated in Figure 7-9 there are two sets of data. Master Unit Information and Slave 1 Information. There are two PM8 15A IPDUs are daisy-chained through Serial Port 1.

**Table 7-4:** Expert > View IPDUs Unit Information

| | **Description** | **Example** |
|---|---|---|
| **Model** | AlterPath PM model number | PM8 15A |
| **Software Version** | AlterPath PM firmware version | 1.5.0 |
| **Alarm Threshold** | Number of amperes that triggers an alarm or syslog message if it is reached | 15.0A |
| **Current** | Current level on the IPDU | 0.0A |
| **Maximum Detected** | Maximum current detected | 0.4A |
| Clear Max Detected Current | Button to reset the maximum detected current value. | |
| **Temperature** | Temperature on the IPDU (Displayed if equipped with a temperature sensor.) | N/A |
| **Maximum Detected** | Maximum temperature detected on the IPDU | N/A |
| Clear Max Detected Temperature | Button to reset the maximum detected temperature value. | |

### ▼ *To View and Reset IPDU Information*

1. Go to Applications > IPDU Power Mgmt. >View IPDUs Info.

   The “View IPDUs Info” form appears.

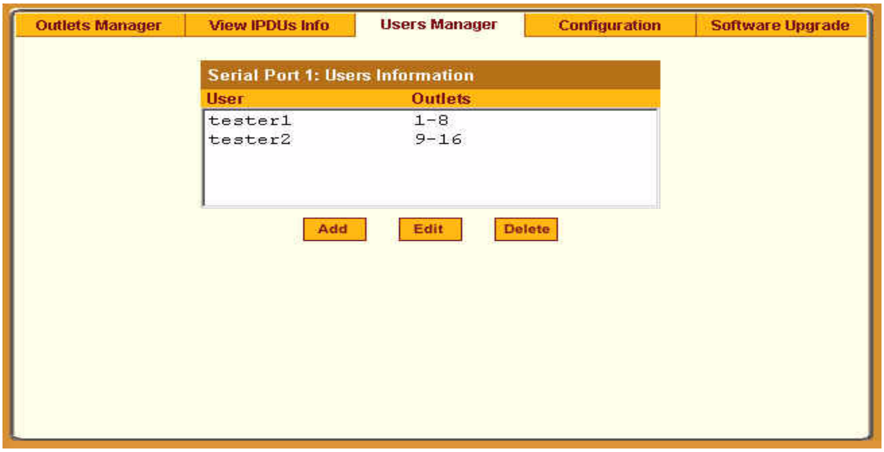
2. To clear the stored values for the maximum detected current, select the “Clear Max Detected Current” button.

3. To clear the stored values for the maximum detected temperature, click the “Clear Max Detected Temperature” button.

## Users Manager

On the “Users Manager” form under Applications > IPDU Power Mgmt., you can assign users to outlets.

The following figure shows the form with two users listed for a dual AlterPath PM. The AlterPath PM is connected to serial port 1, which is configured for power management.



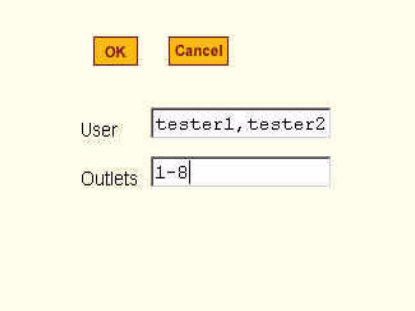
Serial Port 1: Users Information

| User | Outlets |
|---|---|
| tester1 | 1-8 |
| tester2 | 9-16 |

**Figure 7-10:** IPDU Power Mgmt> Users Manager

If more than one serial port is configured for power management, multiple users lists appear, one for each IPDU power management port.

Clicking “Add” brings up the following dialog box where you can specify one or more comma-separated user names and one or more outlets.

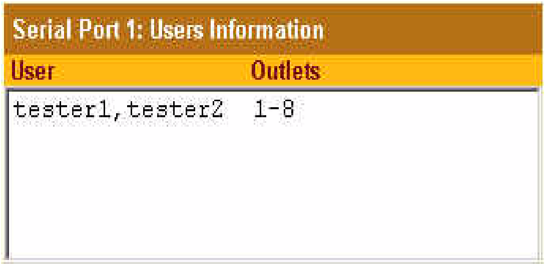


User tester1,tester2

Outlets 1-8

**Figure 7-11:** Expert > IPDU Power Mgmt. > Users Manager > Add User

When a user is added, their name is added to the list on the Users Manager form, as shown in the following figure.



Serial Port 1: Users Information

| User | Outlets |
|---|---|
| tester1,tester2 | 1-8 |

## ▼ *To Configure Users to Manage Power Outlets on IPDUs*

**1.** Go to Applications > IPDU Power Mgmt. > Users Manager.

The “Users Manager” form appears.

**2.** To disable a user’s ability to manage power, select the username from the Users Information list and then click “Delete.”

**3.** To edit a user, select the username from the Users Information list and then click “Edit.”

The “Add/Edit User x Outlets” dialog box appears.

**4.** To add a new user, click “Add.”

The “Add/Edit User x Outlets” dialog box appears.

**5.** In the “Add/Edit User x Outlets” dialog box, do the following as appropriate.

**a.** Enter the username in the “User” field.

**b.** Enter or modify the numbers of the outlets to which the user is assigned in the “Outlets” field.

Use a comma to separate outlet numbers, and use a hyphen to indicate a range of outlets (for example: 1, 3, 4, 6-8).

**6.** Click OK.

The Users Information list displays the changes.

**7.** Click “apply changes.”

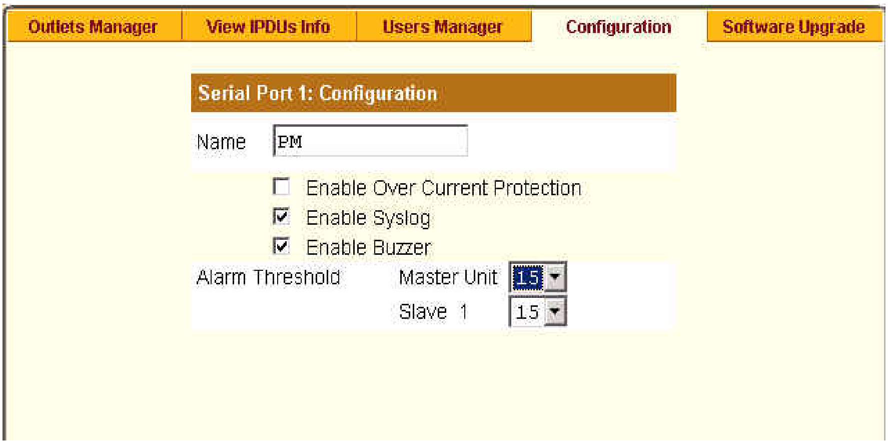
## Configuration

On the “Configuration” form under Applications > IPDU Power Mgmt., you can specify the following:

- An alias for the IPDU
- A threshold current between 1 and xx amperes. (The maximum current depends on the AlterPath PM model. Refer to "View IPDUs Info" section to determine your PM model.
- Any of the following actions to occur if the threshold current is exceeded on the IPDU.
    - Over-current protection. If enabled, the outlets on the IPDU cannot be turned on, when the current on the IPDU exceeds the selected threshold.
    - Syslog messages are generated
    - Buzzer sounds if the current exceeds the defined threshold

The Configuration form shows an entry for each serial port that has an AlterPath PM IPDU connected to, and is configured for power management. The first connected IPDU is called the *master*, the second and subsequently-connected IPDUs are called *slaves*. On the form “Master Unit” refers to the first or only connected IPDU. When IPDUs are daisy-chained, the form displays additional lines to allow you to specify separate alarm thresholds for slave IPDU(s).

The following figure shows the Configuration form when two AlterPath PMs are connected to Serial port 1 configured for power management.



Serial Port 1: Configuration

Name PM

□ Enable Over Current Protection

☑ Enable Syslog

☑ Enable Buzzer

Alarm Threshold Master Unit 15

Slave 1 15

**Figure 7-12:** Expert > Applications > IPDU Power Mgmt. > Configuration

**Note:** The number of amps shown in the Master Unit (and Slave units if available) pull-down menu varies according to the model of the connected PM. Figure 7-12 shows number 15 for two 15 amp PMs as a Master and a Slave.

### ▼ *To Specify Names, Alarms, Syslogging, and Over Current Protection for IPDUs*

Perform this procedure if you want to specify an alias or configure a threshold current to trigger alarms, syslogging, or over-current protection for an IPDU.

1. Go to Applications > IPDU Power Mgmt. > Configuration.
2. The Configuration form displays entries for all ports configured for power management. Perform the following steps for each IPDU.
   a. Assign a name to the IPDU in the “Name” field, if desired.
   b. For each AlterPath PM, click the appropriate check boxes to enable or disable Over Current Protection, the generation of Syslog files, and the sounding of a Buzzer.

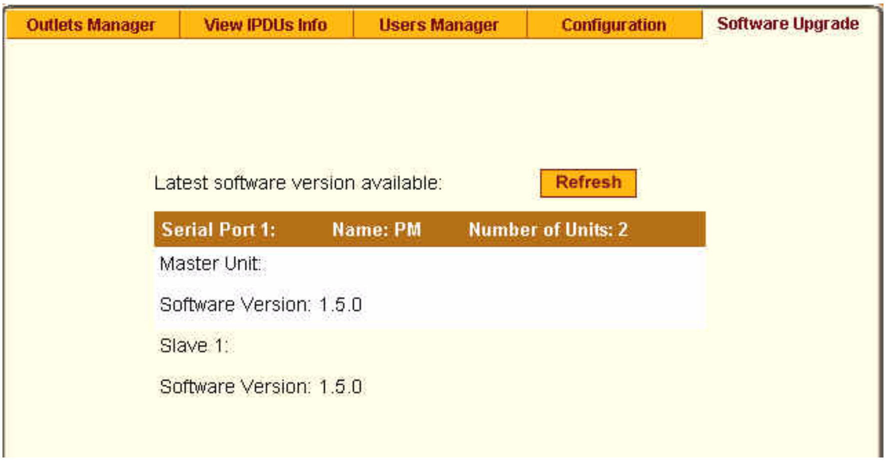
      All of the selected actions occur if a defined threshold is exceeded on the IPDU.
   c. If enabling over-current protection, a buzzer, or alarm notification, select an Alarm Threshold from the pull-down menu.

3. Click “apply changes.”

## Software Upgrade [for the AlterPath PM]

On the “Software Upgrade” form under Applications > IPDU Power Mgmt., you can upgrade the software on AlterPath PM IPDUs.

The following figure shows the Software Upgrade form listing the current software version on the AlterPath PM IPDU connected to Serial Port 1.



Latest software version available:

Serial Port 1: Name: PM Number of Units: 2

Master Unit:

Software Version: 1.5.0

Slave 1:

Software Version: 1.5.0

**Figure 7-13:** Expert > Applications > IPDU Power Mgmt. > Software Upgrade

An entry for each serial port configured for power management, and information about each directly-connected PM is displayed. The primary connected IPDU is referred to as the “master”, and any daisy-chained PMs are called “slaves.” The form displays the version number of the software that is currently installed on each PM.

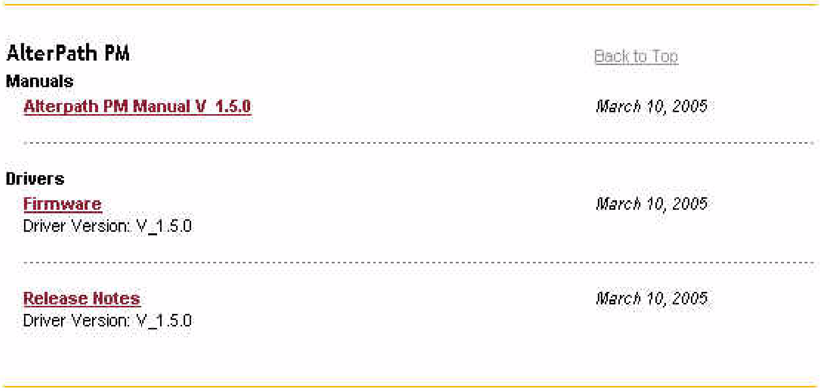
To upgrade IPDU software using this form, you first must download a more-recent version of the AlterPath PM software into the CS’s `/tmp` directory with the filename `pmfirmware`. Clicking the “Refresh” button checks for a more-recent version of the PM firmware in the `/tmp/pmfirmware` file. If the `/tmp/pmfirmware` file is present and the software version it contains is more recent than the installed version, information about the new version is displayed, and an “Update” button appears on the form.

### ▼ To Download AlterPath PM Software

You can use this procedure to download the AlterPath PM software.

1. On a computer in the same subnet as the CS, bring up a browser and go to http://www.cyclades.com/support/downloads.php
2. Find the section on the downloads page for the AlterPath PM, and compare the latest driver's version number to the version shown in the Applications > IPDU Power Mgmt. > Software Upgrade form.

   The following example shows the "AlterPath PM" section on the downloads page.



AlterPath PM

Back to Top

Manuals

Alterpath PM Manual V 1.5.0 March 10, 2005

Drivers

Firmware March 10, 2005
Driver Version: V_1.5.0

Release Notes March 10, 2005
Driver Version: V_1.5.0

   For example, the version of AlterPath PM firmware in the previous figure is Software Version: 1.5.0. In this case the software is updated. You would download it if it is more recent than the version shown on the form.

3. Click the "Firmware" link.
4. In the version directory, click the name of the binary you want to download.

   For example, `pm_150.bin` is the name of the version 1.5.0 firmware file.

5. After the download completes, copy the file to the `/tmp` folder with the name `pmfirmware.`

### ▼ To Upgrade Software on an AlterPath PM

Perform this procedure to upgrade the software on an AlterPath PM.

This procedure requires the following:

- A more-recent version of the AlterPath PM software than the one shown on the “Software Upgrade” form.
- You downloaded the more-recent version of the AlterPath PM software and copied it into the CS’s `/tmp` directory with the filename `pmfirmware`.

1. Go to Applications > Power Mgmt. > Software Upgrade.

   The Software Upgrade form displays.

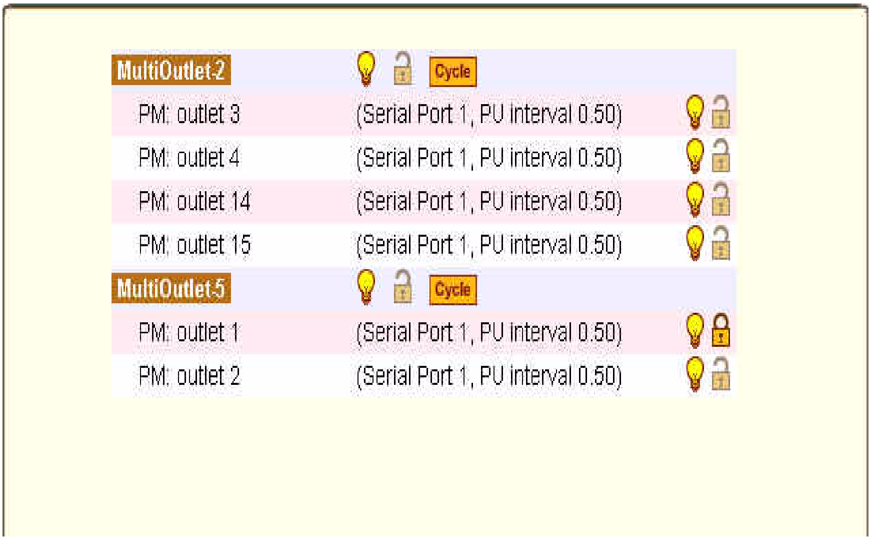
2. Click the Refresh button.

   If a `/tmp/pmfirmware` exists containing a more recent version of the PM firmware than the one currently installed, an “Update” button appears.

3. Click “Update.”
4. Click “apply changes.”

## *IPDU Multi-Outlet Ctrl*

Selecting Applications > IPDU Multi-Outlet Ctrl display the following form used for managing power on a group of outlets that provide power to a multi power supply server or device connected to a serial port.

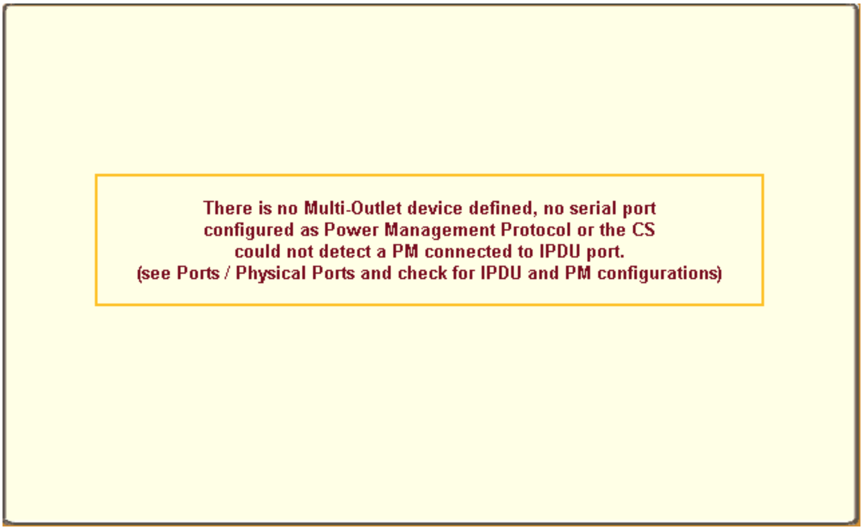


| | | |
|---|---|---|
| MultiOutlet-2 | Cycle | |
| PM: outlet 3 | (Serial Port 1, PU interval 0.50) | |
| PM: outlet 4 | (Serial Port 1, PU interval 0.50) | |
| PM: outlet 14 | (Serial Port 1, PU interval 0.50) | |
| PM: outlet 15 | (Serial Port 1, PU interval 0.50) | |
| MultiOutlet-5 | Cycle | |
| PM: outlet 1 | (Serial Port 1, PU interval 0.50) | |
| PM: outlet 2 | (Serial Port 1, PU interval 0.50) | |

**Figure 7-14:** Expert > Applications > IPDU Multi-Outlet Ctrl

Whether the power supplies are connected to the same PM or not, all outlets that are configured to the same serial port can be treated as a group and controlled simultaneously from this form.

The following form displays if Multi-Outlet Ctrl is not configured. For the procedure, see “To Configure a Serial Port for IPDU or IPMI Power Management” on page 143.”



There is no Multi-Outlet device defined, no serial port
configured as Power Management Protocol or the CS
could not detect a PM connected to IPDU port.
(see Ports / Physical Ports and check for IPDU and PM configurations)

**Figure 7-15:** Expert > Applications > Multi-Outlet Ctrl [not configured]

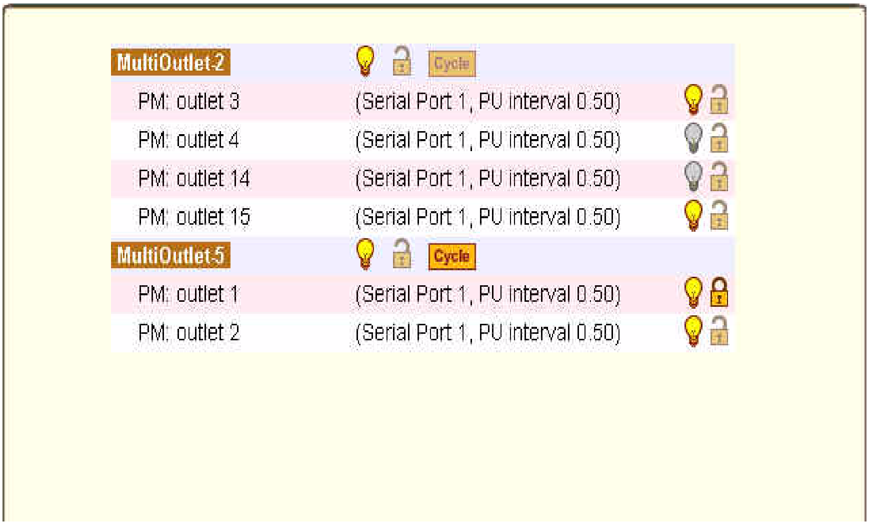
## Prerequisites for Multi-Outlet Control

In order to control groups of outlets from the IPDU Multi-Outlet Control page, the following prerequisites must be met.

- An AlterPath PM must be plugged into one of the serial ports, and that serial port must be configured for power management.
- A device connected to a serial port must be plugged into at least two outlets on the PM.
- The PM and the outlet numbers to which the device is plugged must be configured on the serial port that the device is connected to.

## Power Management Icons

In the first line of each group, the light bulb and the lock icons as well as the Cycle button operate over the entire group. The light bulb and lock icons next to the individual outlets are used to display the status of each outlet but cannot be used to control the individual outlets.



| | | |
|---|---|---|
| MultiOutlet-2 | 💡 🔓 Cycle | |
| PM: outlet 3 | (Serial Port 1, PU interval 0.50) | 💡 🔓 |
| PM: outlet 4 | (Serial Port 1, PU interval 0.50) | 💡 🔓 |
| PM: outlet 14 | (Serial Port 1, PU interval 0.50) | 💡 🔓 |
| PM: outlet 15 | (Serial Port 1, PU interval 0.50) | 💡 🔓 |
| MultiOutlet-5 | 💡 🔓 Cycle | |
| PM: outlet 1 | (Serial Port 1, PU interval 0.50) | 💡 🔒 |
| PM: outlet 2 | (Serial Port 1, PU interval 0.50) | 💡 🔓 |

**Figure 7-16:** Expert > Applications > Multi-Outlet Control Icons

The icons in the first line of each group are described in the following table.

**Table 7-5:** Expert > IPDU Multi-Outlet Ctrl form icons

| Button | Purpose |
|---|---|
| 💡 💡 | A grey light bulb icon indicates that the group is off.<br>A yellow light bulb indicates that the group is on.<br>Clicking the light bulb icon once changes the power status of all of the outlets in the group. |
| 🔒 🔓 | A grey and open lock icon indicates that the outlets are unlocked and can be powered on or off.<br>A full-color, closed lock icon indicates that the outlet is locked and cannot be turned on or off.<br>Clicking the lock icon once changes the lock status of all of the icons in the group. |
| Cycle | Turn power briefly off and then on again |

**Note:** Only one outlet needs to be powered on or unlocked in order for the entire group to be considered on or unlocked. In this case, it takes two clicks to turn the power off or to lock the entire group instead of the one click. (one click is sufficient when all of the outlets are in the same state). The first click turns the other outlets on or unlocks them so that all the outlets are in the same state; the second click turns all of the outlets off or locks them.

The Cycle button operates only if all outlets of a group are turned on.

**Note:** The "power up interval" parameter configured for each outlet plays an important role in the power up sequence of multi-outlet devices because the next outlet in the group turns on only after the power up interval specified for the current outlet has elapsed. To configure this parameter go to Applications > IPDU Power Mgmt > Outlets Manager > Edit.

### ▼ To Power On or Power Off a Group of Outlets in the Same Power State

Use these instructions if all of the outlets in a group are turned either off or on.

1. Go to Applications > IPDU Multi-Outlet Ctrl.
2. To power on the group of outlets in OFF state, click the grey light bulb adjacent to the group name.
3. To power off the group of outlets in ON, click the yellow light bulb adjacent to the group name.

### ▼ To Power On or Power Off a Group of Outlets in Different Power States

Use these instructions if not all of the outlets in a group are turned either off or on.

1. Go to Applications > IPDU Multi-Outlet Ctrl.
2. To power on the group, click the yellow light bulb adjacent to the group name.

   All of the outlets turns on.
3. To power off the group, do the following steps:

a. Click the yellow light bulb icon adjacent to the group name once to turn all of the outlets off.

   All of the outlets are in the same state.

b. To turn all of the outlets on, click the grey light bulb icon adjacent to the group name.

### ▼ *To Lock or Unlock a Group of Outlets in the Same Power State*

Use these instructions if all of the outlets in a group are either locked or unlocked.

1. Go to Applications > IPDU Multi-Outlet Ctrl.
2. To lock the group of outlets, click the open padlock icon adjacent to the group name.
3. To unlock the group of outlets, click the closed padlock icon adjacent to the group name.

### ▼ *To Lock or Unlock a Group of Outlets in Different Lock States*

Use these instructions if not all of the outlets in a group are locked or unlocked.

1. Go to Applications > IPDU Multi-Outlet Ctrl.
2. To lock the group of outlets, do the following steps:
   a. Click the open padlock icon adjacent to the group name once to unlock all of the outlets.

      All of the outlets are in the same state (open padlock).

   b. To lock all of the outlets, click the open padlock icon adjacent to the group name.
3. To unlock the group of outlets, click the closed padlock icon adjacent to the group name.

### ▼ *To Turn the Power of a Group of Outlets Off and On Again*

This procedure works only with groups of outlets that are all turned on.

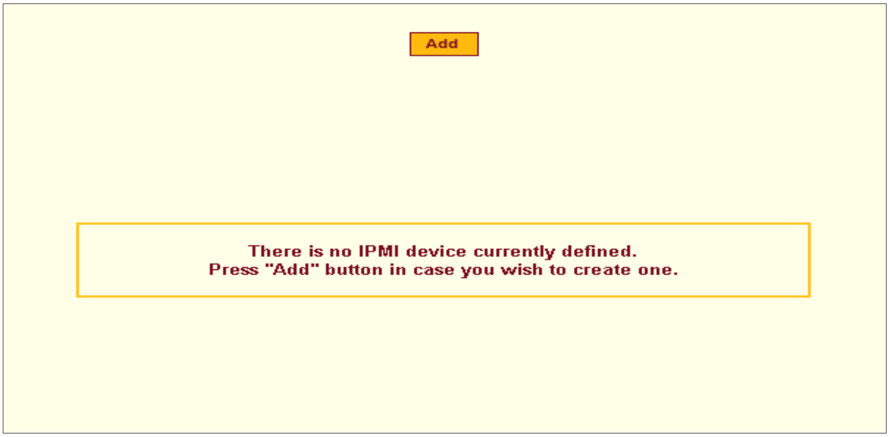
1. Go to Applications > IPDU Multi-Outlet Ctrl.
2. Make sure that all of the outlets are turned on.
3. See “To Power On or Power Off a Group of Outlets in the Same Power State” on page 137 if needed.
4. Click the Cycle button adjacent to the group name.

## *IPMI Power Management*

Intelligent Platform Management Interface or IPMI refers to the monitoring and control functions that are built into the platform hardware and primarily is used for monitoring a server’s hardware such as temperature, voltage, and errors.

On the “IPMI Power Mgmt.” form under “Applications”, you can enable and perform power management of devices that have IPMI controllers.

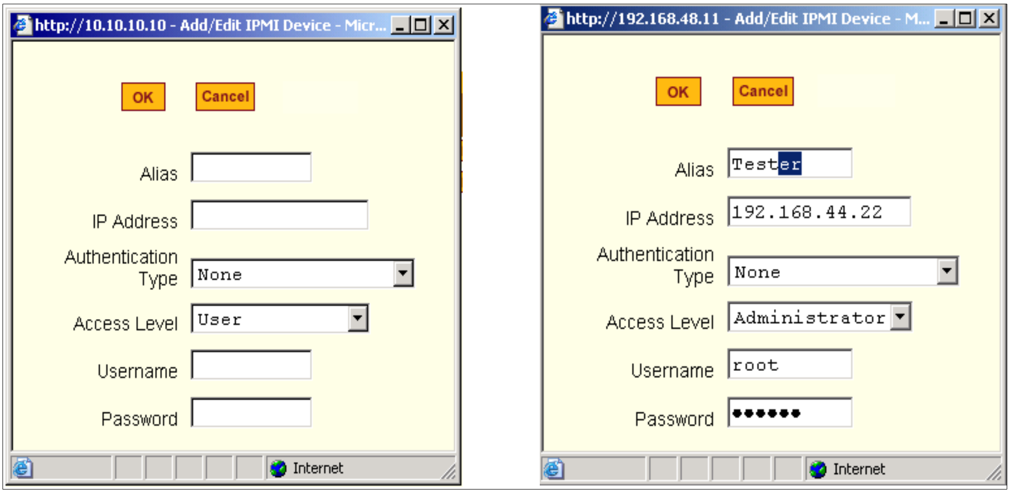
As shown in the following figure, if no IPMI devices have been added previously, only the “Add” button appears.



There is no IPMI device currently defined.
Press "Add" button in case you wish to create one.

**Figure 7-17:** Expert > Applications > IPMI Power Mgmt.

When an “Add” button or “Edit” button is pressed, a form appears for adding or editing a device.

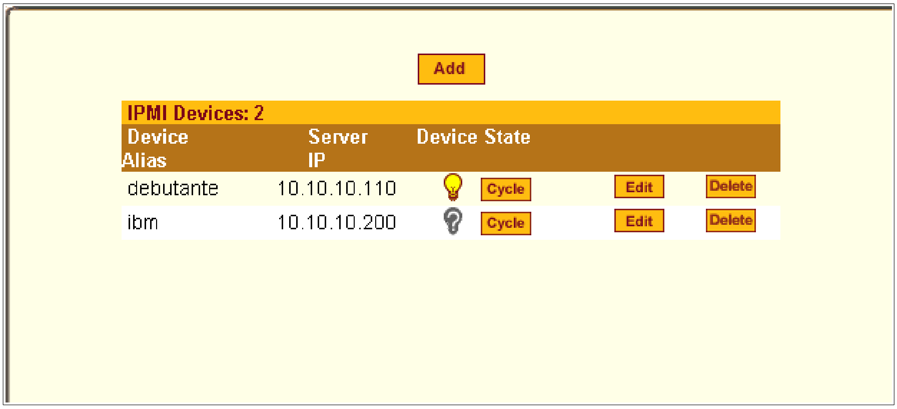

http://10.10.10.10 - Add/Edit IPMI Device - Micr...
OK
Cancel
Internet
http://192.168.48.11 - Add/Edit IPMI Device - M...
OK
Cancel
Internet

| | |
|---|---|
| Alias | |
| IP Address | |
| Authentication Type | None |
| Access Level | User |
| Username | |
| Password | |

| | |
|---|---|
| Alias | Tester |
| IP Address | 192.168.44.22 |
| Authentication Type | None |
| Access Level | Administrator |
| Username | root |
| Password | •••••• |

**Figure 7-18:** Expert > IPMI Power Mgmt. “Add/Edit IPMI Device” Dialog Boxes

After you fill out the fields or make changes and save the changes, the device is added to the IPMI Devices list or the configuration for the device is changed. The following figure shows an entry for an IPMI server.



IPMI Devices: 2

| Device Alias | Server IP | Device State | | | |
|---|---|---|---|---|---|
| debutante | 10.10.10.110 | 💡 | Cycle | Edit | Delete |
| ibm | 10.10.10.200 | 💡 | Cycle | Edit | Delete |

**Figure 7-19:** Expert > IPMI Power Mgmt. Device Entry Example

Once an IP address for a device is added to the list of IPMI devices on this form, any user authorized for power management can turn power on and off and cycle power for the IPMI device through the Web Manager. Also, users authorized to connect to serial ports can perform IPMI power management on a serially-connected device while connected.

To configure power management of IPMI devices the following CS information must be obtained from the IPMI device's administrator.

**Table 7-6:** Expert > IPMI Information

| Field Name | Description |
|---|---|
| **Device Alias** | Optional |
| **IP Address** | IP address of the device on the network |
| **Authentication type** | None, Straight Password, MD5, MD2 |
| **Access Level** | (User/Operator/Administrator) Default is User. |
| **Username** | Default is NULL user. |
| **Password** | Password for administering the remote device |

The information is updated in the `/etc/portslave/pslave.conf` and `/etc/IPMIServer.conf` files.

The "admin" or user in the "admin" group can Add, Edit, or Delete an IPMI device in an IPMI Devices List. The user with power management privileges can manage power on listed IPMI devices.

The following table describes the icons available in the IPMI Power Mgmt. form.

**Table 7-7:** Expert > IPMI Power Mgmt. Form Icons

| Button | Purpose |
|---|---|
| 💡 | A yellow light bulb indicates the current state of the device. Clicking the light bulb icon toggles the state of the device. |

| Button | Purpose |
|---|---|
| ? | When the status is unknown, a question mark appears instead of the light bulb. A question mark indicates either of the following conditions.<br>• The device was added or deleted and the changes were not saved.<br>• The device did not answer IPMI requests. |
| Cycle | Turn power briefly off and then on again |
| Add | Add and configure a new IPMI device. |
| Edit | Select an IPMI device to review or change its configuration. |
| Delete | Delete an IPMI device. |

### ▼ *To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management*

**1.** Go to Applications> IPMI Power Mgmt.

The IPMI Power Management form appears.

**2.** To delete a previously added IPMI device, click the “Delete” button on the line with the device’s name.

**3.** To add a device, click the “Add” button, and perform the following steps.

**a.** Enter an alias for the device in the “Alias:” field, if desired.

**b.** Enter the IP address of the IPMI device in the “IP Address” field.

**c.** Choose an authentication type, if desired, from the “Authentication Type” pull-down menu.

**d.** Choose a user permission type from the “Access Level” pull-down menu.

The default is “User.”

**e.** Enter a Username.

f. Enter a password for administering the remote device in the "Password" field and go to Step 5.

4. To edit the configuration for a device, click the "Edit" button on the line with the device's name, and make the desired changes on the Edit dialog box.
5. Click OK.
6. Click "apply changes."

### ▼ *To Manage Power on an IPMI Device*

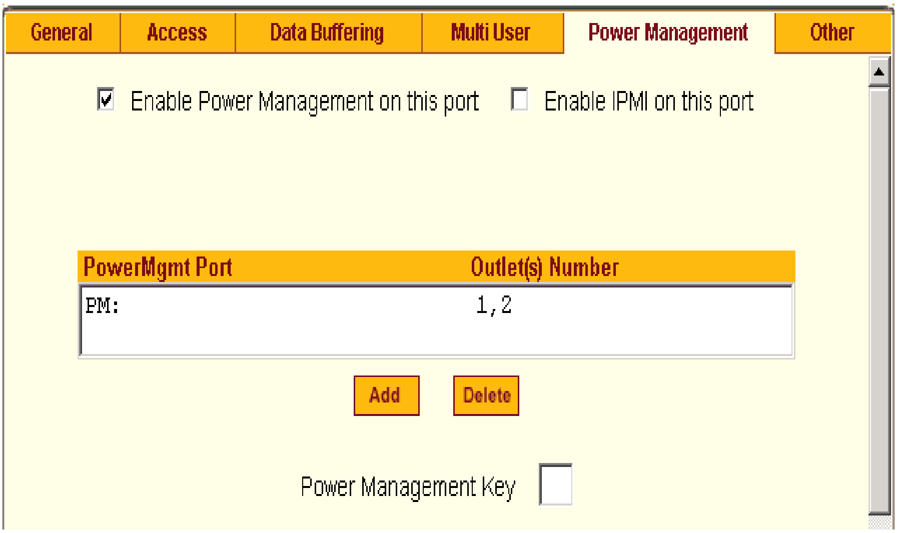
1. Go to Applications > IPMI Power Mgmt.

   Entries for all previously-defined IPMI devices appear on the form.
2. To toggle the state of a device, click the adjacent light bulb icon.
3. To briefly turn the power off then on again, click the "Cycle" button.

### ▼ *To Configure a Serial Port for IPDU or IPMI Power Management*

1. Go to Ports > Physical Ports
2. To select a port or ports to modify, click the appropriate "Modify Ports" button, and then the "Power Management" tab.
3. 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.".

   The following form appears.



☑ Enable Power Management on this port ☐ Enable IPMI on this port

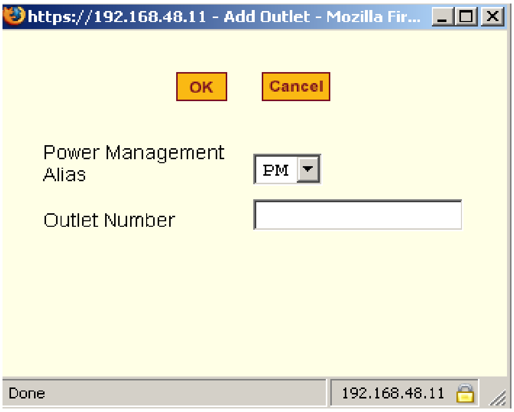
| PowerMgmt Port | Outlet(s) Number |
|---|---|
| PM: | 1,2 |

Power Management Key □

**Figure 7-20:** Expert > Serial Port > Power Management > Enable Power Management

4. Click the “Add” button

   The “Add Outlet” dialog box appears.



Power Management Alias: PM

Outlet Number:

**Figure 7-21:** Expert > Power Management Add Outlet Dialog Box

5. Enter the outlet number(s) - separated by comma - into which the device is connected to.

6. Click OK.

The power management port and the specified outlet numbers display on the PowerMgmt Port list.

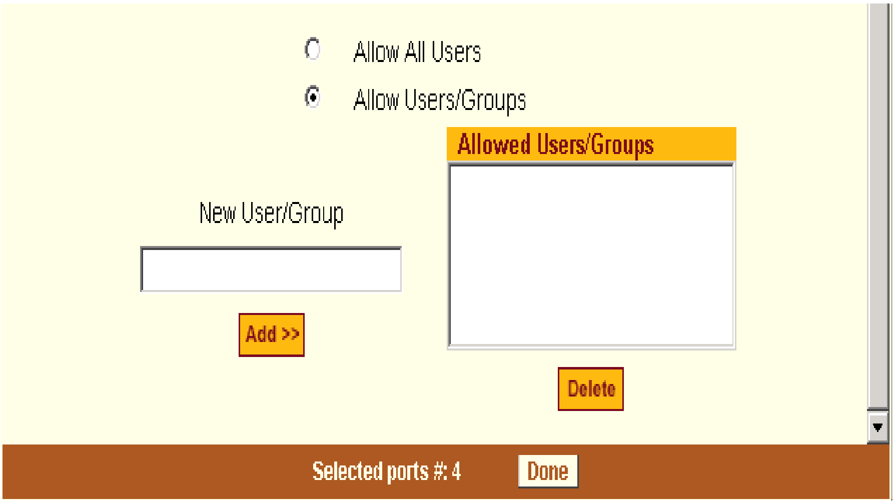
7. Enter the power management hot key in the “Power Management Key” field.

   Enter a caret (^) for the escape key, as in `^p`. The caret stands for the `Ctrl` key.

### ▼ *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 for a device while connected to the device through one of the CS’s serial ports.

1. To allow everyone with access permissions for this port to perform power management on this port, click the “Allow All Users” radio button.
2. To restrict power management on this port to a restricted list of users authorized to access this port, click the “Allow Users/Groups.”



○ Allow All Users

● Allow Users/Groups

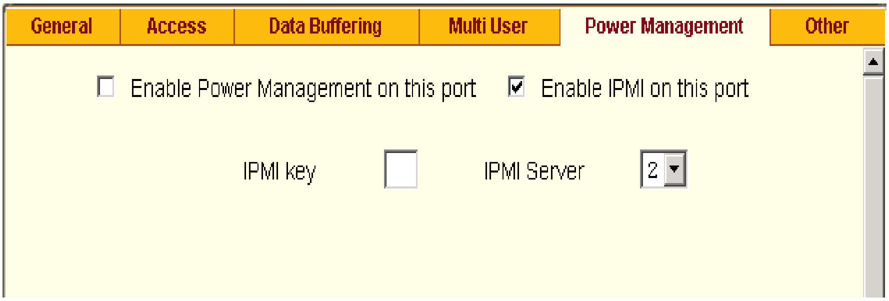
**Figure 7-22:** Expert > Serial Port > Power Management > User Permissions

3. Enter a valid username or groupname in the “New User/Group” field, and click “Add.”
4. Click “Done.”
5. Click “apply changes.”

### ▼ *To enable IPMI Power Management of an IPMI device connected to the currently-selected port*

**1.** Check the checkbox next to “Enable IPMI on this port.”

The “IPMI key” and “IPMI Server” fields appear.



□ Enable Power Management on this port ☑ Enable IPMI on this port

IPMI key □ IPMI Server 2

**Figure 7-23:** Expert > Serial Port > Power Management > Enable IPMI

**2.** Enter an IPMI hot key.

A user of the device connected to this serial port can use this hot key to bring up the IPMI power management screen while connected to the port.

Enter the key combination in the IPMI key field with `^`, as in `^I`. The caret (`^`) stands for the `Ctrl` key.

**Note:** The default IPMI hot key is “^I”. The hexadecimal code for the <Ctrl-I> is the same as the keyboard’s <Tab> key. You can choose to change the default IPMI hotkey.

**3.** Select the name of the previously-added IPMI device from the “IPMI Server” pull-down menu.

**4.** Click “Done.”

**5.** Click “apply changes.”

## *Terminal Profile Menu*

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

The following figure shows an empty menu.

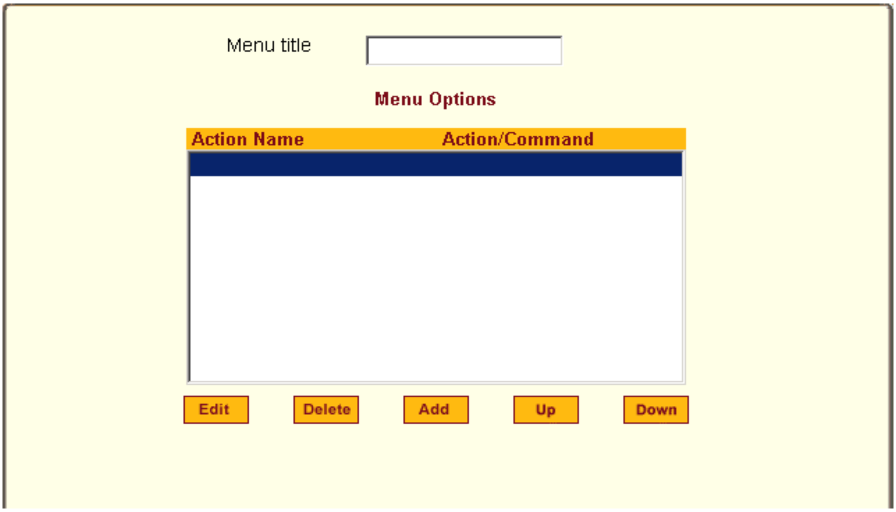


**Figure 7-24:** Expert > Applications > Terminal Profile Menu

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

When you click “Add,” the “Add Option” dialog box appears, as shown in the following figure.

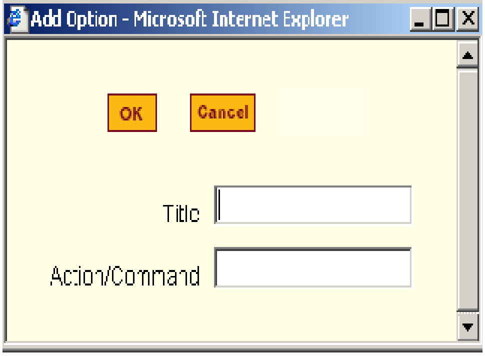
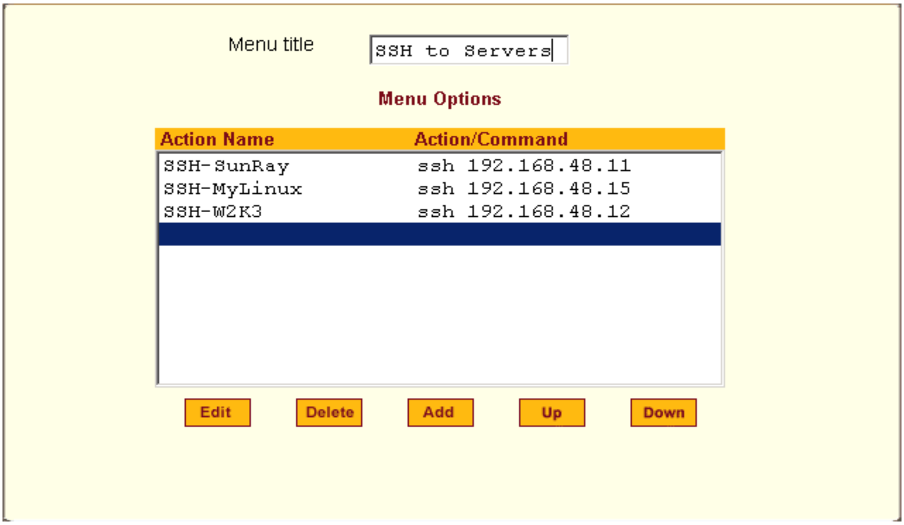


**Figure 7-25:** Expert >Terminal Profile Menu “Add Option” Dialog Box

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



Menu title: SSH to Servers

Menu Options

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

**Figure 7-26:** Expert > Terminal Profile Menu Example

The command menu then appears when the terminal is powered on.

### ▼ *To Create a Menu for a Local Computer Terminal*

1. Go to Applications > Terminal Profile Menu.

   The “Terminal Profile” menu displays.

2. Enter a title for the menu in the “Menu title” field.

3. To edit an existing menu option, select the “Action Name” from the table and then click “Edit.”

4. To add a new menu option, click “Add.”

   The “Add Option” dialog box 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.

   c. Click OK.

5. Click “apply changes.”

# Chapter 8
# Network Menu & Forms

This Chapter describes the “Network” menu and the related forms. The following table provides a description of the left menu panel and links to the detailed information and procedures.

**Table 8-1:** Expert > Network Menu

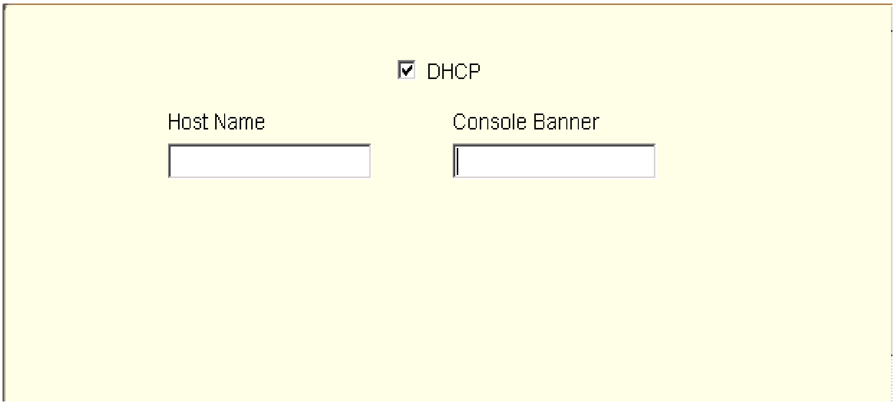
| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Host Settings** | Configure the network parameters such as Host Name, IP addresses, DNS services, Gateway, and Bonding | Page 152 |
| **Syslog** | Configure how the CS will handle its syslog messages. The CS generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit and control purposes. | Page 157 |
| **PCMCIA Management** | Configure the optional PCMCIA cards. CS supports several PCMCIA cards including modem, ISDN, GSM, CDMA, wireless LAN, Ethernet LAN, Compact Flash, and IDE drives for data buffer storage. For a list of supported PCMCIA cards see Appendix C. | Page 158 |
| **VPN Connections** | Configure one or more VPN connections to other systems or CS attached devices. | Page 176 |

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **SNMP** | Configure Simple Network Management Protocol (SNMP) with community names, OID and user names. This section and the dialog boxes guide you to configure the required parameters. | Page 181 |
| **Firewall Configuration** | Configure static IP tables, and how packets should be filtered. | Page 186 |
| **Host Tables** | View information about the local network environment. View table of hosts; create, edit, and delete hosts. | Page 201 |
| **Static Routes** | To manually add routes. Static routes are a very quick and effective way to route data from one subnet to different subnets. | Page 202 |

# Network

## *Host Settings*

When you select Network > Host Settings the following form appears.



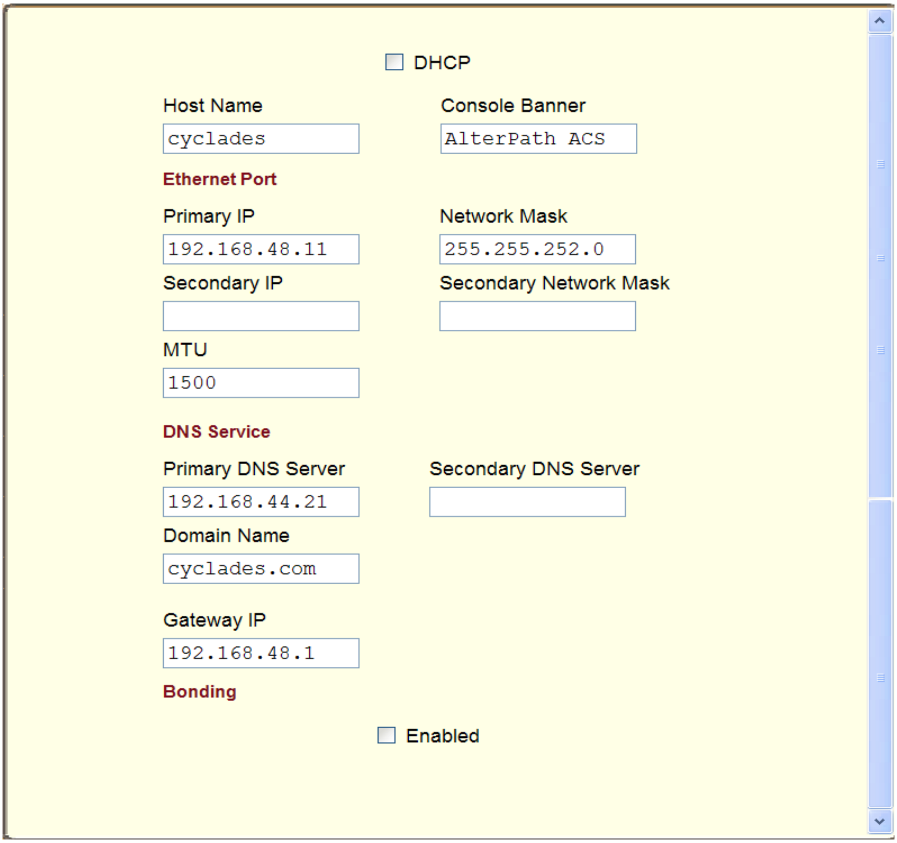
☑ DHCP

Host Name

Console Banner

**Figure 8-1:** Expert > Network > Host Settings [DHCP Enabled]

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



☐ DHCP

Host Name: cyclades

Console Banner: AlterPath ACS

**Ethernet Port**

Primary IP: 192.168.48.11

Network Mask: 255.255.252.0

Secondary IP:

Secondary Network Mask:

MTU: 1500

**DNS Service**

Primary DNS Server: 192.168.44.21

Secondary DNS Server:

Domain Name: cyclades.com

Gateway IP: 192.168.48.1

**Bonding**

☐ Enabled

**Figure 8-2:** Expert > Network > Host Settings [DHCP Disabled]

The following table provides a brief definition of the Host Settings form fields.

**Table 8-2:** Expert > Host Settings Form Fields

| Filed Name | Field Definition |
|---|---|
| **Host Name** | The fully qualified domain name identifying the specific host computer on the network. |

**Table 8-2:** Expert > Host Settings Form Fields

| Filed Name | Field Definition |
|---|---|
| **Console Banner** | A text string designed to appear on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection. |
| **Primary IP** | IP address of the CS unit. |
| **Secondary IP** | The secondary IP address of the CS unit. By configuring a second IP address, the unit will be available for more than one network. |
| **Network Mask** | The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for a subnet. |
| **Secondary Network Mask** | Optional. |
| **MTU** | Maximum Transmission Unit used by the TCP protocol. |
| **DNS Server** | Address of the Domain Name Server. |
| **Secondary DNS Server** | Address of the backup Domain Name Server. |
| **Domain Name** | The name that identifies the domain, for example, domainname.com. |
| **Gateway IP** | The IP address to the gateway on the subnet. |

**Table 8-2:** Expert > Host Settings Form Fields

| Filed Name | Field Definition |
|---|---|
| **Bonding** | Enables redundancy for the Ethernet devices using the standard Ethernet interface as the primary mode of access and a PCMCIA card as a secondary mode of access.<br>If bonding is enabled, the following values should be set.<br>**Miimon:** The interval in which the active interface is checked to see if it is still communicating (in milliseconds).<br>**Updelay**: The time that the system will wait to make the primary interface active after it has been detected as up (in milliseconds). |

**Caution:** If you have set IP Filtering rules before bonding is activated, the interface reference in the firewall configuration will be eth0. You need to change the interface to bond0 in order to reference the bonded interface. See *BLACK BOX® CS Installation, Administration, and User's Guide*, Chapter 3.

## ▼ *To Configure Host Settings [Expert]*

**1.** Go to Network > Host Settings.

The Host Settings form appears.

**2.** By default, the DHCP is enabled. To disable DHCP, click the checkbox to remove the check mark.

Additional fields appear.

**3.** Enter the name assigned to the IP address of the CS in the “Host Name” field.

**4.** Enter a console banner in the “Console Banner” field.

The console banner appears on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection

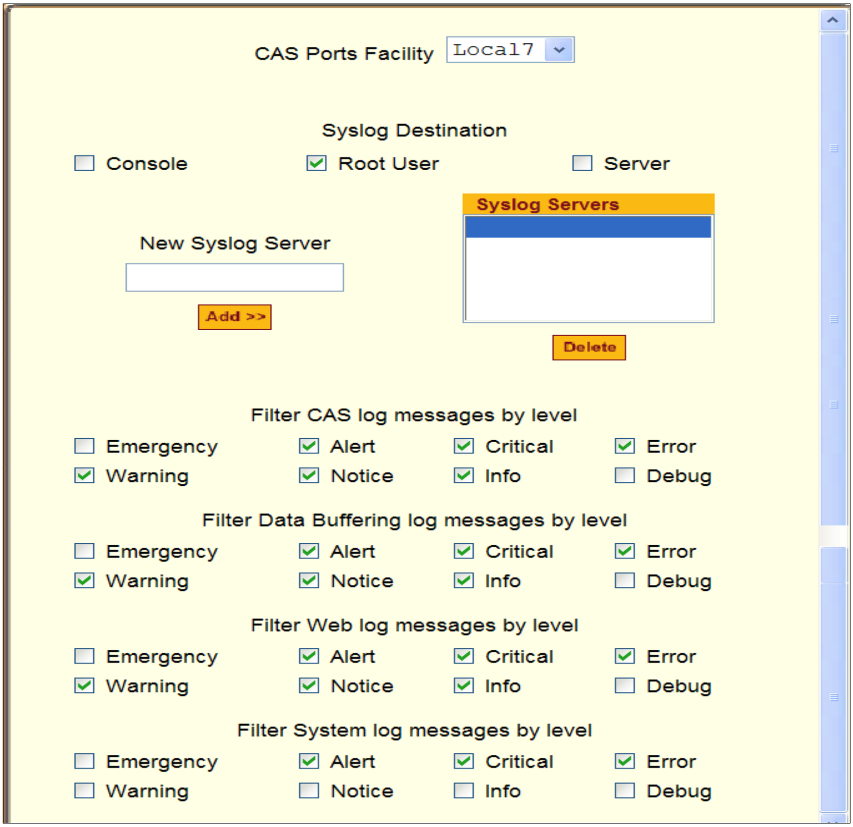
5. Under Ethernet Port, complete or edit the following fields, as necessary.
   a. Enter the IP address of the CS in the "Primary IP" field.
   b. Enter the netmask in the "Network Mask" field.
   c. If the CS has a second Ethernet card in a PCMCIA slot, enter the CS's second IP address in the "Secondary IP" field.
   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.
6. Under "DNS Service" specify or change the following information, if desired.
   a. Enter the address of the domain name server in the "Primary DNS Server" field.
   b. If there is a backup DNS server, enter the address of the secondary DNS in the "Primary DNS Server" field
   c. Enter the domain in the "Domain Name" field.
   d. Enter the IP address of the gateway in the "Gateway IP" field.
7. If you are done go to step 9. If you are enabling "Bonding" continue to step 8.
8. To activate Bonding place a checkmark in the "Enabled" field.

   "Miimon" and "Updelay" fields appear.

   a. Enter a positive integer in the "Miimon" field. This value represents the interval in which the active interface is checked to see if it is still communicating, measured in milliseconds.
   b. Enter a positive integer in the "Updelay" field. This value represents the time that the system will wait to make the primary interface active after it has been detected as up, measured in milliseconds.
9. Click "apply changes."

## Syslog

When Network > Syslog is selected the form shown in the following figure appears.



CAS Ports Facility Local7

Syslog Destination

□ Console ☑ Root User □ Server

New Syslog Server

Syslog Servers

Filter CAS log messages by level

□ Emergency ☑ Alert ☑ Critical ☑ Error
☑ Warning ☑ Notice ☑ Info □ Debug

Filter Data Buffering log messages by level

□ Emergency ☑ Alert ☑ Critical ☑ Error
☑ Warning ☑ Notice ☑ Info □ Debug

Filter Web log messages by level

□ Emergency ☑ Alert ☑ Critical ☑ Error
☑ Warning ☑ Notice ☑ Info □ Debug

Filter System log messages by level

□ Emergency ☑ Alert ☑ Critical ☑ Error
□ Warning □ Notice □ Info □ Debug

**Figure 8-3:** Expert > Network > Syslog

You can use the Syslog form to configure how the CS handles system logged messages. The Syslog form allows you to do 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 CS 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

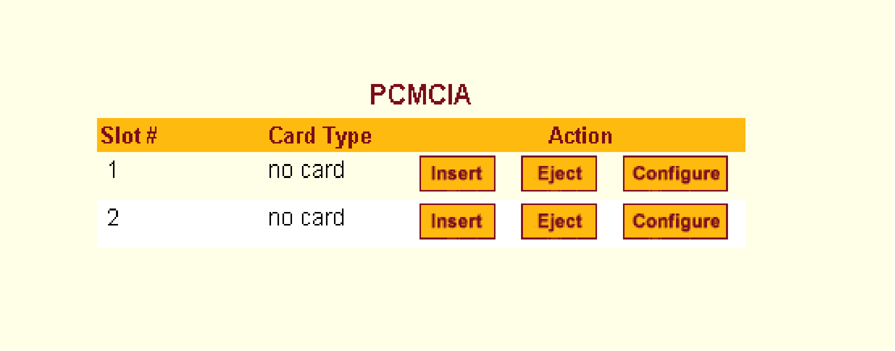
1. Go to Network > Syslog in Expert mode.

   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 the “Add>>” button.
5. Configure the message filtering as per your requirements.
6. Click “apply changes.”

## PCMCIA Management

When Network > PCMCIA Management is selected the following form appears.



PCMCIA

| Slot # | Card Type | Action | | |
|---|---|---|---|---|
| 1 | no card | Insert | Eject | Configure |
| 2 | no card | Insert | Eject | Configure |

**Figure 8-4:** Expert > Network > PCMCIA Management

You can use the PCMCIA management form to configure the following types of PCMCIA cards. For a list of the supported PCMCIA cards see Appendix C.

- 10/100 Base-T Ethernet
- 802.11b Wireless LAN
- V.90 Modem
- ISDN
- GSM
- CDMA
- Compact Flash
- IDE Hard Disk

**Note:** You can insert a card at any time and the corresponding driver should load automatically. Before removing a card, however, you must use the Web Manager to eject the card and stop the system from using the card. If you install an IDE PCMCIA card in a slot, it automatically mounts and no configuration is necessary through this form.

**Note:** CS supports GPRS and 1xRTT PCMCIA cards through a Generic Dial-Out application. For Configuration details refer to the *CS Command Reference Guide*, *Chapter 7, Section 7.3 “Generic Dial-Out”*.

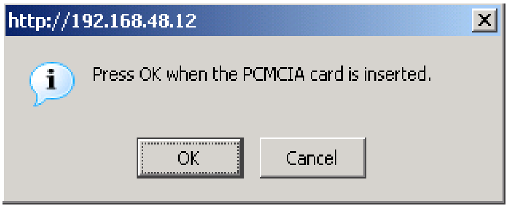
## ▼ *To Configure a PCMCIA Card*

1. Go to Network > PCMCIA Management.

   The PCMCIA Management form appears.

2. Insert the card into the PCMCIA slot on the front of the CS and Click the "Insert" button for the slot in which you installed the PCMCIA card.

   The following dialog box appears.

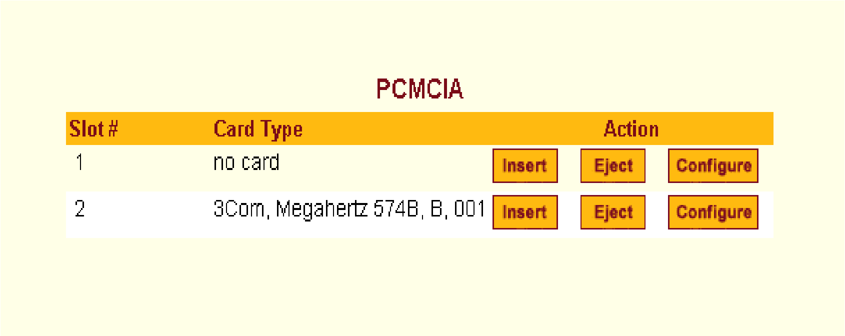


http://192.168.48.12

Press OK when the PCMCIA card is inserted.

3. Click OK.

   The card information appears under the "Card Type" column as shown in the following figure.

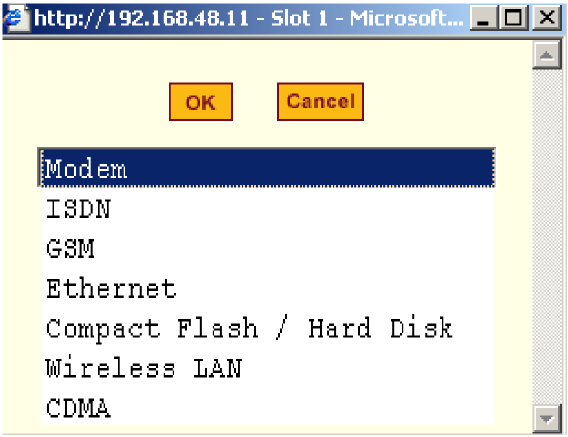


PCMCIA

| Slot # | Card Type | Action | | |
|---|---|---|---|---|
| 1 | no card | Insert | Eject | Configure |
| 2 | 3Com, Megahertz 574B, B, 001 | Insert | Eject | Configure |

4. Click the Configure button.

5. The "Slot" dialog box appears


http://192.168.48.11 - Slot 1 - Microsoft...
OK
Cancel
Modem
ISDN
GSM
Ethernet
Compact Flash / Hard Disk
Wireless LAN
CDMA

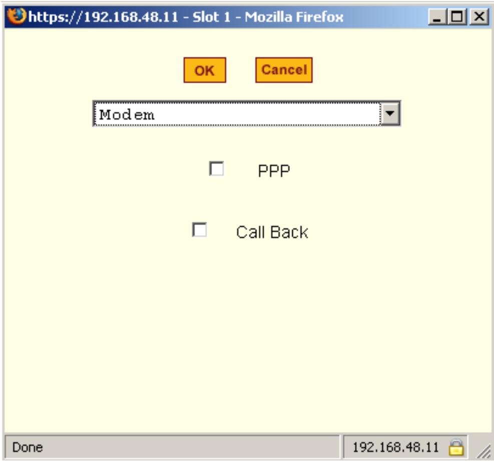
6. Select the desired PCMCIA card type from the pull-down menu.

7. Follow the procedure that corresponds to the type of the PCMCIA card you have installed.

| | |
|---|---|
| Configuring a Modem PCMCIA Card | Page 164 |
| Configuring an ISDN PCMCIA Card | Page 165 |
| Configuring a GSM PCMCIA Card | Page 168 |
| Configuring an Ethernet PCMCIA Card | Page 170 |
| Configuring a PCMCIA Compact Flash Card or a PCMCIA Hard Disk Drive | Page 171 |
| Configuring a Wireless LAN PCMCIA Card | Page 173 |
| Configuring a CDMA PCMCIA Card | Page 175 |

## Configuring a Modem PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to enable a remote user to call into the CS through an installed modem PCMCIA card. When you select Modem from the pull-down menu, the dialog box shown in the following figure appears.



Modem

☐ PPP

☐ Call Back

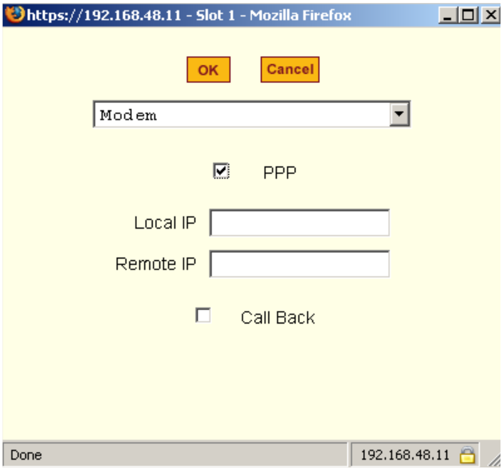
**Figure 8-5:** Expert > PCMCIA Modem Card Configuration Dialog Box

The following table provides a brief description of the fields available in the Modem dialog box.

**Table 8-3:** Expert > Form Fields for a Modem Card

| Field Name | Definition |
|---|---|
| **[PCMCIA Card]** | Pull-down menu to select the type of PCMCIA card that you are using. |
| **PPP** | Check box to enable point-to-point protocol. |
| **Local IP** | The local IP address of the PCMCIA card. |
| **Remote IP** | The remote IP address of the PCMCIA card. |
| **Call Back** | Check box to enable the callback security feature. |
| **Phone Number** | The phone number that the CS uses to call back. |

If you click the PPP checkbox, additional fields for a local and remote IP address and a “Call Back” checkbox appear, as shown in the following figure.


https://192.168.48.11 - Slot 1 - Mozilla Firefox

Modem

☑ PPP

Local IP

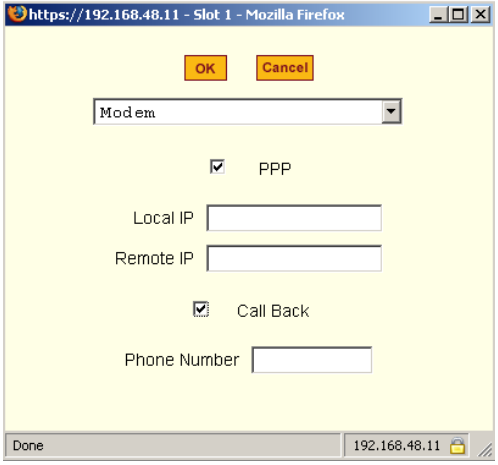
Remote IP

□ Call Back

Done 192.168.48.11

**Figure 8-6:** Expert > PCMCIA Modem Card Configuration Dialog Box - PPP

If you enable “Call Back”, the Phone Number field appears on the Slot dialog box, as shown in the following figure.


https://192.168.48.11 - Slot 1 - Mozilla Firefox

Modem

☑ PPP

Local IP

Remote IP

☑ Call Back

Phone Number

Done 192.168.48.11

**Figure 8-7:** Expert > Modem PCMCIA Card Configuration Dialog Box - Call Back

### ▼ *To Configure a Modem PCMCIA Card*

1. Install the modem card and select “Modem” from the pull-down menu on the PCMCIA Management form.
2. To enable PPP, do the following steps:
    a. Check the PPP checkbox.
    b. The “Local IP and the “Remote IP” fields, and the “Call Back” check box appear on the Slot dialog box.
    c. Enter an IP address in the “Local IP” field, if desired.

       By default, the IP address of the CS is used. Only change the IP address if you have a specific reason to do so.
    d. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

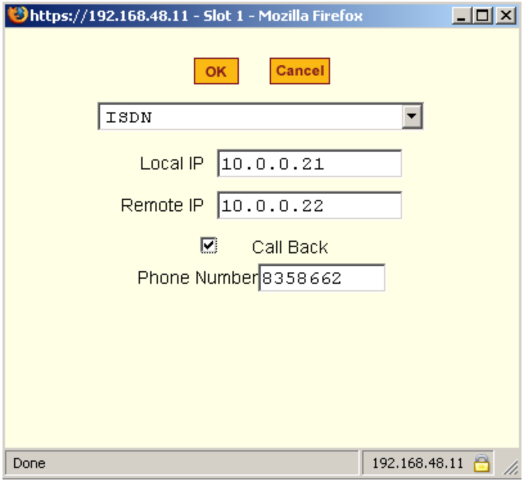
       By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.
3. To enable call back, do the following:
    a. Check the “Call Back” check box.

       The Phone Number field appears on the Slot dialog box.
    b. Enter a number to use to call back the modem.
4. Click OK.
5. Click “apply changes.”

## Configuring an ISDN PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to enable users to connect to the CS through an ISDN PCMCIA card.

When you select ISDN from the pull-down menu, the dialog box shown in the following figure appears.



ISDN

Local IP 10.0.0.21

Remote IP 10.0.0.22

☑ Call Back

Phone Number 8358662

**Figure 8-8:** Expert > ISDN PCMCIA Card Configuration Dialog Box

The following table provides a brief description of the fields available in the ISDN dialog box.

**Table 8-4:** Expert > Form Fields for an ISDN Card

| **Field Name** | **Definition** |
|---|---|
| [PCMCIA Card] | Select ISDN from the pull-down menu. |
| **Local IP** | The local IP address of the PCMCIA card. |
| **Remote IP** | The remote IP address of the PCMCIA card. |
| **Call Back** | Check box to enable the callback security feature. |
| **Phone Number** | The phone number that CS uses to call back. |

### ▼ *To Configure an ISDN PCMCIA Card*

**1.** Install the ISDN card and select “ISDN” from the pull-down menu on the PCMCIA Management form.

The “Local IP” and “Remote IP” fields and the “Call Back” check box appear on the Slot dialog box.

2. Enter an IP address in the “Local IP” field, if desired.

   By default, the IP address of the CS is used. Only change the IP address if you have a specific reason to do so.

3. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

   By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

4. To enable call back, do the following:

   a. Check the “Call Back” check box.

      The “Phone Number” field appears on the Slot dialog box.

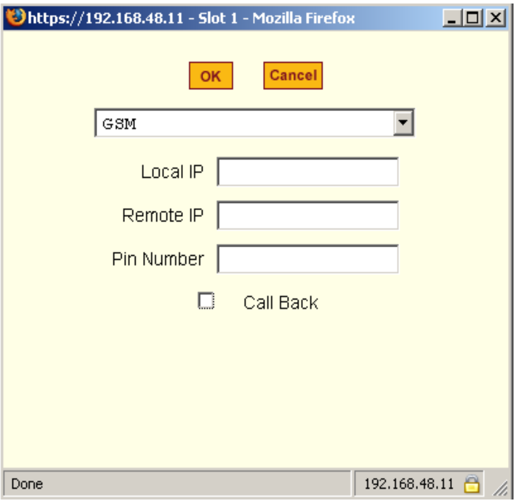
   b. Enter a number for CS to use to call back modem.

5. Click OK.

6. Click “apply changes.”

## Configuring a GSM PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to enable a remote user to call into the CS through an installed and configured GSM PCMCIA card. When you select GSM from the pull-down menu, the dialog box shown in the following figure appears.



GSM

Local IP

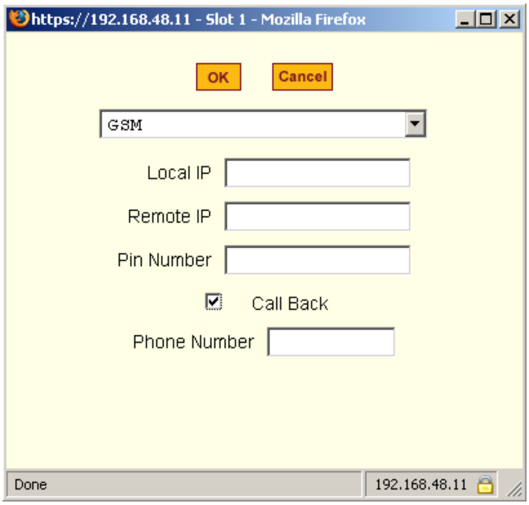
Remote IP

Pin Number

□ Call Back

**Figure 8-9:** Expert > GSM PCMCIA Card Configuration Dialog Box

When the “Call Back” checkbox is checked, the Phone Number field appears as shown in the following figure.



GSM

Local IP

Remote IP

Pin Number

☑ Call Back

Phone Number

**Figure 8-10:** Expert > GSM PCMCIA Card Configuration Dialog Box - Call Back

The following table provides a brief description of the fields available in the GSM dialog box.

**Table 8-5:** Expert > Form Fields For a GSM Card

| Field Name | Definition |
|---|---|
| [PCMCIA Card] | Select GSM from the pull-down menu. |
| **Local IP** | The local IP address of the PCMCIA card. |
| **Remote IP** | The remote IP address of the PCMCIA card. |
| **Pin Number** | The personal identification number associated with the GSM. |
| **Call Back** | Check box to enable the callback security feature. |
| **Phone Number** | The phone number that CS uses to call back. |

### ▼ *To Configure a GSM PCMCIA Card*

1. Install the GSM card and select “GSM” from the pull-down menu on the PCMCIA Management form.

   The “Local IP,” “Remote IP,” and “Pin Number” fields and the “Call Back” check box appear on the Slot dialog box.

2. Enter an IP address in the “Local IP” field, if desired.

   By default, the IP address of CS is used. Only change the IP address if you have a specific reason to do so.

3. In the “Remote IP” field, specify the IP address to assign to the other end of the PPP connection, if desired.

   By default, the IP address 10.0.0.1 is assigned. Only change the IP address if you have a specific reason to do so.

4. Enter a personal identification number known to the owner of the GSM card in the “PIN Number” field.

5. To enable call back, do the following:

   a. Check the “Call Back” check box.

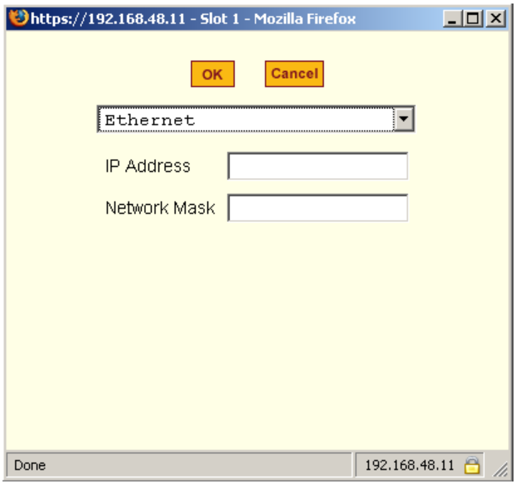
      The “Phone Number” field appears on the Slot dialog box.

   b. Enter a number for the CS to use to call back the GSM phone.

6. Click OK.
7. Click “apply changes.”

## Configuring an Ethernet PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to configure an Ethernet PCMCIA card. When you select Ethernet from the pull-down menu, the dialog box shown in the following figure appears.



Ethernet

IP Address

Network Mask

**Figure 8-11:** Expert > Ethernet PCMCIA Card Configuration Dialog Box

The following table provides a brief description of the fields available in the Ethernet dialog box

**Table 8-6:** Expert > Form Fields for an Ethernet Card.

| Field Name | Definition |
|---|---|
| [PCMCIA Card] | Select Ethernet from the Pull-down menu. |
| **IP Address** | The local IP address of the Ethernet. |

| Field Name | Definition |
|---|---|
| **Network Address** | The network address of the Ethernet. |

### ▼ *To Configure an Ethernet PCMCIA Card*

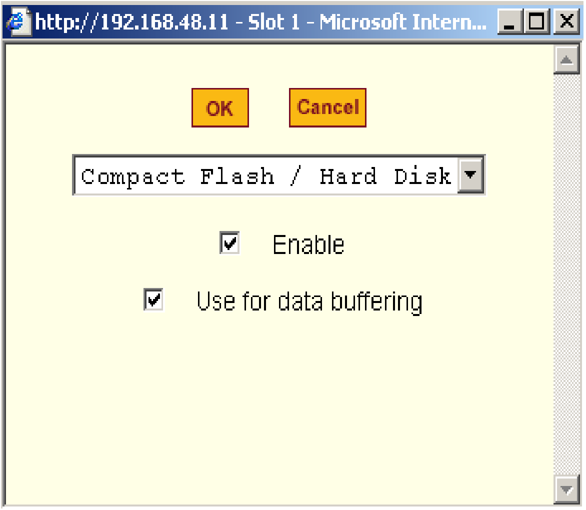
1. Install the Ethernet card and select “Ethernet” from the pull-down menu on the PCMCIA Management form.

   The “IP Address” and “Network Mask” fields appear on the Slot dialog box.

2. In the “IP address” field, enter the IP address to assign to the Ethernet port.
3. In the “Network Mask” field, enter the netmask to assign to the subnet.
4. Click OK.
5. Click “apply changes.

## Configuring a PCMCIA Compact Flash Card or a PCMCIA Hard Disk Drive

You can use the “PCMCIA Management” form under “Network” to configure a PCMCIA Compact Flash card or a PCMCIA Hard Disk Drive. When you select Compact Flash/Hard Disk from the pull-down menu, the dialog box shown in the following figure appears.



http://192.168.48.11 - Slot 1 - Microsoft Intern...

OK Cancel

Compact Flash / Hard Disk

☑ Enable

☑ Use for data buffering

**Figure 8-12:** Expert > PCMCIA Compact Flash/Hard Disk Configuration Dialog Box

The following table provides a brief description of the fields available in the Compact Flash/Hard Disk dialog box.

**Table 8-7:** Expert > Form Fields for a Compact Flash/Hard Disk

| Field Name | Definition |
|---|---|
| [PCMCIA Card] | Select Compact Flash/Hard Disk from the Pull-down menu. |
| **Enable** | Check box to enable the storage device. |
| **Use for Data Buffering** | Check box to use the storage device for data buffering. |

### ▼ *To Configure a Compact Flash PCMCIA Card or a PCMCIA Hard Disk Drive*

**1.** Install the compact flash card or the hard disk drive and select “Compact Flash/Hard Disk” from the pull-down menu on the PCMCIA Management form.

The “Enable” checkbox appears on the Slot dialog box.

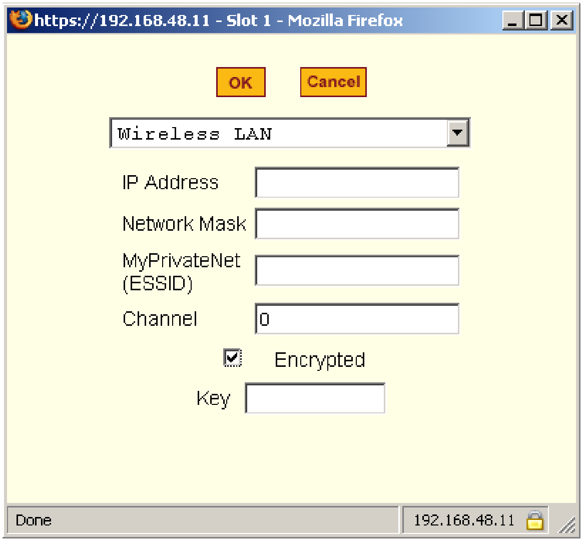
2. Click the “Enable” checkbox.

   The “Use for data buffering” checkbox appear on the Slot dialog box.

3. If desired, uncheck the “Use for data buffering” checkbox. Default is checked.
4. Click OK.
5. Click “apply changes.”

## Configuring a Wireless LAN PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to configure a Wireless LAN PCMCIA card. When you select “Wireless LAN” from the pull-down menu, the dialog box shown in the following figure appears.



https://192.168.48.11 - Slot 1 - Mozilla Firefox

Wireless LAN

IP Address:

Network Mask:

MyPrivateNet (ESSID):

Channel: 0

☑ Encrypted

Key:

Done

192.168.48.11

**Figure 8-13:** Expert > PCMCIA Wireless LAN Card Configuration Dialog Box

The following table provides a brief description of the fields available in the Wireless LAN dialog box.

**Table 8-8:** Expert > Form Fields for a Wireless LAN Card.

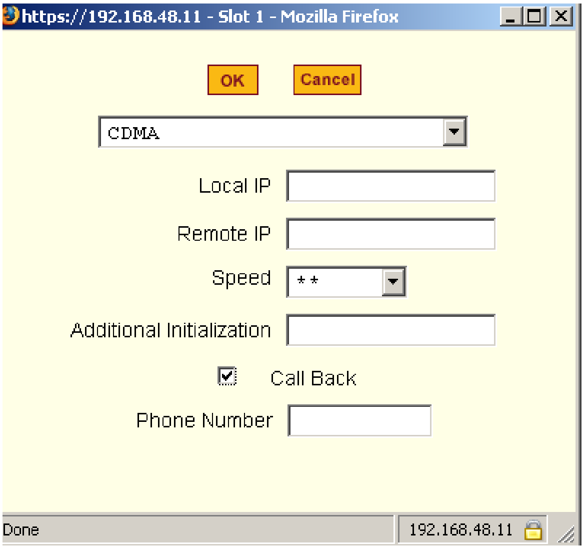
| Field Name | Definition |
|---|---|
| [PCMCIA Card] | Pull-down box to select the type of PCMCIA card that you are using. |
| **IP Address** | The local IP address of the Ethernet. |
| **Network Mask** | The network address of the Ethernet. |
| **MyPrivateNet (ESSID)** | The unique identifier for the wireless access point. |
| **Channel** | The communication channel with the access point. |
| **Encrypted** | The translation of data into code during transmission. |
| **Key** | The key or password to decode the encrypted data. |

### ▼ *To Configure a Wireless LAN PCMCIA Card*

1. Install the wireless LAN card and select “Wireless LAN” from the pull-down menu on the PCMCIA Management form.
2. In the “IP address” field, enter an IP address.
3. In the “Network Mask” field, enter the netmask for the subnet.
4. In the “MyPrivateNet (ESSID)” field, enter the SSID for communicating with others in your network.
5. In the “Channel” field, enter a channel number.
6. Click the “Encrypted” checkbox, if an encrypted data communication is required.
7. Enter a unique key for decoding the encrypted data.
8. Click OK.
9. Click “apply changes.”

## Configuring a CDMA PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to configure a CDMA PCMCIA card. When you select “CDMA” from the pull-down menu, the dialog box shown in the following figure appears.



CDMA

Local IP

Remote IP

Speed **

Additional Initialization

☑ Call Back

Phone Number

**Figure 8-14:** Expert > PCMCIA CDMA Card Configuration Dialog Box

CDMA cards are modem cards that makes it possible for CS to receive a dial-in connection and support callback feature using the "ppp" protocol.
The following table provides a brief description of the fields available in the CDMA dialog box.

**Table 8-9:** Expert > Form Fields for a CDMA Card.

| Field Name | Definition |
|---|---|
| [PCMCIA Card] | Pull-down box to select the type of PCMCIA card that you are using. |
| **Local IP** | The local IP address of the CDMA card used by the ppp connection. |
| **Remote IP** | The remote IP address of the CDMA card used by the ppp connection. |

| Field Name | Definition |
|---|---|
| **Speed** | The speed used by CS to access the card. |
| **Additional Initialization** | Additional initialization parameter to be sent to the card. CDMA configuration has a default command sequence to initialize the card, but if additional initialization command is required by the card, it will be added to default command sequence. For example, additional initialization parameters may be required in communication networks of some countries. |
| **Call Back** | Check box to enable the callback security feature |
| **Phone Number** | The phone number that CS uses to call back. |

### ▼ *To Configure a CDMA PCMCIA Card*

1. Install the CDMA card and select “CDMA” from the pull-down menu on the PCMCIA Management form.
2. In the “Local IP” field, enter the local IP address.
3. In the “Remote IP” field, enter the remote IP address.
4. Form the “Speed” pull-down menu, select the speed defined by the specifications of the CDMA card you are using.
5. In the “Additional Initialization” field, enter additional parameters if required by the card.
6. To enable call back, do the following:
   - **a.** Check the “Call Back” check box.

     The “Phone Number” field appears on the Slot dialog box.
   - **b.** Enter a number for the CS to use to call back the CDMA card.
7. Click OK.
8. Click “apply changes.”

## Ejecting a PCMCIA Card

Use the “Eject” button on the PCMCIA management form to eject any PCMCIA card before physically ejecting it. Any other method can cause a kernel panic.

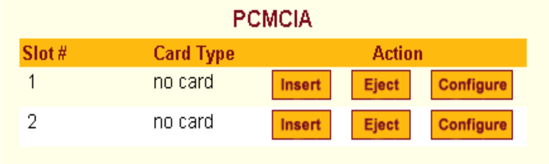
### ▼ *To Eject a PCMCIA Card From the Card Slot*

1. Go to Network > PCMCIA Management.

   The PCMCIA Management form appears.

2. Click the Eject button adjacent to the card you want to remove.

   The card type clears under the Card Type column.



PCMCIA

| Slot # | Card Type | Action | | |
|---|---|---|---|---|
| 1 | no card | Insert | Eject | Configure |
| 2 | no card | Insert | Eject | Configure |

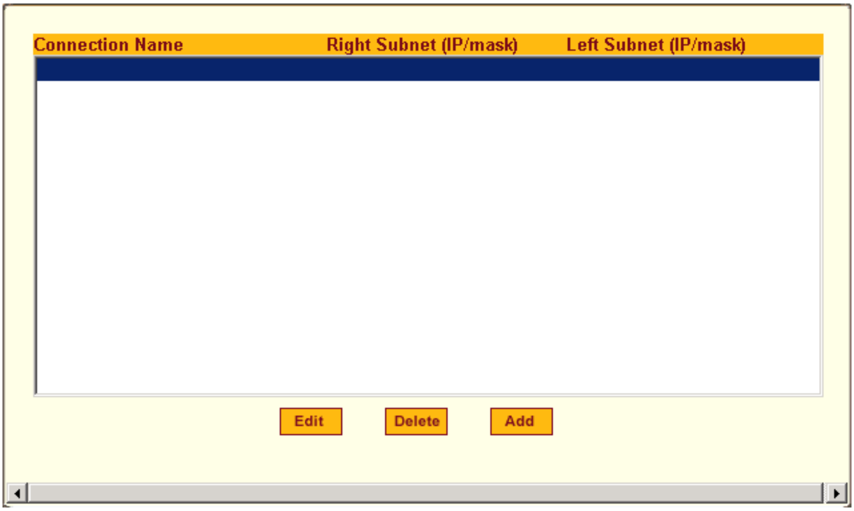
3. Click “apply changes.”

4. Physically remove the card from the PCMCIA slot on the front of the CS.

# *VPN Connections*

VPN, or Virtual Private Network enables a secured communication between CS and a remote network by utilizing a gateway, and creating a secured tunnel between CS 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.

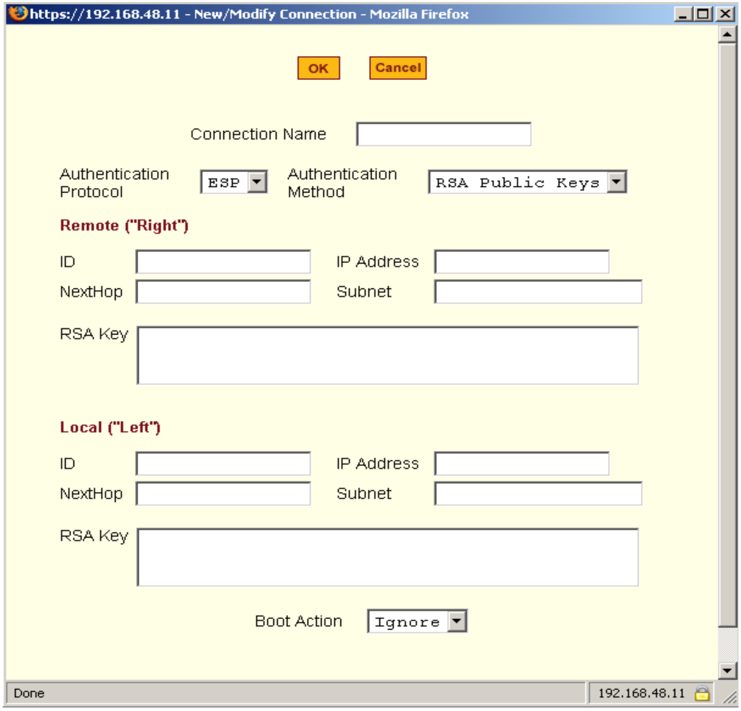
When “VPN Connections” is selected under “Network”, the form shown in the following figure appears.



| Connection Name | Right Subnet (IP/mask) | Left Subnet (IP/mask) |
|---|---|---|

**Figure 8-15:** Expert > Network > VPN Connections

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


https://192.168.48.11 - New/Modify Connection - Mozilla Firefox
OK
Cancel
Remote ("Right")
Local ("Left")
Done
192.168.48.11

Connection Name

Authentication Protocol: ESP

Authentication Method: RSA Public Keys

Remote ("Right")

ID

IP Address

NextHop

Subnet

RSA Key

Local ("Left")

ID

IP Address

NextHop

Subnet

RSA Key

Boot Action: Ignore

**Figure 8-16:** Expert > VPN “New/Modify Connection” Dialog Box

The remote gateway is referred to as the Remote or “Right” host, and the CS 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 CS 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 8-10:** Expert > Field and Menu Options for Configuring a VPN Connection

| Field Name | Definition |
|---|---|
| **Connection Name** | Any descriptive name you want 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. |
| **NextHop** | The router through which the CS (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.<br>**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 CS 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. |

| Field Name | Definition |
|---|---|
| **Boot Action** | The boot action configured for the host, either Ignore, Add, Start. |

### ▼ *To Configure VPN*

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

1. Go to Network > VPN Connections.

   The VPN Connections form appears.

2. To edit a VPN connection, select the name of the VPN connection, and click the “Edit” button.

3. To add a VPN Connection, click the “Add” button.

   The “New/Modify Connection” dialog box appears.

4. Enter any descriptive name you choose for the connection in the “Connection Name” field.

5. Select either ESP or “AH” from the “Authentication Protocol” pull-down menu.

6. Select “Shared Secret” or “RSA Public Keys” from the “Authentication Method” pull-down menu.

7. 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 CS (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.

8. Select either “Ignore”, “Add”, or “Start” from the “Boot Action pull-down menu.

9. Click OK.

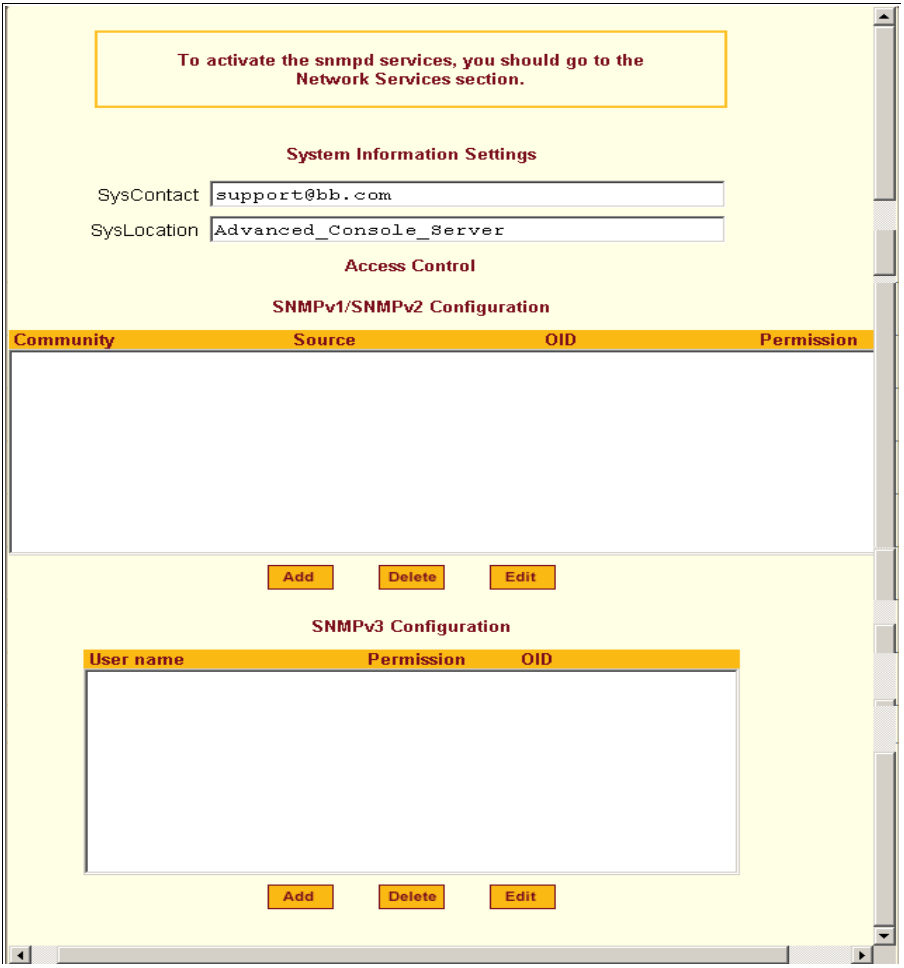
10. Click “apply changes.”

## SNMP

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

Selecting Network > SNMP brings up the form shown in the following figure.



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

System Information Settings

SysContact: support@bb.com

SysLocation: Advanced_Console_Server

Access Control

SNMPv1/SNMPv2 Configuration

| Community | Source | OID | Permission |
|---|---|---|---|

SNMPv3 Configuration

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

**Figure 8-17:** Expert > Network > SNMP

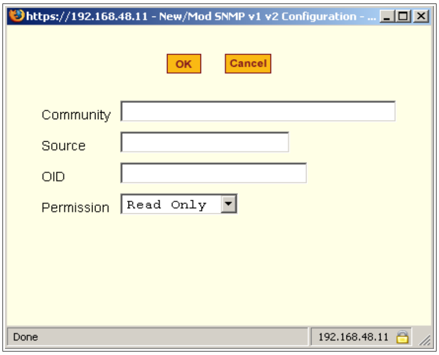
You can use this form to enable notifications about significant events or traps from CS to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager.

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

**Table 8-11:** Expert > Fields and Menu Options for SNMP Configuration

| Field or Menu Option | Description |
|---|---|
| **SysContact** | The email address of the CS's administrator, for example, `support@bb.com`. |
| **SysLocation** | The physical location of the CS. |
| **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". Take caution in using a "public" community name as it is commonly known. By default, the "public" community cannot access SNMP information on the CS. |
| **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 (Management Information Base) except for SNMP configuration objects.<br>"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" brings up the "New/Mod SNMP v1 v2 Configuration" dialog box, as shown in the following figure.


https://192.168.48.11 - New/Mod SNMP v1 v2 Configuration - ...
OK
Cancel
Done
192.168.48.11

Community

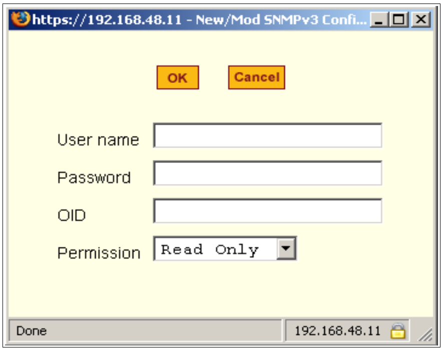
Source

OID

Permission: Read Only

**Figure 8-18:** Expert > "New/Mod SNMP v1 v2 Configuration" Dialog Box

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



User name

Password

OID

Permission: Read Only

**Figure 8-19:** Expert > "New/Mod SNMP v3 Configuration" Dialog Box

### ▼ *To Configure SNMP*

1. Go to Networks > SNMP.

   The SNMP form appears.

2. To enable any version of SNMP, do the following:

   - To add an SNMPv1/SNMPv2 entry, press the "Add" button under the "SNMPv1/SNMPv2 Configuration" table.

   - 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, do the following steps.
   a. To edit an SNMPv1/SNMPv2 entry, 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 user name in the “User name” field.
   b. Enter the password in the “Password” field.

**Note:** The SNMPv3 password must be less than 31 characters.

6. For any version of SNMP, do the following steps.
   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. The related tasks are listed in the following table.

**Table 8-12:** Expert > Tasks for Configuring SNMP

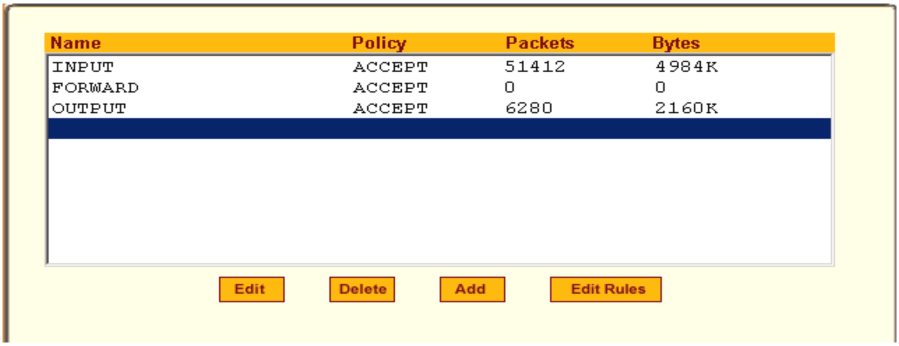
| Task | Where Documented |
|---|---|
| To configure one or more serial ports to send SNMP traps. | See “SNMP Trap Notifications Entry” on page 302 |

## Firewall Configuration

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

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

Selecting Network > Firewall Configuration brings up the form shown in the following figure.



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

**Figure 8-20:** Expert > Network > Firewall Configuration

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

Packet filtering relies on defined chains and rules. See “Packet Filtering on CS” on page 13 for details.

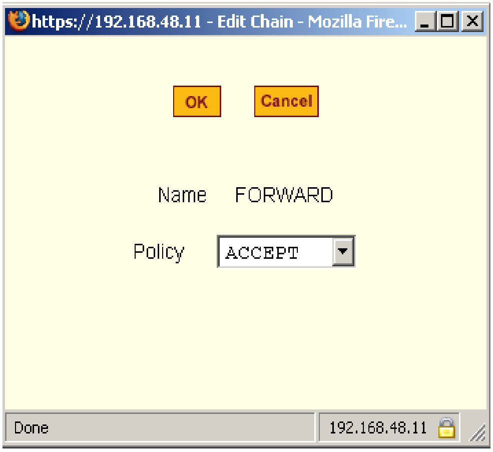
Each entry in the list on the Firewall Configuration form represents a chain with a set of rules.

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

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

### *“Edit” Button*

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



https://192.168.48.11 - Edit Chain - Mozilla Fire...

Name FORWARD

Policy ACCEPT

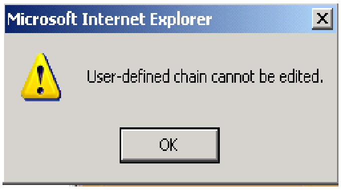
Done

192.168.48.11

**Figure 8-21:** Expert > Firewall Configuration “Edit Chain” Dialog Box

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

**Note:** User-defined chains cannot be edited. If a user-defined chain is selected for editing, the message shown in the following figure appears.


Microsoft Internet Explorer

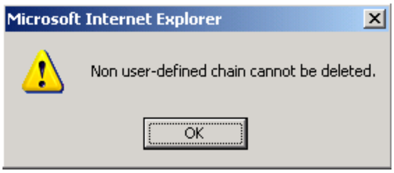
User-defined chain cannot be edited.

**Figure 8-22:** Firewall Configuration “User-defined Chain” Message

### *“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 the message shown in the following figure appears.


Microsoft Internet Explorer

Non user-defined chain cannot be deleted.

**Figure 8-23:** Firewall Configuration “Delete Default Chain” Message

### *“Add” Button*

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

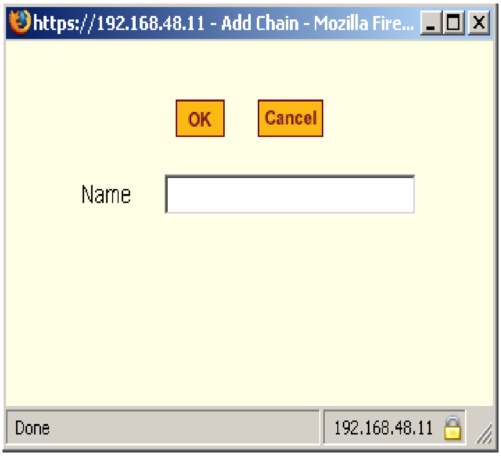
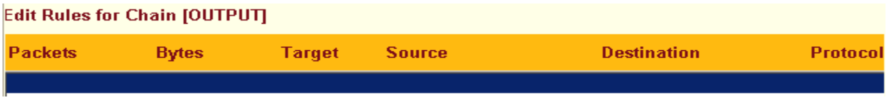


**Figure 8-24:** Expert > Firewall Configuration “Add Chain” Dialog Box

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

### *“Edit Rules” Button*

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



Edit Rules for Chain [OUTPUT]

| Packets | Bytes | Target | Source | Destination | Protocol |
|---|---|---|---|---|---|

**Figure 8-25:** Firewall Configuration “Edit Rules for chain_name” Form

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

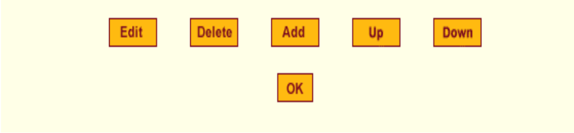
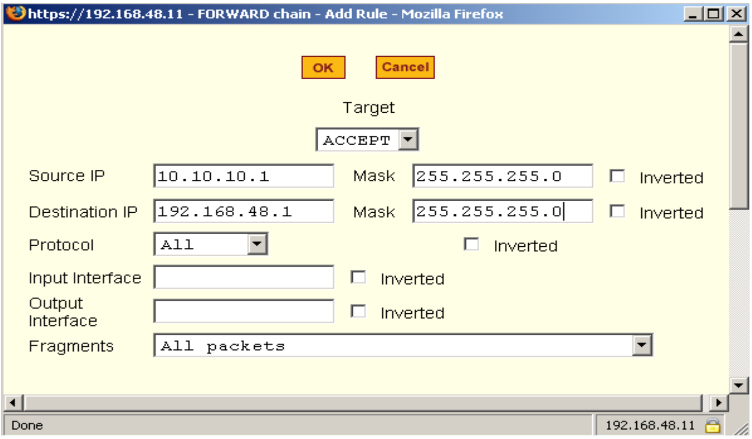


**Figure 8-26:** Firewall Configuration “Edit Rules for chain_name” Buttons

- Pressing the “Add” button opens the “Add Rule” dialog box.
- Selecting a “Rule” and pressing the “Edit” button opens the “Edit Rule” dialog box.
- Selecting a rule and pressing the “Up” and “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.


https://192.168.48.11 - FORWARD chain - Add Rule - Mozilla Firefox
OK
Cancel
Done
192.168.48.11

Target: ACCEPT

Source IP: 10.10.10.1 Mask: 255.255.255.0 □ Inverted

Destination IP: 192.168.48.1 Mask: 255.255.255.0 □ Inverted

Protocol: All □ Inverted

Input Interface: □ Inverted

Output Interface: □ Inverted

Fragments: All packets

**Figure 8-27:** 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, you select “DROP” as the target action from the “Target” drop-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. The default target pull-down menu is shown in the following figure.

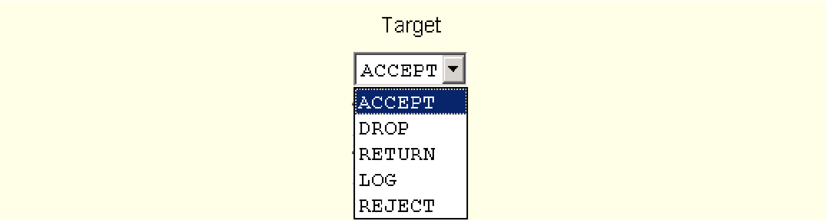


**Figure 8-28:** Firewall Configuration “Add Rule” and “Edit Rule” Target Menu Options

### 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.

The source and destination IP and related fields are shown in the following figure.

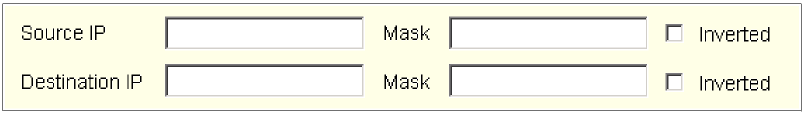


**Figure 8-29:** Firewall Configuration “Add Rule” and “Edit Rule” Source and Destination IP and Mask Fields

### Protocol

You can select a protocol for filtering. The “Protocol” pull-down menu is shown in the following figure.

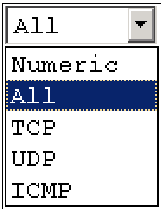


**Figure 8-30:** Firewall Configuration “Add Rule” and “Edit Rule” Protocol Menu Options

The additional 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, as shown in the following figure.

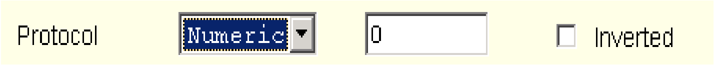
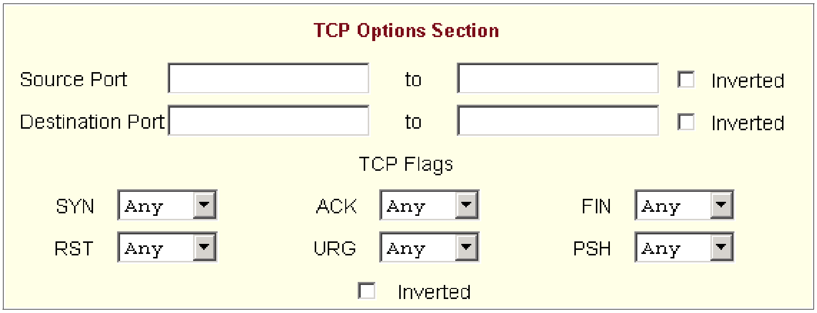

Protocol Numeric 0 □ Inverted

**Figure 8-31:** Firewall Configuration “Add Rule” and “Edit Rule” Numeric Protocol Fields

### TCP Protocol Fields

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



TCP Options Section

Source Port ________ to ________ □ Inverted

Destination Port ________ to ________ □ Inverted

TCP Flags

SYN Any ACK Any FIN Any

RST Any URG Any PSH Any

□ Inverted

**Figure 8-32:** Firewall Configuration “Add Rule” and “Edit Rule” TCP Protocol Fields and Menu Options

The following table defines the fields and menu options in the “TCP Options Section.”

**Table 8-13:** Expert > TCP Options Fields

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

### *UDP Protocol Fields*

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

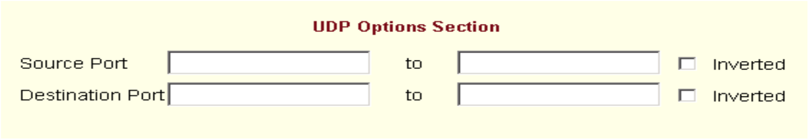


**Figure 8-33:** Firewall Configuration “Add Rule” and “Edit Rule” UDP Protocol Fields

The following table defines the fields in the UDP Options Section.

**Table 8-14:** Expert > UDP Options Fields

| Field | Definition |
|---|---|
| **Source Port**<br>- OR -<br>**Destination Port**<br>-AND-<br>**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 appears in the “ICMP Options Section” at the bottom of the Firewall Configuration form. The following figure shows the options.

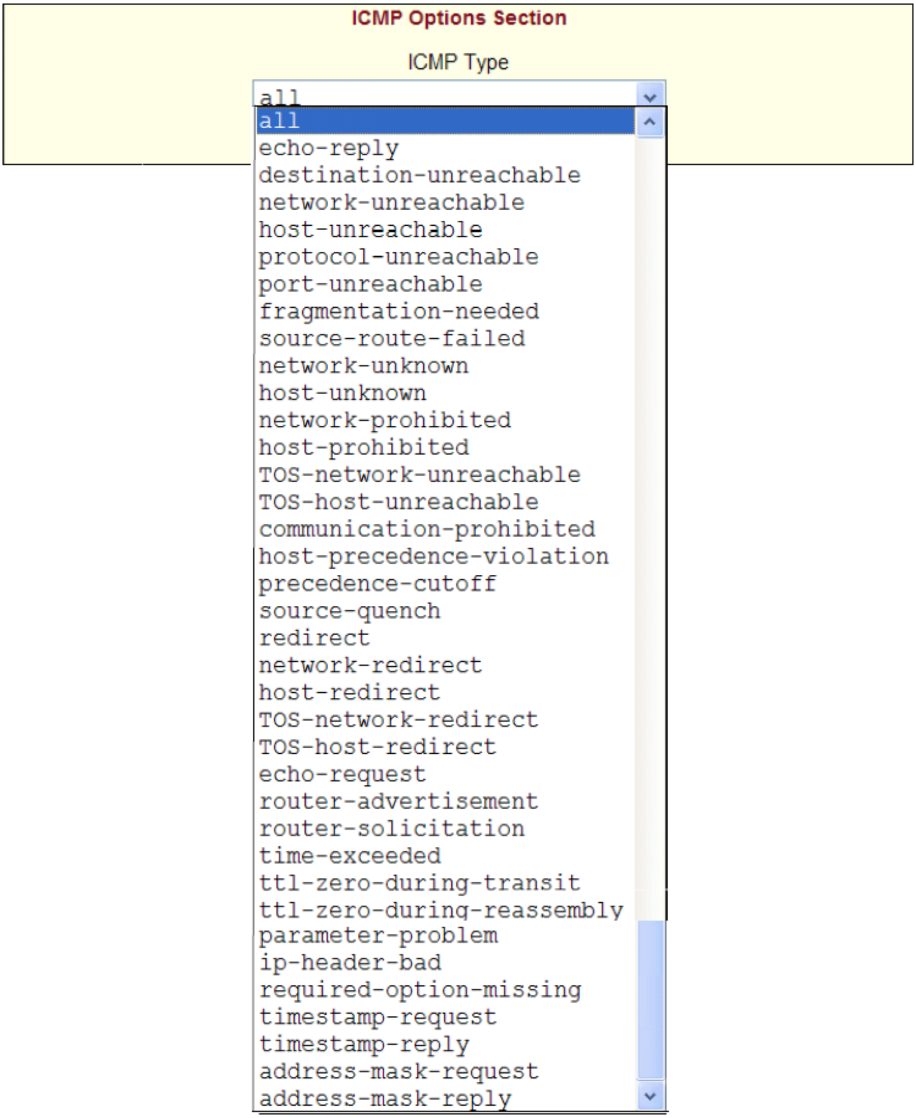


**Figure 8-34:** Firewall Configuration "Add Rule" and "Edit Rule" ICMP Type Menu Options

### *Input Interface, Output Interface, and Fragments*

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

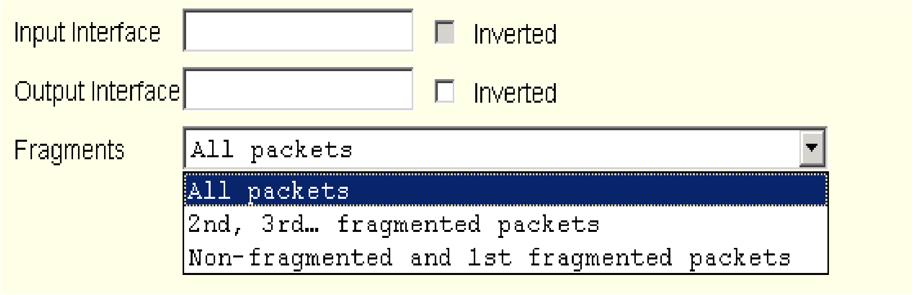


**Figure 8-35:** Firewall Configuration Input and Output Interface Fields and Fragments Menu Options

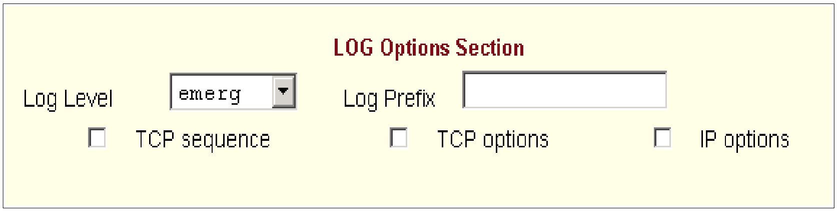
The following table defines the fields in the above figure.

**Table 8-15:** Expert > Firewall Configuration Input and Output Interface, and Fragments Fields Definitions.

| Field | Definition |
|---|---|
| **Input Interface** | The input interface (eth*N*) for the packet |
| **Output Interface** | The output interface (eth*N*) 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:<br>• All packets<br>• 2nd, 3rd... fragmented packets<br>• Non-fragmented and 1st fragmented packets |

### *LOG Target*

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



LOG Options Section

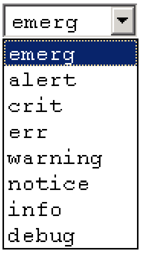
Log Level: emerg    Log Prefix:

□ TCP sequence    □ TCP options    □ IP options

**Figure 8-36:** Firewall Configuration “Add Rule” and “Edit Rule” LOG Target Fields

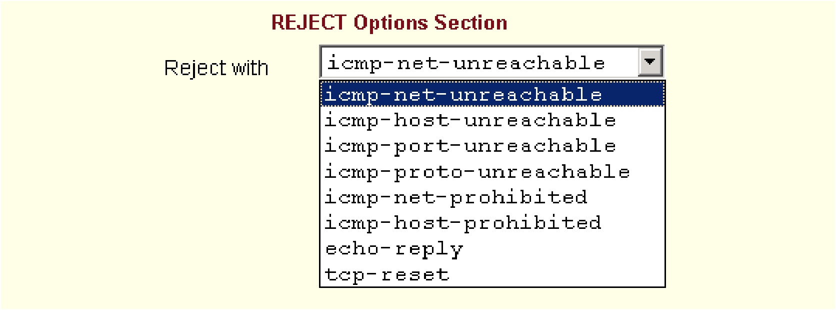
The following table defines the menu options and fields in the “LOG Options Section.”

**Table 8-16:** Expert > Target LOG Options Selection Fields

| Field or Menu Name | Definition |
|---|---|
| **Log Level** | One of the options in the pull-down menu:<br><br> emerg<br>emerg<br>alert<br>crit<br>err<br>warning<br>notice<br>info<br>debug |
| **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



REJECT Options Section

Reject with: icmp-net-unreachable

**Figure 8-37:** Firewall Configuration “Add Rule” and “Edit Rule” REJECT Target Menu Options

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

**Table 8-17:** Expert > Reject Options Sections

| 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. |

**Table 8-17:** Expert > Reject Options Sections

| Field Name | Definition |
|---|---|
| **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 and then click OK.

**Note:** Spaces are not allowed in the chain name.

The name of the new chain appears in the list.

4. Finish defining the chain by adding one or more rules, as described in "To Add a Rule"

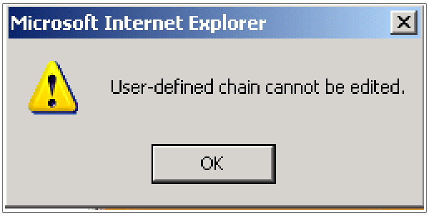
## ▼ *To Edit a Chain*

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

**Note:** User-defined chains cannot be edited. If you want 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.

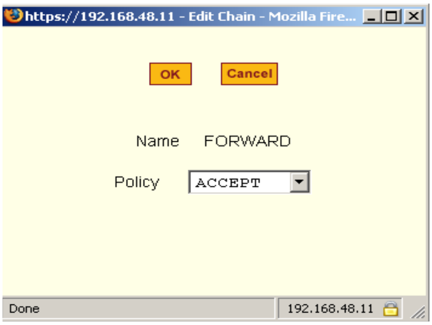
   If you select a user-defined chain, the dialog box shown in the following figure appears.



Microsoft Internet Explorer

User-defined chain cannot be edited.

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



https://192.168.48.11 - Edit Chain - Mozilla Fire...

Name FORWARD

Policy ACCEPT

Done 192.168.48.11

3. Select the desired policy from the Policy pull-down menu, and then click OK.
4. Click “apply changes.”
5. 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 want to add a rule from Chain list, and then click the “Edit Rules” button.
3. Click the “Add Rule” button.

   The “Add Rule” dialog box appears.
4. Configure the rule as desired.

   For definitions of the fields in this form see “Firewall Configuration” on page 186.
5. Click OK.
6. Click “apply changes.”

### ▼ *To Edit a Rule*

1. Go to Network > Firewall Configuration
2. Select the chain that you want to edit from the list and click the “Edit Rules” button.

   The “Edit Rules” form appears.
3. Select the rule to be edited from the Rules list, and then click the “Edit” button.

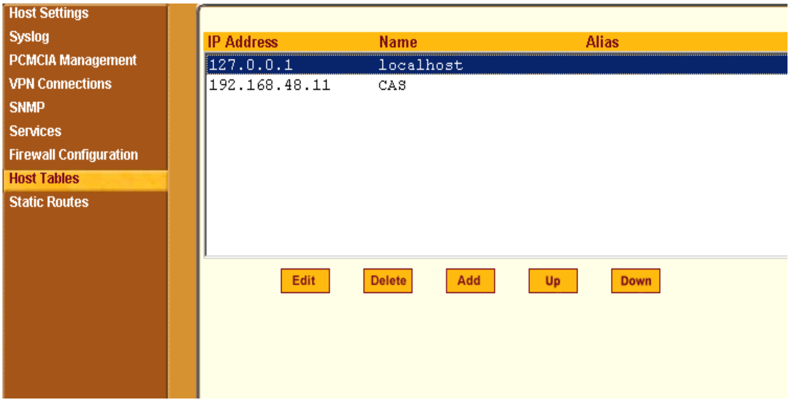
   The “Edit Rule” dialog box appears.
4. Modify the rule as desired.

   For definitions of the fields in this form see “Firewall Configuration” on page 186
5. Click OK.
6. Click “apply changes.”

## Host Table

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

Selecting Network > Host Tables brings up the form shown in the following figure.



| IP Address | Name | Alias |
|---|---|---|
| 127.0.0.1 | localhost | |
| 192.168.48.11 | CAS | |

**Figure 8-38:** Expert > Network > Host Tables

### ▼ *To Define the CS'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. (You can use the "Up" and "Down" buttons to navigate through the list.)

**3.** To add a host, click the "Add" button.

The "host table" dialog box appears.

**4.** Enter the new or modified host address in the "IP Address field," and the host name in the "Name" field, and then click "OK."

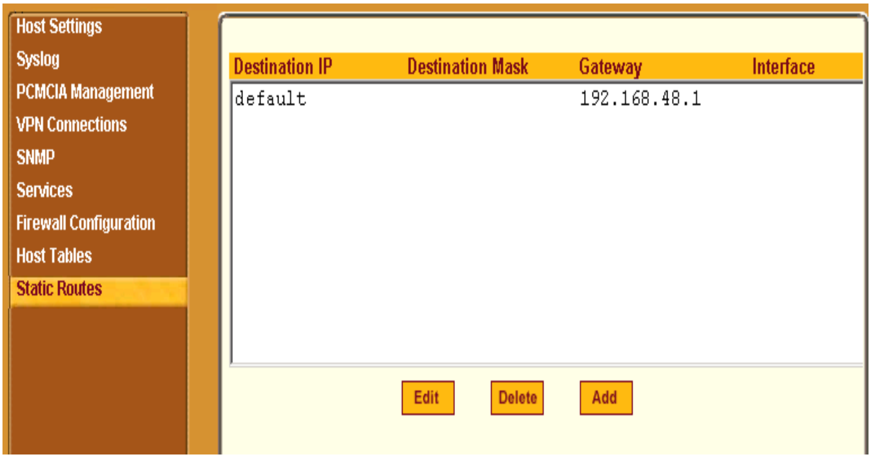
**5.** To delete a host, select the host you wish to delete and click "Delete."

**6.** Click "apply changes."

## *Static Routes*

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

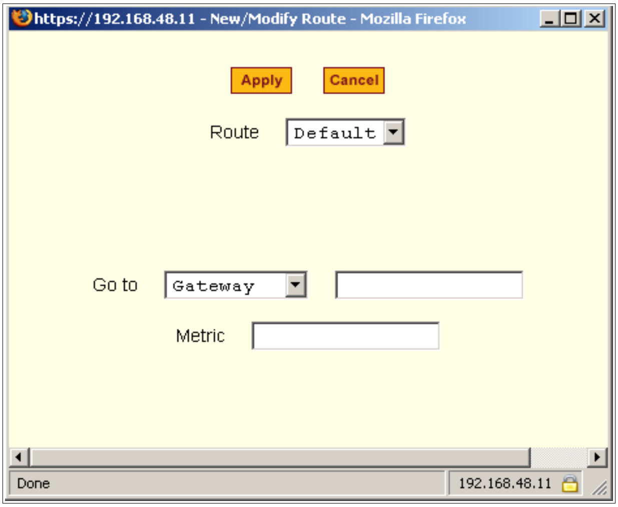
Selecting Network > Static Routes brings up the form shown in the following figure.



| Destination IP | Destination Mask | Gateway | Interface |
|---|---|---|---|
| default | | 192.168.48.1 | |

**Figure 8-39:** Expert > Network > Static Routes

Clicking the “Edit” or “Add” buttons brings up a form shown in the following figure.



Route: Default

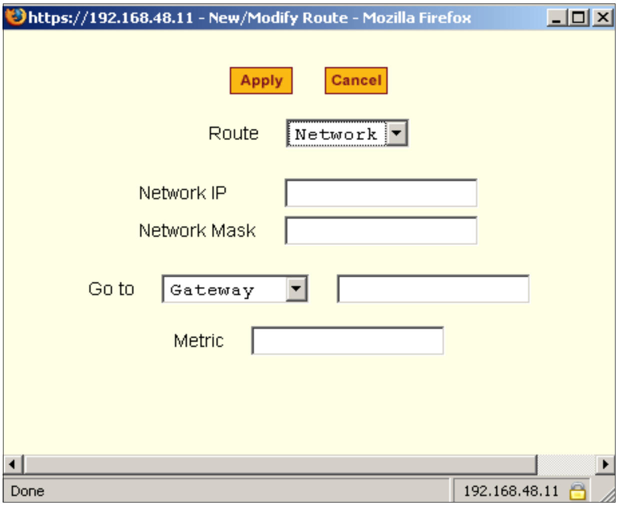
Go to: Gateway

Metric:

**Figure 8-40:** Expert > Static Routes “Add” and “Edit” Dialog Boxes - Default Route

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

The following figure shows the fields and menus that appear when the "Network" route type is selected from the "Route" pull-down menu.

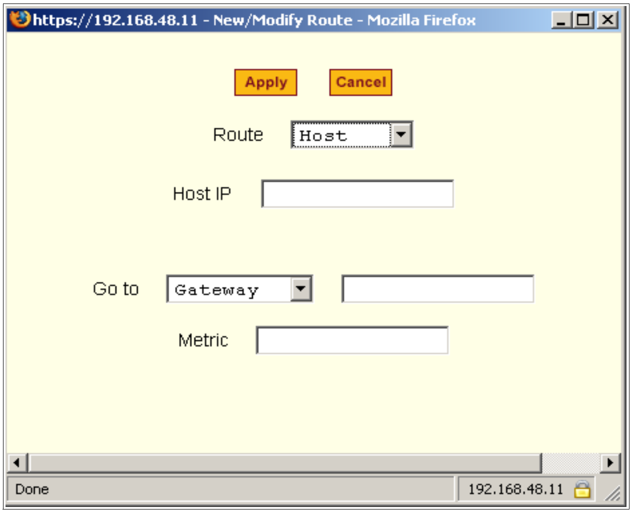


Route Network

Go to Gateway

**Figure 8-41:** Expert > Static Routes "Add" and "Edit" Dialog Boxes - Network Route

The following figure shows the fields and menus that appear when the "Host" route type is selected from the "Route" pull-down menu.



Route Host

Go to Gateway

**Figure 8-42:** Expert > Static Routes "Add" and "Edit" Dialog Boxes - Host Route

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

**Table 8-18:** Expert > Fields and Menus for Configuring Static Routes

| 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. |
| **Network Mask** | Appears only when "Network" route is selected. Type the netmask of the destination network. |
| **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]*

See Table 8-17 on page 198 for the field descriptions.

1. Go to Network > Static Routes

   The Static Routes form appears.

   - To edit a static route, select a route from the "Static Routes" list, and then select the "Edit" button.
   - To add a static route, select the "Add" button from the form.

   The system invokes the "New/Modify Route" dialog box.

2. Choose "Default", "Network", or "Host" from the "Route" pull-down menu.

3. If you selected “Network, do 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 9
# Security Menu & Forms

This Chapter describes the “Security” menu and the related forms. The following table provides a description of the left menu panel and links to the detailed information and procedures.

**Table 9-1:** Expert > Security Menu

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Users and Groups** | Create or edit users and groups, establish or change their passwords, and access rights and privileges. | Page 208 |
| **Active Port Sessions** | Show the active sessions, as well as their identifications, features and usage statistics. | Page 212 |
| **Authentication** | Enter the authentication method used to access CS. | Page 214 |
| **Security Profiles** | Select a pre-defined Security Profile, or choose Custom Profile to configure individual settings. | Page 226 |

## Users and Groups

Users and Groups form allows you to do the following tasks:

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

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

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

**Caution:** There is only one “root” user for the initial setup of the CS by the administrator. The username is “root”, and the default password is “bb”. For security purposes make sure you change this default password as soon as possible!

Selecting Security > Users & Groups in Expert mode brings up the form shown in the following figure.

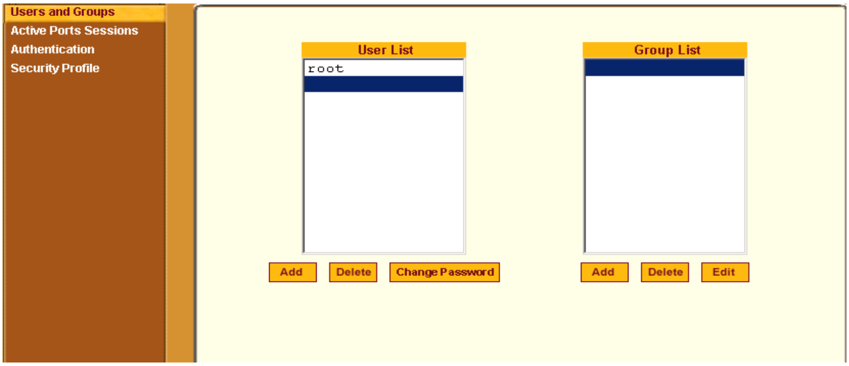


**Figure 9-1:** Expert > Security > Users and Groups Form

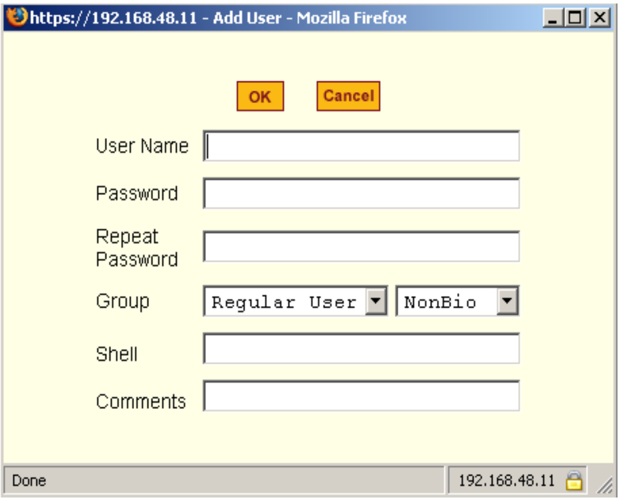
You can use the Users and Groups form to do the following:

- Add or delete users
- Assign or change user passwords
- Add or delete groups

- Add users to a group
- Delete users from a group

## Adding a User

If you click the “Add” button on the Security > Users and Groups form under the “Users List”, the following dialog box appears.



https://192.168.48.11 - Add User - Mozilla Firefox

User Name
Password
Repeat Password
Group Regular User NonBio
Shell
Comments

Done
192.168.48.11

**Figure 9-2:** Expert > Security > Users and Groups > “Add User” Dialog Box

The following table describes the fields in the “Add User” dialog box.

**Table 9-2:** 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 user name. |
| 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. |

**Table 9-2:** Expert > Add User Dialog Field Names and Definitions

| Field Name | Definition |
|---|---|
| Shell | Optional. The default shell is /bin/sh when the user makes an 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 following dialog box appears.

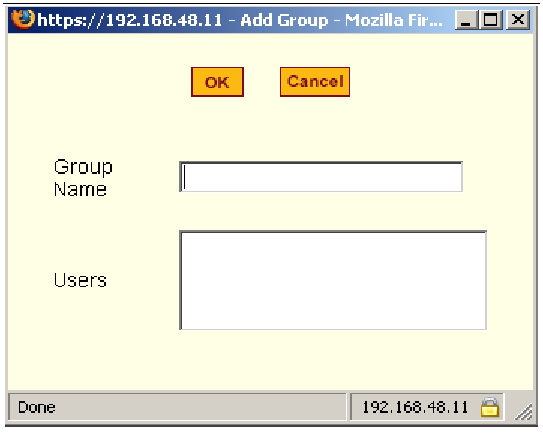


**Figure 9-3:** Expert > Security > Users and Groups > "Add Group" Dialog Box

You can add a new group by entering a group name and a comma-separated list of users.

### ▼ *To Add a User*

1. Go to Security > Users and Groups

   The Users and Groups form displays.

2. Click "Add."

   The "Add User" dialog box displays.

3. Enter the name 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 & 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 want 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 & Groups form displays.

2. Under the list of groups, click “Add.”

   The “Add Group” dialog box displays.

3. Enter the name for the new group in the “Group Name” field.

4. Enter one user name or multiple comma-separated user names in the “Users” field.

5. Click OK.

6. Click “apply changes.”

### ▼ *To Modify a Group*

1. Go to Security > Users and Groups

   The Users and Groups form displays.

2. Select the name of a group to modify.

3. Click “Edit.”

   The “Edit Group” form displays.

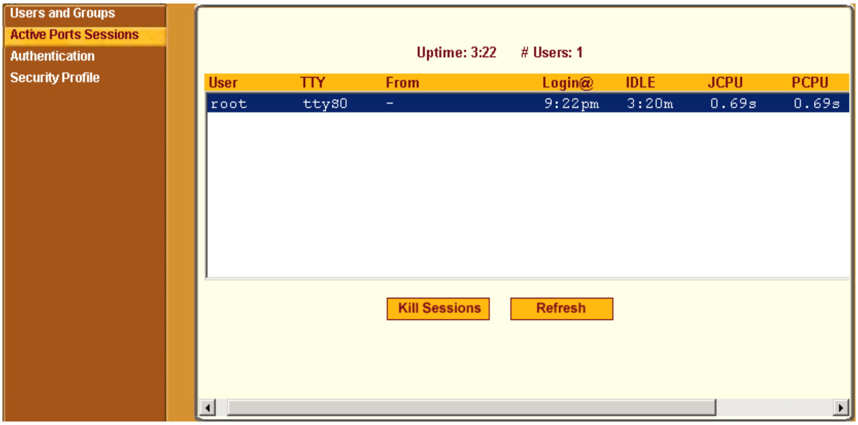
4. Add or delete users from the group as desired.

5. Click OK.

6. Click “apply changes.”

## *Active Ports Sessions*

Selecting Security > Active Ports Sessions brings up the form shown in the following figure.



Uptime: 3:22 # Users: 1

| User | TTY | From | Login@ | IDLE | JCPU | PCPU |
|---|---|---|---|---|---|---|
| root | ttyS0 | - | 9:22pm | 3:20m | 0.69s | 0.69s |

**Figure 9-4:** Expert > Security > Active Ports Sessions

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

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

The following table defines the active ports sessions form fields.

**Table 9-3:** 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. |

| Field Name | Definition |
|---|---|
| **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 in Expert mode.

   The Active Ports Sessions form appears.

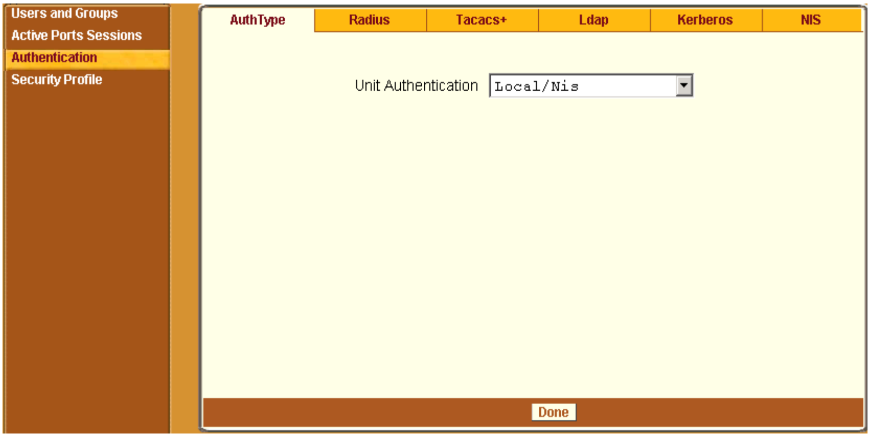
2. To refresh the display, click the “Refresh” button.

   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 brings up the form shown in the following figure, which is comprised of six tabs.



Unit Authentication: Local/Nis

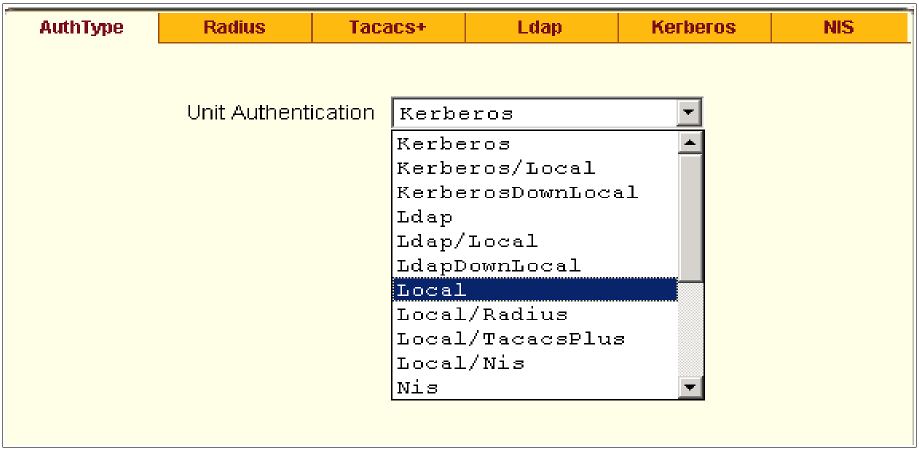
**Figure 9-5:** Expert > Security > Authentication

You can use the Authentication forms to:

- Select a method for authenticating logins to CS.
- Identify authentication servers that are configured for logins to CS or to the serial ports.

## Configuring Authentication for CS Logins

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



Unit Authentication: Kerberos

**Figure 9-6:** Expert > Security > Authentication > AuthType Form

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

### ▼ *To Configure the CS Login Authentication Method*

1. Go to Security > Authentication.

   The "AuthType" form displays, as shown in the figure 9-6.

2. To specify an authentication method for login to CS, select a method from the "Unit Authentication" pull-down menu.

3. Click "apply changes."

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

## Configuring Authentication Servers for Logins to CS 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.

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

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

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

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

**Table 9-4:** Tasks for Setting up Authentication Servers.

| Method | Variations | Procedures |
|---|---|---|
| RADIUS | RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal | See “To Configure a RADIUS Authentication Server” on page 218 |
| TACACS+ | TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal | See “To Configure a TACACS+ Authentication Server” on page 219 |
| LDAP | LDAP, LDAP/Local, or LDAPDownLocal | See “To Configure an LDAP Authentication Server” on page 221 |
| Kerberos | Kerberos, Kerberos/Local, or KerberosDownLocal | See “To Configure a Kerberos Authentication Server” on page 223 |

**Table 9-4:** Tasks for Setting up Authentication Servers.

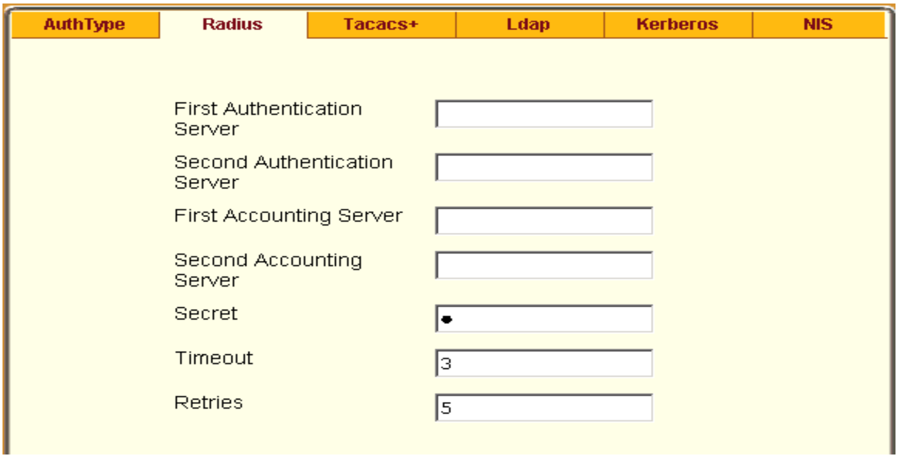
| Method | Variations | Procedures |
|---|---|---|
| NIS | NIS, Local/NIS, NIS/Local, or NISDownLocal | See "To Configure a NIS Authentication Server" on page 225 |

### ▼ *To Configure a RADIUS Authentication Server*

Perform the following procedure to configure a RADIUS authentication server when CS 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.

The RADIUS form displays as shown in the following figure.



| | |
|---|---|
| First Authentication Server | |
| Second Authentication Server | |
| First Accounting Server | |
| Second Accounting Server | |
| Secret | • |
| Timeout | 3 |
| Retries | 5 |

**Figure 9-7:** Expert > Security > Authentication > Radius

**2.** Fill in the form according to your local RADIUS server configuration.

**3.** Click "apply changes."

The changes are stored in `/etc/raddb/server` on CS.

### Group Authorization on RADIUS

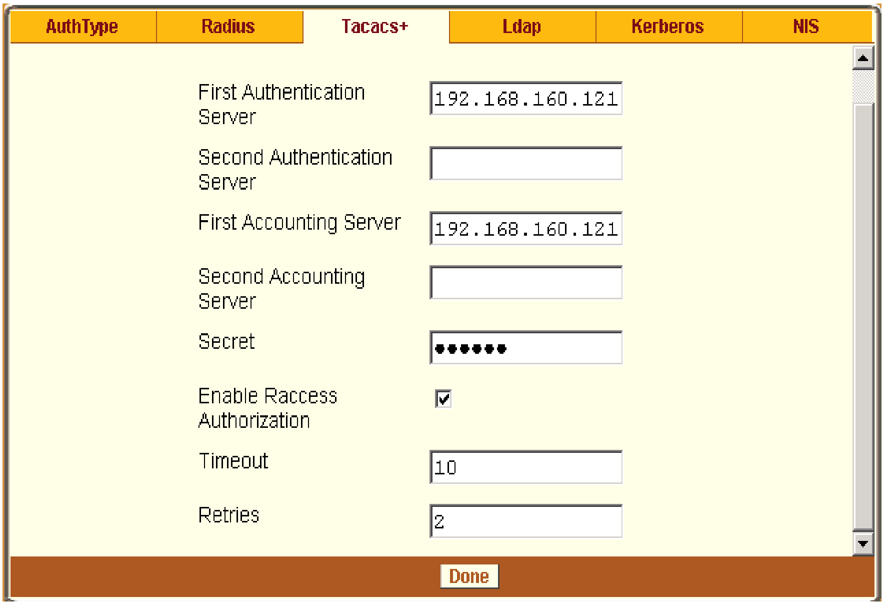
Group information retrieval from a RADIUS authentication server adds another layer of security by adding a network-based authorization. It retrieves the “group” information from the authentication server and performs an authorization through CS. To see the configuration procedures for a RADIUS authentication server refer to the *CS Command Reference Guide, Chapter 3, Section 3.4 “Group Authorization”*.

### ▼ *To Configure a TACACS+ Authentication Server*

Perform the following procedure to configure a TACACS+ authentication server when CS 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 appears as shown in the following figure.



First Authentication Server: 192.168.160.121

Second Authentication Server:

First Accounting Server: 192.168.160.121

Second Accounting Server:

Secret: ●●●●●●

Enable Raccess Authorization: ☑

Timeout: 10

Retries: 2

**Figure 9-8:** Expert > Security > Authentication > TACACS+

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” check box.

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 CS or its ports using TACACS+ authentication is checked. Users with administrator privileges have administrative access, and users with regular user privileges have regular user access.

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

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

5 To specify a number of times the user can request authentication verification from the server before sending an authentication failure message to the user, enter a number in the “Retries” field.

6 Click “apply changes.”

The changes are stored in `/etc/tacplus.conf` on the CS.

## 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 brings up 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” check box, an additional level of security checking is implemented. After each user is successfully authenticated through the standard login procedure, the CS uses TACACS+ to authorize whether or not each user is allowed 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 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 *CS Command Reference Guide, Chapter 3, Section 3.4 “Group Authorization”.*

### ▼ *To Configure an LDAP Authentication Server*

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

Before starting this procedure, find out 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 following fields, but an entry is not required:

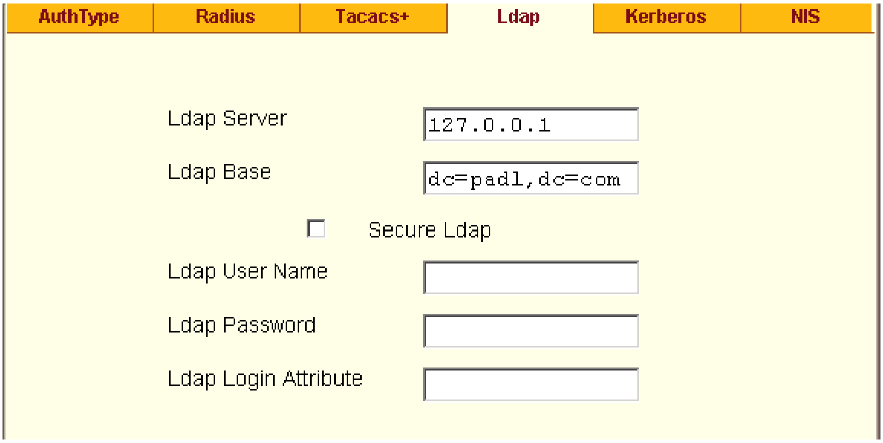
- LDAP User Name
- LDAP Password
- LDAP Login Attribute

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 CS and the connected devices know the passwords assigned to the accounts:

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

**1.** Go to Security > Authentication > LDAP in Expert mode.

The “LDAP” form displays with “LDAP Server” and “LDAP Base” fields filled in from with the current values in the `/etc/ldap.conf` file.



Ldap Server 127.0.0.1

Ldap Base dc=padl,dc=com

□ Secure Ldap

Ldap User Name

Ldap Password

Ldap Login Attribute

**Figure 9-9:** Expert > Security > Authentication > LDAP

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

   The default distinguished name is “dc,” as in dc=*value*,dc=*value*. If the distinguished name on the LDAP server is “o,” then replace dc in the base field with o, as in o=*value*,o=*value*.
4. Replace the default base name with the name of your LDAP domain.

   For example, for the LDAP domain name blackbox.com, the correct entry is: dc=blackbox,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 CS.

## 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 CS. To see the configuration procedures for an LDAP authentication server refer to the *CS Command Reference Guide, Chapter 3, Section 3.4 “Group Authorization”.*

### ▼ *To Configure a Kerberos Authentication Server*

Perform the following procedure to configure a Kerberos authentication server when CS 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’s 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 CS and connected devices know the passwords assigned to the accounts:

- An account for “admin”
- If Kerberos authentication is specified for CS, accounts for all users who need to log into the CS to administer connected devices.
- If Kerberos authentication is specified for the serial ports, accounts for users who need administrative access to connected devices

**1.** Make sure an entry for the CS and the Kerberos server exist in the CS’s `/etc/hosts` file.

  **a.** Go to Network > Host Table in Expert mode.

  The “Host Table” form appears.

  **b.** Add an entry for CS if none exists and an entry for the Kerberos server.

    **i.** Click “Add.”

    The “New/Modify Host” dialog appears.

    ii. Enter the address in the “IP Address” field.

    iii. Enter the name in the “Name” field.

iv. Enter an optional alias in the “Alias” field.

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

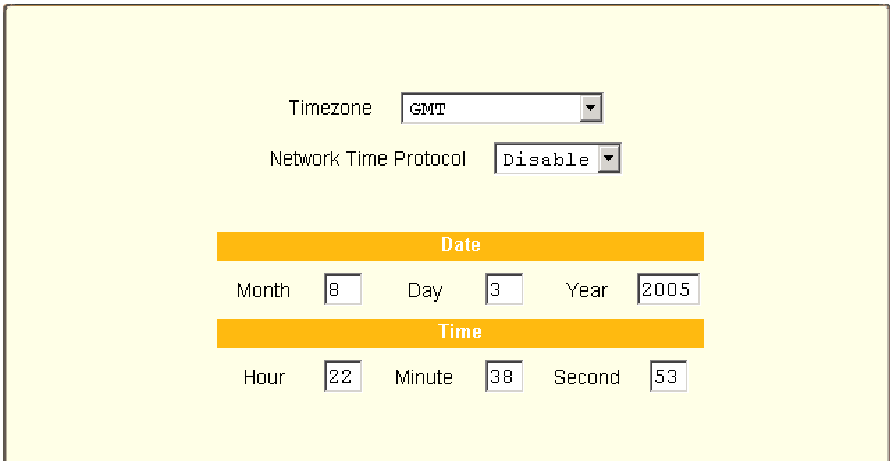
**Note:** Kerberos authentication depends on time synchronization. Time and date synchronization can be achieved by setting both CS and the Kerberos server to use the same NTP server.

a. To specify an NTP server, see “To Configure Time and Date Using an NTP Server” on page 306.

b. To manually set the time and date on the CS, see “To Manually Set the Time and Date” on page 306.

c. Work with the Kerberos authentication server administrator to synchronize the time and date between CS and the Kerberos server.

3. Set the timezone on CS by going to Administration > Time/Date in Expert mode as per the following figure. The default is GMT.



Timezone GMT

Network Time Protocol Disable

Date

Month 8 Day 3 Year 2005

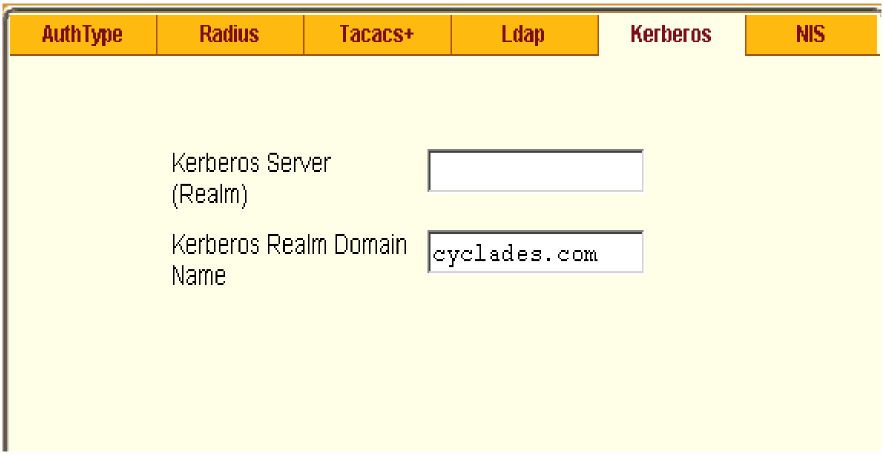
Time

Hour 22 Minute 38 Second 53

**Figure 9-10:** Expert > Administration > Time/Date

4. Go to Security > Authentication> Kerberos in Expert mode.

The Kerberos form displays as shown in the following figure.



Kerberos Server (Realm)

Kerberos Realm Domain Name: cyclades.com

**Figure 9-11:** Expert > Security > Authentication > Kerberos

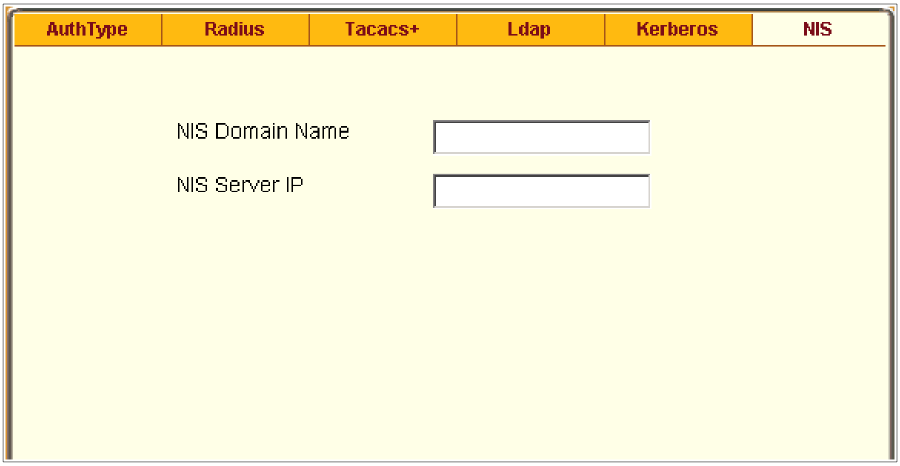
5. Fill in the form according to your local setup of the Kerberos server.
6. Click "apply changes."

## ▼ *To Configure a NIS Authentication Server*

Perform the following procedure to configure a NIS authentication server when CS or any of its ports is 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.

   The NIS form displays as shown in the following figure.



NIS Domain Name

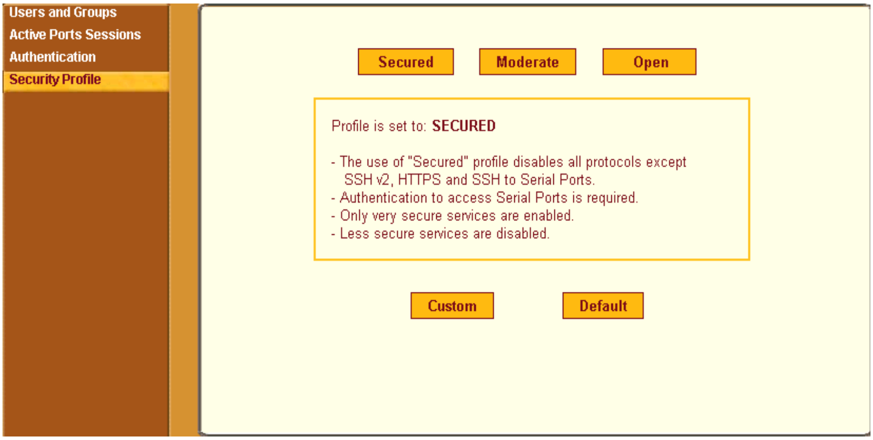
NIS Server IP

**Figure 9-12:** Expert > Security > Authentication > NIS

2. Fill in the form according to your configuration of the NIS server.
3. Click “apply changes.”

## *Security Profiles*

Selecting Security > Security Profile brings up the form shown in the following figure.



Profile is set to: SECURED

- The use of "Secured" profile disables all protocols except SSH v2, HTTPS and SSH to Serial Ports.
- Authentication to access Serial Ports is required.
- Only very secure services are enabled.
- Less secure services are disabled.

**Figure 9-13:** Expert > Security > Security Profile

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:

1. 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 “Secure” security profile is selected, you need to switch to a “Custom” security profile, and enable “allow root access” option.

2. 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.
3. 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 sets the parameters to same as *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 user’s custom requirements.

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

**Table 9-5:** Expert > Enabled services to access the CS under each security profile.

| Access to CS | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| Telnet | | | ✓ | | User Configurable |
| SSHv1 | | ✓ | ✓ | ✓ | |
| SSHv2 | ✓ | ✓ | ✓ | ✓ | |
| Allow SSH root access | | ✓ | ✓ | ✓ | |
| HTTP | | ✓ | ✓ | ✓ | |
| HTTPS | ✓ | ✓ | ✓ | ✓ | |
| HTTP redirection to HTTPS | | ✓ | | ✓ | |

1-The *Default* security profile parameters is the same as Moderate profile.

**Table 9-6:** Expert > Enabled services to access the serial ports under each security profile.

| Access to Serial Ports | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| Console (Telnet) | | ✓ | ✓ | ✓ | User Configurable |
| Console (SSH) | ✓ | ✓ | ✓ | ✓ | |
| Console (Raw) | | ✓ | ✓ | ✓ | |
| Serial Port Authentication | ✓ | | | | |
| Bidirect (Dynamic Mode Support) | | ✓ | ✓ | ✓ | |

1-The *Default* security profile parameters is the same as Moderate profile.

**Table 9-7:** Expert > Enabled protocols for each security profile shown with a check mark.

| Other Services | Secure | Moderate | Open | Default[1] | Custom |
|---|---|---|---|---|---|
| SNMP | | | ✓ | | **User Configurable** |
| RPC | | | ✓ | | |
| ICMP | | ✓ | ✓ | ✓ | |
| FTP | | | | | |
| IPSec | | | | | |

1-The *Default* security profile parameters is the same as Moderate profile.

The first step in configuring your Advanced Console Server is to define a Security Profile. One of the following situations is applicable when you boot up the CS unit.

1. CS is starting for the first time, or after a reset to factory default parameters.

   In this situation when you boot CS up and login 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 CS restarts.

2. CS firmware is upgraded and the system is restarting with the new firmware.

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

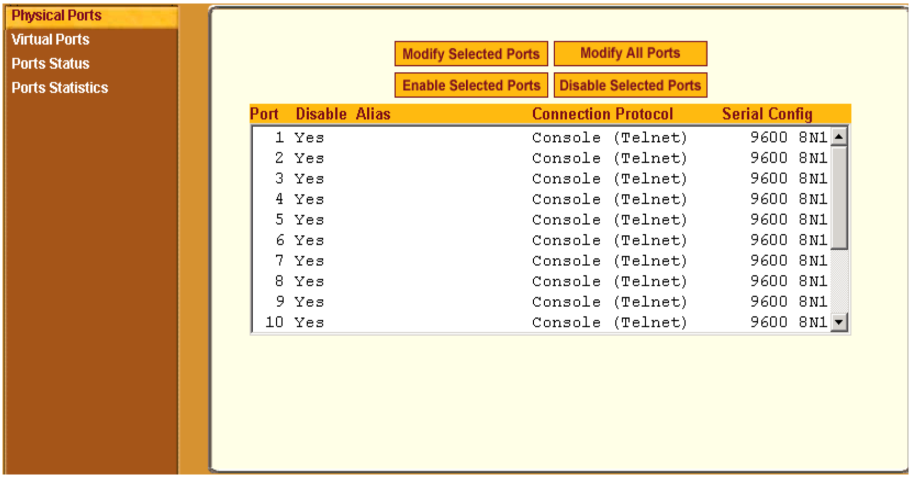
3. CS is restarting normally.

   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 CS units 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 figure shows the default factory settings of serial ports.



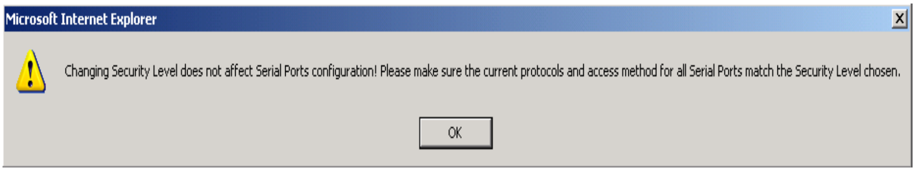
```
Port  Disable  Alias                Connection Protocol     Serial Config
  1  Yes                           Console (Telnet)         9600 8N1
  2  Yes                           Console (Telnet)         9600 8N1
  3  Yes                           Console (Telnet)         9600 8N1
  4  Yes       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

**Figure 9-14:** Expert > Physical Ports Default Factory Settings

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.

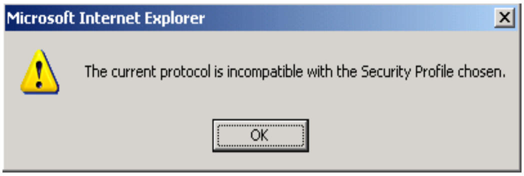
  The following reminder dialog box appears when you access Ports in Expert mode.



Changing Security Level does not affect Serial Ports configuration! Please make sure the current protocols and access method for all Serial Ports match the Security Level chosen.

**Figure 9-15:** Security Profile and Serial Ports Configuration Alert

- If the serial port connection protocol is incompatible with the selected security profile the following dialog box appears when you try to access Expert > Ports > Physical Ports



The current protocol is incompatible with the Security Profile chosen.

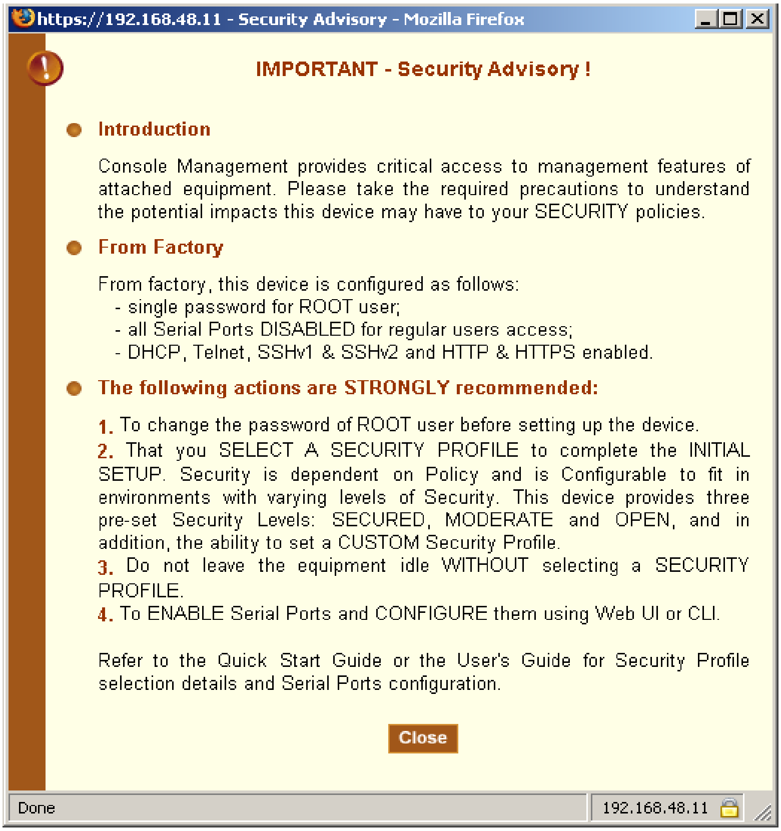
**Figure 9-16:** Serial Ports Protocol Incompatibility Dialog Box

## ▼ *To Select or Configure a Security Profile*

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

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

   The following security warning dialog box appears.



IMPORTANT - Security Advisory !

● Introduction

Console Management provides critical access to management features of attached equipment. Please take the required precautions to understand the potential impacts this device may have to your SECURITY policies.

● From Factory

From factory, this device is configured as follows:
- single password for ROOT user;
- all Serial Ports DISABLED for regular users access;
- DHCP, Telnet, SSHv1 & SSHv2 and HTTP & HTTPS enabled.

● The following actions are STRONGLY recommended:

1. To change the password of ROOT user before setting up the device.
2. That you SELECT A SECURITY PROFILE to complete the INITIAL SETUP. Security is dependent on Policy and is Configurable to fit in environments with varying levels of Security. This device provides three pre-set Security Levels: SECURED, MODERATE and OPEN, and in addition, the ability to set a CUSTOM Security Profile.
3. Do not leave the equipment idle WITHOUT selecting a SECURITY PROFILE.
4. To ENABLE Serial Ports and CONFIGURE them using Web UI or CLI.

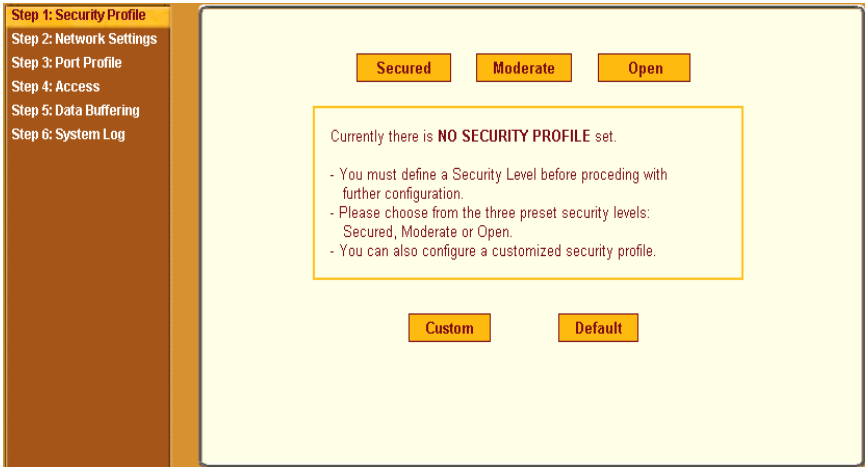
Refer to the Quick Start Guide or the User's Guide for Security Profile selection details and Serial Ports configuration.

**Figure 9-17:** Security Advisory Dialog Box

**Note:** Your browser’s pop-up blocker should be disabled for this dialog box to appear.

2. Review the Security Advisory and click the “Close” button.
3. The Web Manager is redirected to Wizard > Step 1: Security Profile

The following form is displayed.



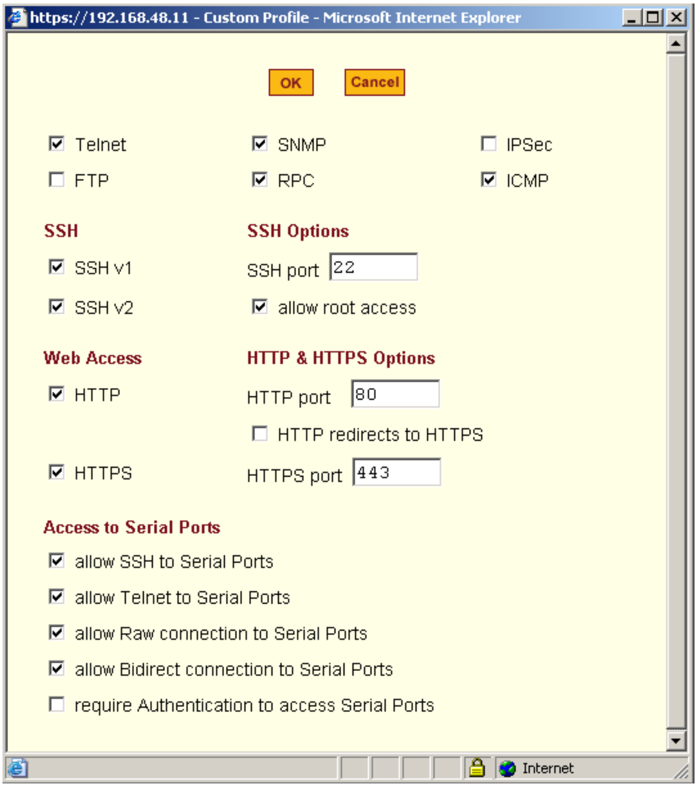
Currently there is **NO SECURITY PROFILE** set.

- You must define a Security Level before proceding with further configuration.
- Please choose from the three preset security levels: Secured, Moderate or Open.
- You can also configure a customized security profile.

**Figure 9-18:** Wizard > Step 1: Security Profile Form

**4.** Select a pre-defined Security Profile by pressing one of the “Secured”, “Moderate”, “Open”, or “Default” profiles, or create a “Custom” profile.

The following dialog box appears when you select the “Custom” profile.


https://192.168.48.11 - Custom Profile - Microsoft Internet Explorer
OK
Cancel
Internet

☑ Telnet
☐ FTP
☑ SNMP
☑ RPC
☐ IPSec
☑ ICMP

SSH

☑ SSH v1
☑ SSH v2

SSH Options

SSH port 22
☑ allow root access

Web Access

☑ HTTP
☑ HTTPS

HTTP & HTTPS Options

HTTP port 80
☐ HTTP redirects to HTTPS
HTTPS port 443

Access to Serial Ports

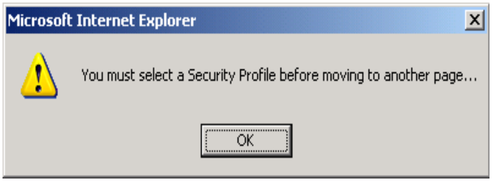
☑ allow SSH to Serial Ports
☑ allow Telnet to Serial Ports
☑ allow Raw connection to Serial Ports
☑ allow Bidirect connection to Serial Ports
☐ require Authentication to access Serial Ports

**Figure 9-19:** Custom Security Profile Dialog Box

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

Refer to Table 9-5 on page 228, and the subsequent tables for a comparison of the available services in each security profile. Refer to the Glossary for a definition on some of the available services.

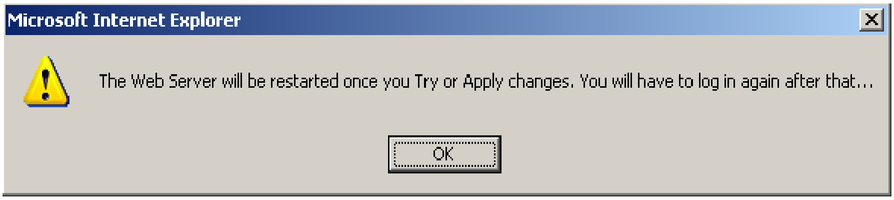
**Note:** It is not possible to continue working in the Web Manager without selecting a Security Profile. The following dialog box appears if you try to navigate to other sections of the Web Manager.


Microsoft Internet Explorer

You must select a Security Profile before moving to another page...

5. Once you select a security profile or configure a custom profile and apply the changes, the CS Web Manager restarts in order for the changes to take effect.

   The following dialog box appears.


Microsoft Internet Explorer

The Web Server will be restarted once you Try or Apply changes. You will have to log in again after that...

6. Select “apply changes” to save the configuration to Flash.

   CS Web Manager restarts.

7. Login after Web Manager restarts.
8. The Web Manager defaults to Ports > Ports Status page.

Proceed to the desired forms and the related tasks outlined in the table below.

**Table 9-8:** Configuring CS in Expert Mode

| | |
|---|---|
| Configure Users and Groups | “Users and Groups” on page 208 |
| Configure Serial Ports | “Physical Ports” on page 239 |
| Configure Network Settings | “Host Settings” on page 152 |
| Configure IPDU Power Management | “IPDU Power Mgmt.” on page 120 |

# *Security Certificates*

CS 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 CS generated certificate.

## Certificate for HTTP Security

A certificate for HTTP security is created by a CA (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 *CS Command Reference Guide, Chapter 3 “Authentication”, Section 3.7 “Certificate for HTTP Security”*.

## User Configured Digital Certificate

You can generate a self-signed digital certificate. It is highly recommended that you use the “openssl” tool to generate a self-signed certificate and replace the CS generated certificate.The procedures to configure a self-signed digital certificate is documented in the *CS Command Reference Guide, Chapter 3 “Authentication”, Section 3.8 “User Configured Digital Certificate”*

## X.509 Certificate on SSH

The OpenSSH software included with CS 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 *CS Command Reference Guide, Chapter 3 “Authentication”, Section 3.8 “X.509 Certificate on SSH”*.

# Chapter 10
# Ports Menu & Forms

This Chapter describes the “Ports” menu and the related forms. The following table provides a description of the left menu panel in the Web Manager and links to the detailed information and procedures.

**Table 10-1:** Expert > Ports Menu

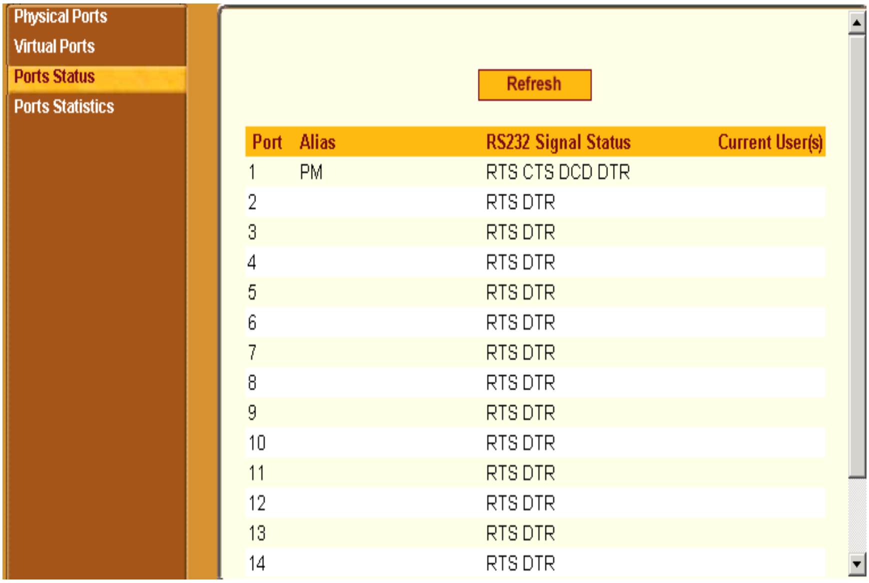
| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Physical Ports** | Activate or deactivate the serial ports. Set the parameters for each or all ports. Configure specific parameters for the serial ports where IPDU devices are connected. | Page 239 |
| **Virtual Ports** | Perform Clustering. This section shows how to define and configure slaves. One CS can be used as a Master to control other CS (slaves) units. All ports of the slave unit appear as if they are part of the master unit. | Page 281 |
| **Port Status** | View the current status of each port. The information provided here are RS232 Signal Status and user connected to each port. | Page 287 |

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Ports Statistics** | View information on the data reception (Rx bytes) and transmission (Tx bytes) on each physical port. View current CAS user(s), Baud rate, frame, parity, break, and overruns. | Page 288 |

The Ports section of CS configuration in Expert Mode provides the following menu choices:

- Physical Ports – Allows you to view and modify the physical port settings.
- Virtual Ports – Allows you to view and modify the slave port settings.
- Ports Status – Allows you to view ports connection status.
- Ports Statistics – Allows you to view serial ports connection statistics.

Selecting Ports in Expert mode brings up the form shown in the following figure.



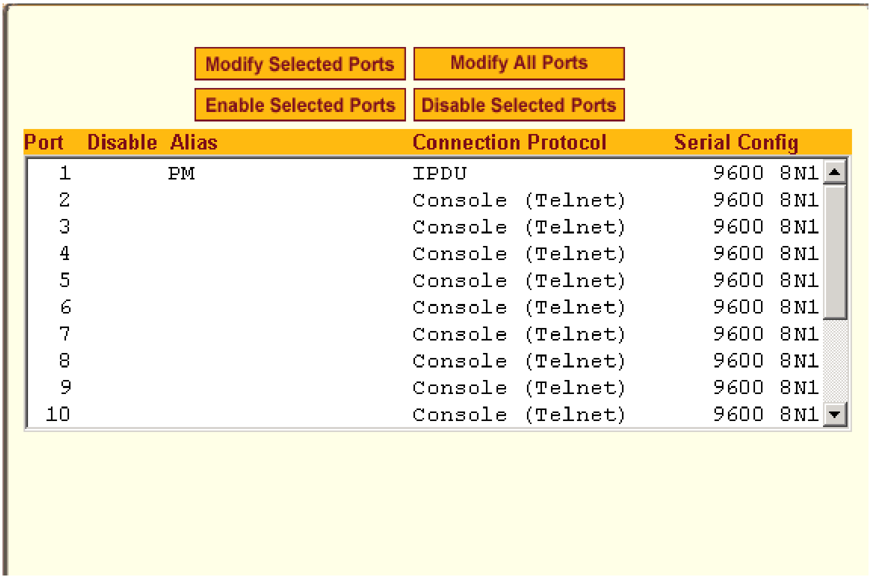
| Port | Alias | RS232 Signal Status | Current User(s) |
|---|---|---|---|
| 1 | PM | RTS CTS DCD DTR | |
| 2 | | RTS DTR | |
| 3 | | RTS DTR | |
| 4 | | RTS DTR | |
| 5 | | RTS DTR | |
| 6 | | RTS DTR | |
| 7 | | RTS DTR | |
| 8 | | RTS DTR | |
| 9 | | RTS DTR | |
| 10 | | RTS DTR | |
| 11 | | RTS DTR | |
| 12 | | RTS DTR | |
| 13 | | RTS DTR | |
| 14 | | RTS DTR | |

**Figure 10-1:** Expert > Ports

Using the forms described in the following sections, you can perform custom configuration of serial ports.

## Physical Ports

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



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

**Figure 10-2:** Expert > Ports > Physical Ports

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

You can select contiguous serial ports on the form by using the [Shift] key, or non-contiguous ports by using the [Ctrl] key on your keyboard. You can “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 “Modify Selected Ports” button, and set values for an individual or a group of ports.

Selecting “Modify Selected Ports” or “Modify All Ports” option brings up a form with the following six tabs

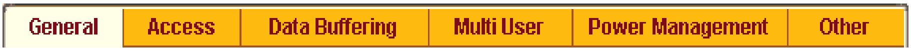


**Figure 10-3:** Expert > Ports > Physical Ports > “Modify .... Ports ” Tab Options

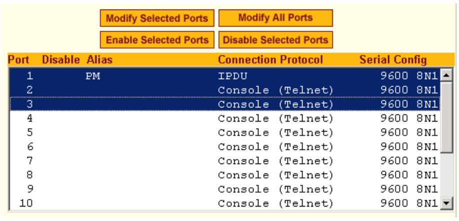
### ▼ *To Select One or More Serial Ports*

**1** Go to Ports > Physical Ports in Expert mode

The Physical Ports form appears.

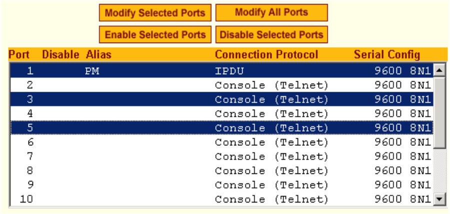
**2** To select a port or ports, do one of the following steps.

- To select a single port, click the port.
- 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.



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

- 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.



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

**3** Go to the desired procedure from the following list.

| | |
|---|---|
| To Configure a Serial Port Connection Protocol for a Console Connection | Page 246 |
| To Configure User Access to Serial Ports | Page 261 |
| To Configure Data Buffering for Serial Ports | Page 267 |

| | |
|---|---|
| To Configure Multiple Sessions and Port Sniffing for One or More Serial Ports | Page 270 |
| To Configure a Serial Port for IPDU or IPMI Power Management | Page 274 |
| To Configure a User for IPDU Power Management While Connected To a Serial Port | Page 276 |
| To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console | Page 279 |

### ▼ *To Enable or Disable Serial Ports*

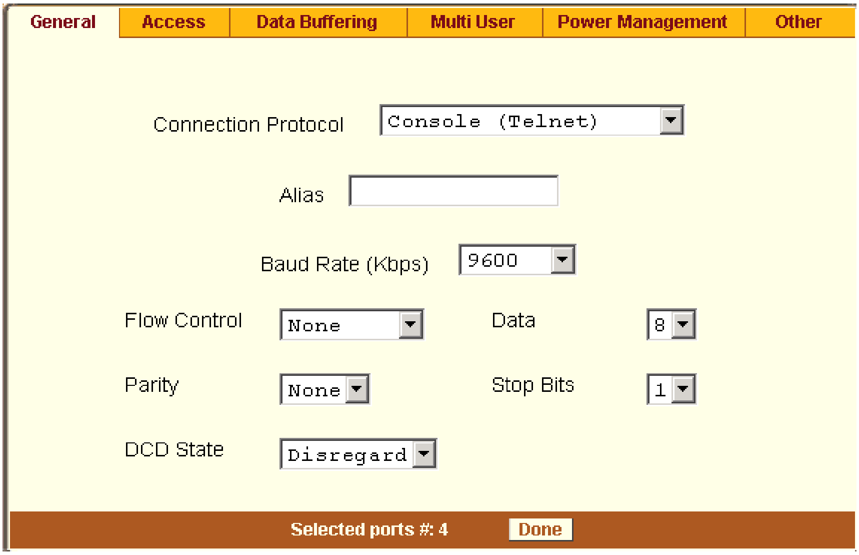
1. Go to Ports > Physical Ports, and select a port or ports to modify.
2. To enable selected ports, click the “Enable Selected Ports” button.
3. To disable selected ports, click the “Disable Selected Ports” button.

**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

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 as shown in the following form.



Connection Protocol: Console (Telnet)

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

Stop Bits: 1

DCD State: Disregard

Selected ports #: 4

**Figure 10-4:** Expert > Ports > Physical Ports > General Form

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(s) of the selected port(s) 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 profile to the serial ports.

| | |
|---|---|
| Console Access Server (CAS) | Page 243 |
| Terminal Server (TS) | Page 243 |
| Bidirectional Telnet | Page 245 |
| Modem (RAS) | Page 246 |
| Power Management | Page 246 |

## Console Access Server (CAS) Profile Connection Protocols

When a serial port is connected to the console port on a device, a Console Access Server (CAS) profile must be defined for the serial port.

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

The CAS connection protocols apply in the following cases:

- When a user access 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 CS serial port is connected to the console port of a server or a device.

**Table 10-2:** Expert > Console Connection Protocols

| Protocol Name | Result |
|---|---|
| Console (Telnet) | Authorized users can use Telnet to connect to the console of the connected device. |
| Console (SSH) | Authorized users can use SSH to connect to the console of the connected device. |
| Console (TelnetSSH) | Authorized users can use Telnet and/or SSH to connect to the console of the connected device simultaneously. When 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 computer terminal is connected to the console port on a device, a Terminal Server (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.

You can configure serial ports to support computer terminals in the following two ways:

- 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 CS.

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 10-3:** Expert > Terminal Server (TS) Connected Protocols

| **Protocol Name** | **Result** |
|---|---|
| Telnet | Dedicates a computer terminal that is connected to a serial port to access a server using the Telnet protocol. When the attached terminal is powered on, CS 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 computer terminal that is connected to the selected serial port to access a server using the SSHv1 protocol. When the attached terminal is powered on, the CS opens an SSHv1 session on the server. The server’s IP address should be specified on the “Other” form, Ports > Physical Ports > Other. |
| SSHv2 | Dedicates a computer terminal that is connected to the selected serial port to access a server using the SSHv2 protocol. When the attached terminal is powered on, the CS opens a SSHv2 session on the server. The server’s IP address should be specified on the “Other” form, Ports > Physical Ports > Other. |

**Table 10-3:** Expert > Terminal Server (TS) Connected Protocols (Continued)

| Protocol Name | Result |
|---|---|
| Local Terminal | Dedicates a computer terminal that is connected to the selected serial port for connecting to CS. When the attached terminal is powered on, CS opens a Telnet session on itself. The user then can use any of the CS'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 computer terminal that is connected to the selected serial port to access a specific remote host using the Raw Socket protocol. When the attached terminal is powered on, the CS opens a Raw Socket session on the host using an IP address and TCP port number that should be specified on the "Other" form, Ports > Physical Ports > Other. |

## 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.

**Note:** The Console profile features such as data buffering, multiple users, and event notifications are not available under this protocol.

When the attached terminal is powered on and the keyboard's [Enter] key is pressed, a login banner and a login prompt is displayed.

**Note:** If the user does not login 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 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.

## Modem and Power Management Connection Protocols

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

**Table 10-4:** Expert > Protocols for Serial Ports Connected to Modems or IPDUs

| Protocol Name | Result |
|---|---|
| PPP-No Auth | Starts a PPP session without interactive authentication required. Assumes the specified CS serial port is connected to an external modem. |
| PPP | Starts a PPP session with authentication required. Assumes the specified CS serial port is connected to an external modem. |
| SLIP | Starts a SLIP session. Assumes the specified CS serial port is connected to an external modem. |
| CSLIP | Starts a CSLIP session. Assumes the specified CS serial port is connected to an external modem. |
| Power Management | Configures the serial port for power management. Assumes an AlterPath PM 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, click the appropriate Modify Ports button.

   The General form appears.

   The port configuration section includes six forms in tabbed format as shown in the following figure.

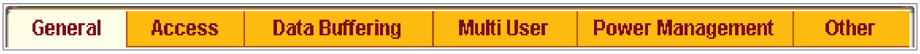
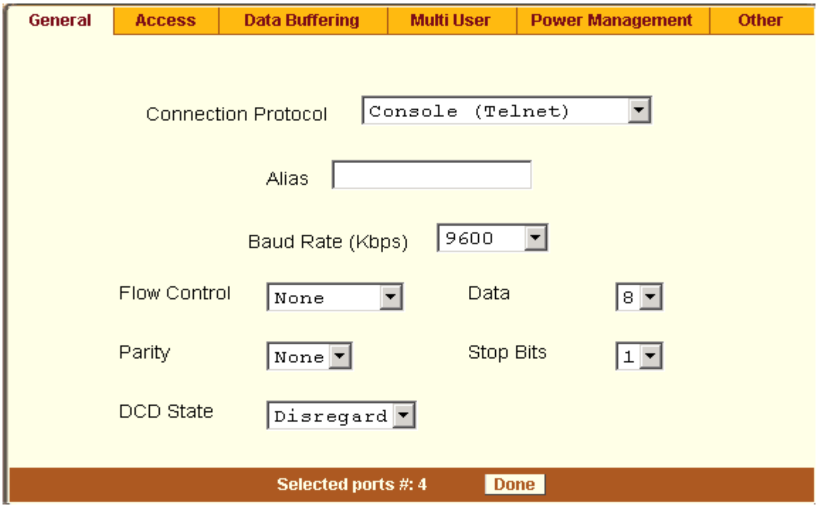


**Figure 10-5:** Expert > Ports > Physical Ports > Console Connection Active Tabs

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 all the active tabs in yellow.



Connection Protocol: Console (Telnet)

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

Stop Bits: 1

DCD State: Disregard

Selected ports #: 4

**Figure 10-6:** Expert > Ports > Physical Ports > Console Connection

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).

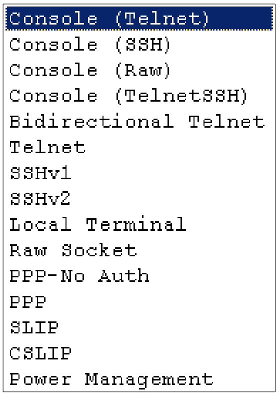


**Figure 10-7:**Connection Protocols > Console

4. If you want to change any of the other current settings, see "To Configure Serial Port Settings to Match the connected devices" on page 257.

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

   - For user access and authentication methods see "Access" on page 259.
   - To specify the TCP Port number and other port configuration options see "Other" on page 277.

## ▼ *To Configure a Serial Port Connection Protocol for a Bidirectional Telnet*

This 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 245.

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.

   The port configuration section includes six forms in tabbed format as shown in the following figure.

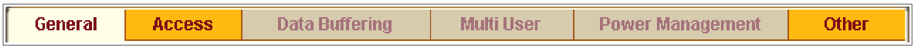
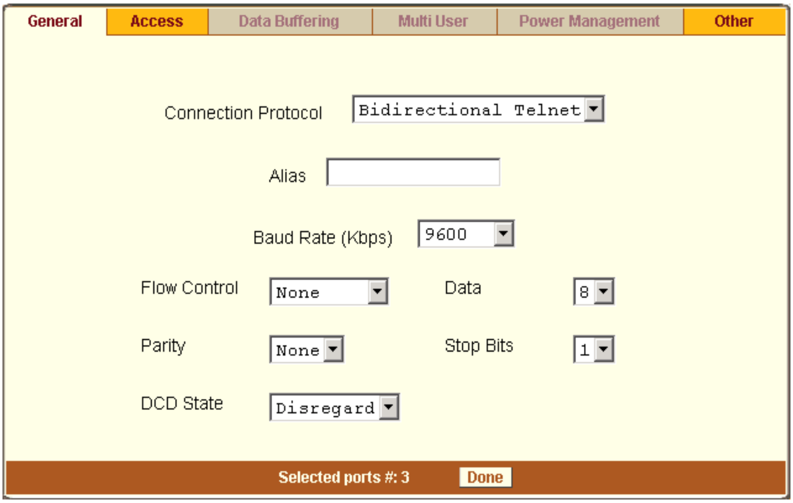


**Figure 10-8:** Expert > Ports > Physical Ports > Bidirectional Telnet Active Tabs

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 highlighted in yellow.



Connection Protocol: Bidirectional Telnet

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

Stop Bits: 1

DCD State: Disregard

Selected ports #: 3

**Figure 10-9:** Expert > Ports > Physical Ports > Bidirectional Telnet Connection

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

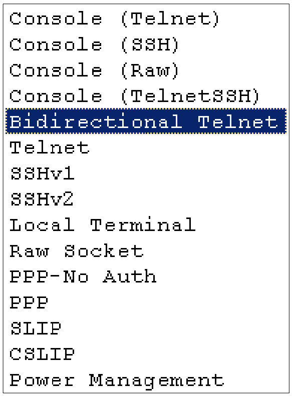


**Figure 10-10:** Connection Protocols > Bidirectional Telnet

4. If you want to change any of the other current settings, see "To Configure Serial Port Settings to Match the connected devices" on page 257.
5. Go to “Access” tab and configure the following settings:
   - In the “Authorized Users/Groups” field restrict or deny access to a serial port by specifying one or more users or groups.
   - From the “Type” pull-down menu, select an authentication type for the serial port. The default is no authentication (Type=None).
   - In the “BidirectionLogin Timeout” field enter the time for the serial port to return to 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.
   - In the “BidirectionShell 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 Web Manager > Applications > Terminal Profile Menu form.  For more information on configuring a menu shell see “Terminal Profile Menu” on page 146.

### ▼ *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 243.

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.

   The port configuration section includes six forms in tabbed format as shown in the following figure.

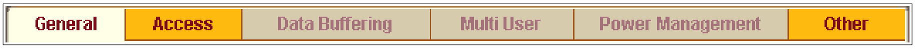
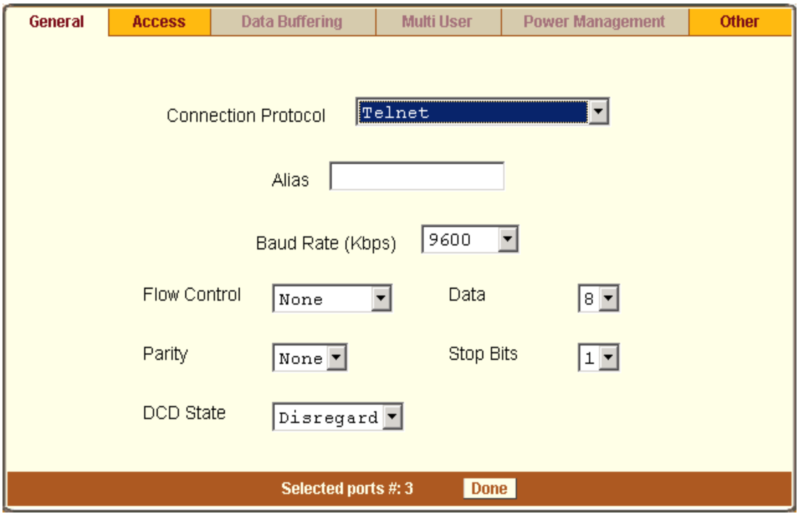


**Figure 10-11:**Expert > Ports > Physical Ports > Terminal Server Active Tabs

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 highlighted in yellow.



Connection Protocol: Telnet

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

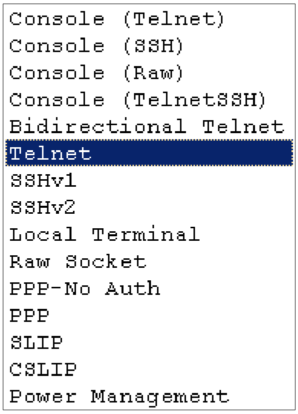
Stop Bits: 1

DCD State: Disregard

Selected ports #: 3

**Figure 10-12:** Expert > Ports > Physical Ports > Terminal Server Connection

**3.** To change the connection protocol, select a Terminal Server connection from the "Connection Protocol" pull-down men, "Telnet", "SSHv1", "SSHv2", "Local Terminal", or "Raw Socket".



```
Console (Telnet)
Console (SSH)
Console (Raw)
Console (TelnetSSH)
Bidirectional Telnet
Telnet
SSHv1
SSHv2
Local Terminal
Raw Socket
PPP-No Auth
PPP
SLIP
CSLIP
Power Management
```

**Figure 10-13:** Connection Protocols > Terminal Server

4. To configure a terminal to automatically connect to CS, do 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, do 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.

   The port configuration section includes six forms in tabbed format as shown in the following figure.

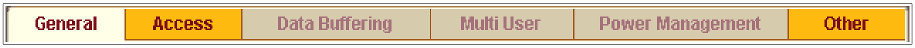
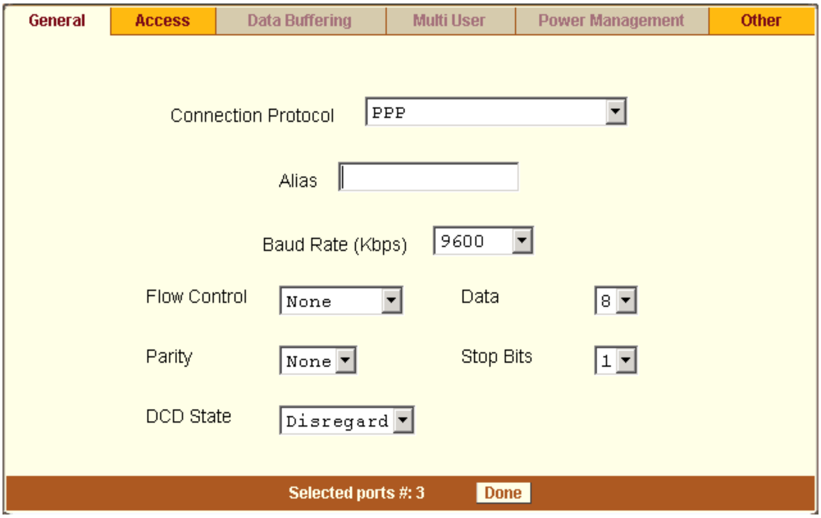


**Figure 10-14:** Expert > Ports > Physical Ports > Modem Connection Active Tabs

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 highlighted in yellow.



Connection Protocol: PPP

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

Stop Bits: 1

DCD State: Disregard

Selected ports #: 3

**Figure 10-15:** Expert > Ports > Physical Ports > Modem Connection

**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".

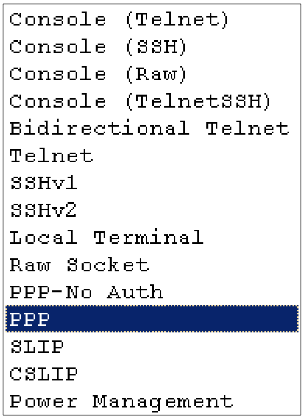


**Figure 10-16:** Connection Protocols > Modem

4. If you want to change any of the other current settings, see "To Configure Serial Port Settings to Match the connected devices" on page 257.
5. To further configure the serial port’s connection protocol:
   - For user access and authentication methods, see "Access" on page 259.
   - To specify the TCP Port number, and configure modem initialization and PPP options see "Other" on page 277.
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, click the appropriate Modify Ports button.

   The General form appears.

   The port configuration section includes six forms in tabbed format as shown in the following figure.

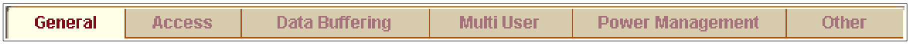
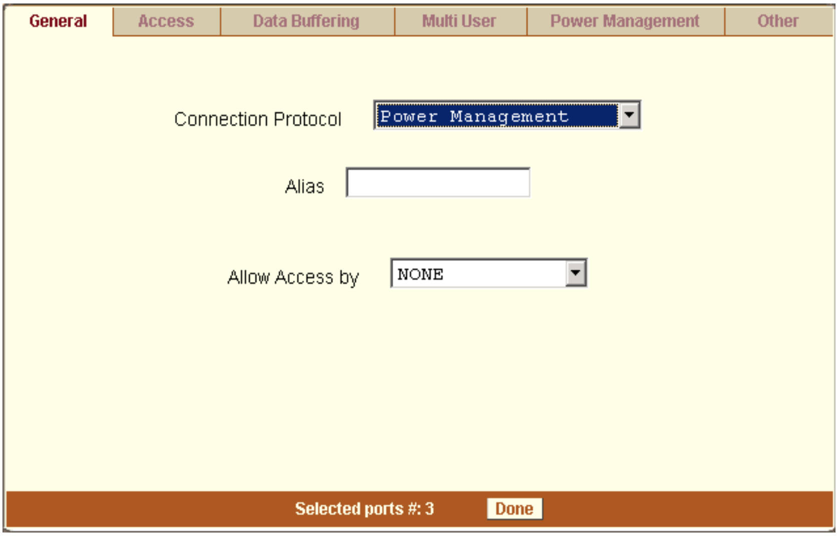


**Figure 10-17:** Expert > Ports > Physical Ports > Power Management Active Tabs

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.



Connection Protocol: Power Management

Alias:

Allow Access by: NONE

Selected ports #: 3

**Figure 10-18:** Expert > Ports > Physical Ports > Power Management Connection

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

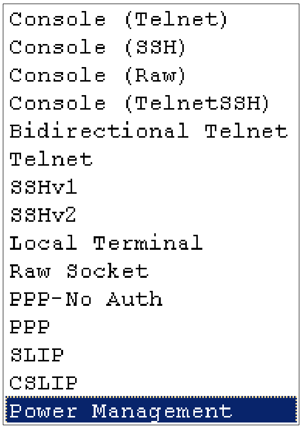


**Figure 10-19:** Connection Protocols > Power Management

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

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

6. Go to “Access” tab.

   a. enter the users/groups that are authorized to access the serial port.

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

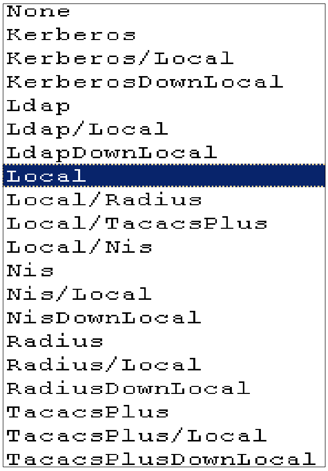


**Figure 10-20:** Access > Authentication Types

---

**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.

---

7. Go to “Other” tab.

   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. Enable “Biometric Authentication Required” if you are using an AlterPath Bio device.

---

**Note:** “Biometric Authentication Required” field is available when the selected access method is SSH or SSH and Telnet.

---

8. If you are finished, click “Done.”
9. Click “apply changes.”

### ▼ To Associate an Alias to a Serial Port

An alias (name) can be associated to a port when it’s individually selected for modification. To associate an alias to a port perform the following steps.

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

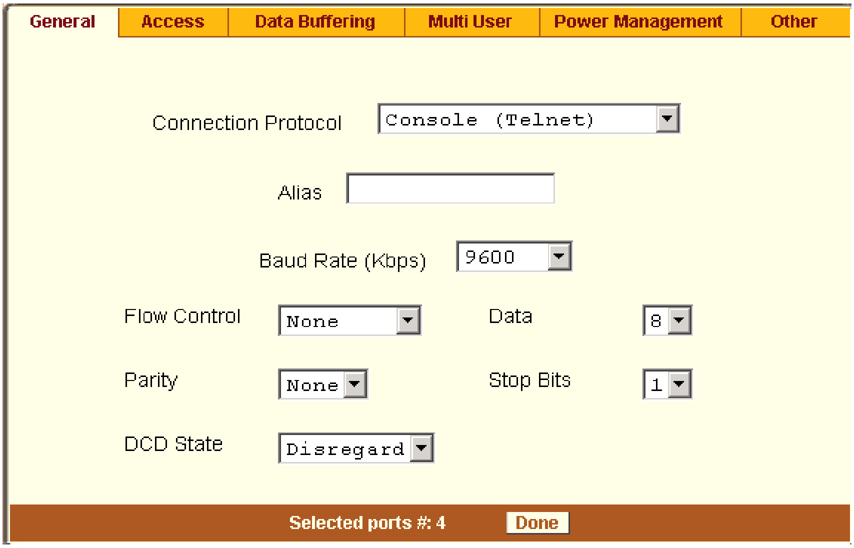
**Note:** The Alias field cannot be set if you select the “Modify All Ports”.

### ▼ To Configure Serial Port Settings to Match the connected devices

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

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

   The General form appears.



Connection Protocol: Console (Telnet)

Alias:

Baud Rate (Kbps): 9600

Flow Control: None

Data: 8

Parity: None

Stop Bits: 1

DCD State: Disregard

Selected ports #: 4

**Figure 10-21:** Expert > Ports > Physical Ports > Serial Port Settings

2. To change the baud rate, select an option from 2400 to 921600 Kbps from the Baud Rate pull-down menu.

   The default is 9600, which is the most common baud rate for serially-managed devices.

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.

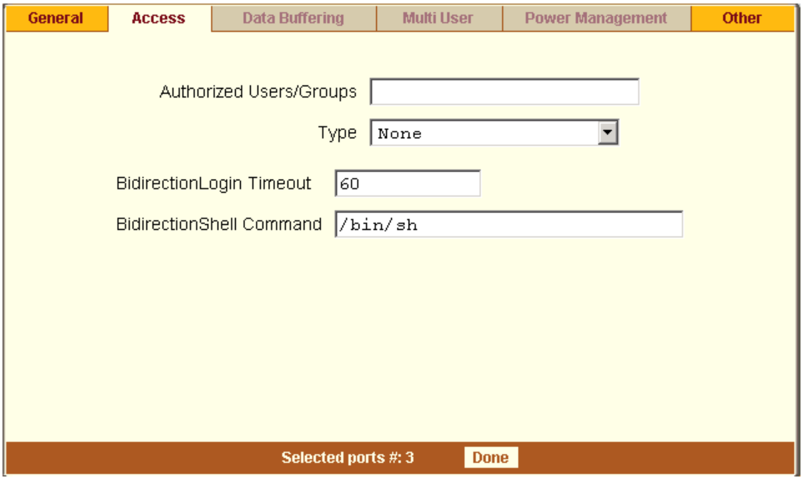
7. To change whether the “DCD (Data Carrier Detect) State” is disregarded or not, select either “Disregard” or “Regard”.

8. Click “Done.”

9. Click “apply changes.”

## Access

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



Authorized Users/Groups

Type: None

BidirectionLogin Timeout: 60

BidirectionShell Command: /bin/sh

Selected ports #: 3

**Figure 10-22:**Expert > Ports > Physical Ports > Access Form

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

**Table 10-5:** Expert > Access Form Fields

| Field | Description |
|---|---|
| Authorized Users/Groups | Restrict or deny access to a serial port by specifying one or more users or groups.<br>You can deny access to one or more users or groups by entering an exclamation point (!) before the user or group name.<br>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:<br>`!noadmin,johnd`<br>Note that the 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).<br>**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.<br>This field is available only when a Bidirectional Telnet protocol is selected from Ports > Physical Ports > General > Connection Protocol. |

**Table 10-5:** Expert > Access Form Fields

| Field | Description |
|---|---|
| BidirectionShell Command | Specify the menu shell command in this field, for example, /bin/menush and build a custom menu for the TS profile using Web Manager > Applications > Terminal Profile Menu form.<br>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 want 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 the 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 him/her. An authentication fallback mechanism can be defined in case the first authentication level fails. See the following table on authentication methods and fallback mechanisms.

**Table 10-6:** Expert > Authentication Methods

| 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 `/etc/portslave/pslave.conf` on CS.
6. Make sure that an authentication server is specified for the selected authentication type.

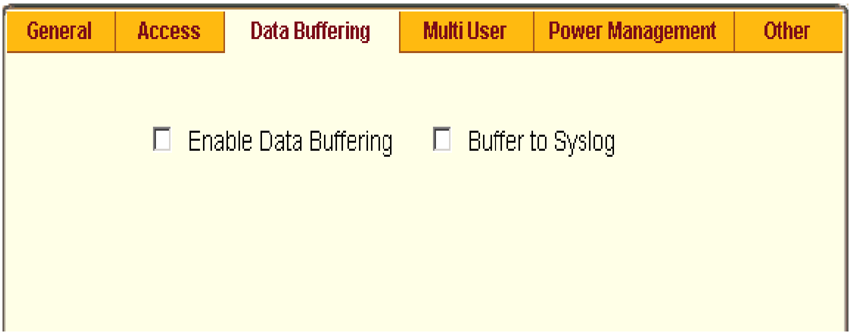
The following table lists the procedures that apply to each authentication method.

**Table 10-7:** Expert > Procedures to Configure an Authentication Server

| Authentication Method | Where Documented |
|---|---|
| **Kerberos, Kerberos/Local, or Kerberos/ DownLocal** | "To Configure a Kerberos Authentication Server" on page 223. |
| **LDAP, LDAP/Local, or LDAP/DownLocal** | "To Configure an LDAP Authentication Server" on page 221. |
| **NIS, Local/NIS, NIS/Local, or NIS/ DownLocal** | "To Configure a NIS Authentication Server" on page 225. |
| **RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal** | "To Configure a RADIUS Authentication Server" on page 218. |
| **TACACSPlus, Local/TACACSPlus, TACACSPlus/Local, or TACACSPlusDownLocal** | "To Configure a TACACS+ Authentication Server" on page 219. |

## 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 following form appears.



☐ Enable Data Buffering ☐ Buffer to Syslog

**Figure 10-23:**Expert > Ports > Physical Ports > Data Buffering

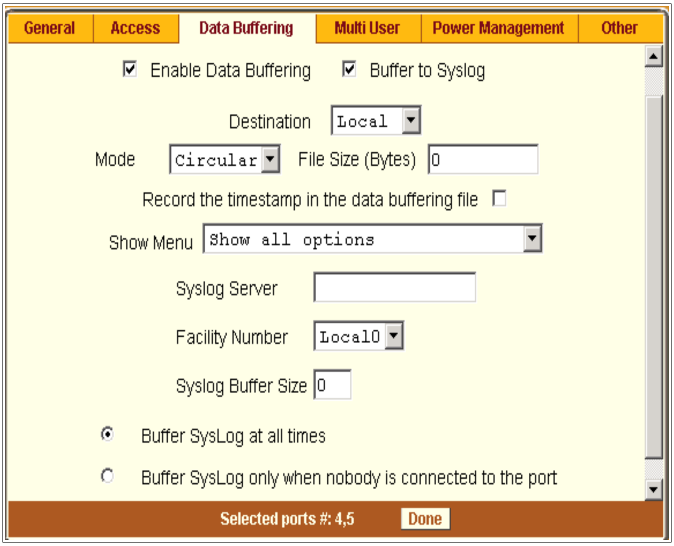
There are different fields on this form depending on whether one or both options are enabled. The form displays “Enable Data Buffering” and “Buffer to Syslog” options.

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

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 form shows both checkboxes (“Enable Data Buffering” and “Buffer to Syslog”) and the “Local” destination selected.



☑ Enable Data Buffering ☑ Buffer to Syslog

Destination: Local

Mode: Circular File Size (Bytes): 0

Record the timestamp in the data buffering file □

Show Menu: Show all options

Syslog Server:

Facility Number: Local0

Syslog Buffer Size: 0

● Buffer SysLog at all times

○ Buffer SysLog only when nobody is connected to the port

Selected ports #: 4,5

**Figure 10-24:** Expert > Ports > Physical Ports > Data Buffering

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

**Table 10-8:** Expert > Data Buffering Form Fields

| Field Name | Definition |
|---|---|
| Destination | Location for the data files. Either “Local” or “Remote” |

**Table 10-8:** Expert > Data Buffering Form Fields

| Field Name | Definition |
|---|---|
| Mode (Local Destination) | *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. |
| 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.<br>**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 CS. |
| Record the timestamp... | Save a timestamp with the data in the data buffer file. |
| Show Menu | Options for the buffer file. |
| Syslog Server | The IP address for the preconfigured Syslog server. |
| Facility Number | Choose a facility number to assign to CS. Obtain the facility number for CS from the system administrator of the syslog server. The facility number is included in any syslog message generated from CS. The server's administrator can use facility numbers to isolate logs from individual devices into individual files.<br>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 nobody is connected to the port | As indicated. |

### ▼ *To Configure Data Buffering for Serial Ports*

Perform this procedure if you want to configure data buffering. Obtain the facility number for the CS 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" and perform the following steps.

   a. 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.

   b. If you chose "Local" from the "Destination" pull-down menu, do the following:

      i. Choose "Circular" or "Linear" from the "Mode" pull-down menu.

      ii. Enter a size larger than 0 in the "File Size (Bytes)" field.

   c. 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.

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

   e. From the "Show Menu" pull-down menu, choose among the following options:

      - Show all options
      - No

- Show data buffering file only
- Show without the erase options

4. If you checked “Buffer to Syslog,” perform the following steps.

   a. Enter the IP address of the syslog server in the “Syslog Server” field.

   b. Choose an option from the “Facility Number” pull-down menu.

**Note:** Obtain the facility number from the system administrator of the syslog server. Options range from Local0 to Local7.

   c. Enter the maximum size of the buffer in the “Syslog Buffer Size” field.

   d. Click the radio button next to one of the following options:

   - Buffer Syslog at all times
   - Buffer only when nobody is connected to the port

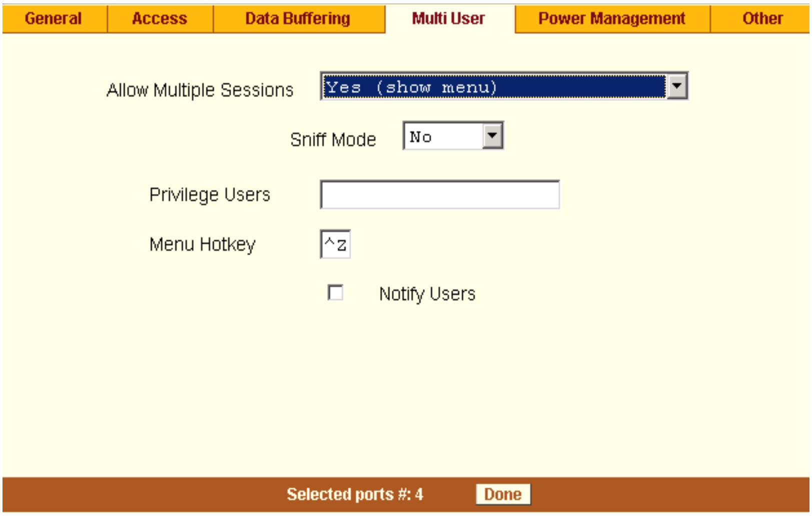
5. Click “Done.”

6. Click “apply changes.”

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

## Multi User

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



Allow Multiple Sessions: Yes (show menu)

Sniff Mode: No

Privilege Users:

Menu Hotkey: ^z

□ Notify Users

**Figure 10-25:**Expert > Port > Physical Ports >Multi User

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” drop-down menu, the “Privilege Users” field should be populated with the usernames who have access rights.

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

**Table 10-9:** 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). See Table 10-9 for more detail. |
| **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. |

| Field Name | Definition |
|---|---|
| **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 10-10:** Expert > Options on the “Allow Multiple Sessions” Menu

| Menu Option | Description |
|---|---|
| No | Do not allow multiple sessions. Only two users can connect to the same port simultaneously. One shared session and one normal session are allowed. |
| Yes (show menu) | More than two simultaneous users can connect to the same serial port.<br>A Sniffer menu is presented to the user and they can choose to:<br>• Open a sniff session<br>• Open a read/write session<br>• Cancel a connection<br>• Send a message to other users connected to the same serial port. |
| Read/Write (do not show menu) | Read/write sessions are opened, and the sniffer menu won’t be presented. |
| ReadOnly (do not show menu) | Read only sessions are opened, and the sniffer menu won’t be presented. |

### ▼ *To Configure Multiple Sessions and Port Sniffing for One or More Serial Ports*

1. Go to Ports > Physical Ports in Expert mode, and select a port or ports to modify.
2. Click the “Multi User” tab.

**3.** To allow or to prevent multiple sessions, select an option from the "Allow Multiple Sessions" pull-down menu.

The options are: "No," "Yes (show menu)," "Read/Write (do not show menu)," "ReadOnly."

**4.** To configure the type of data that displays on the monitor in a port-sharing session, select an option from the "Sniff Mode" pull-down menu.

**5.** If you have allowed multiple sessions, complete the following fields.

**a.** Add usernames to the "Privilege Users" field.

**b.** Enter a hot key 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.

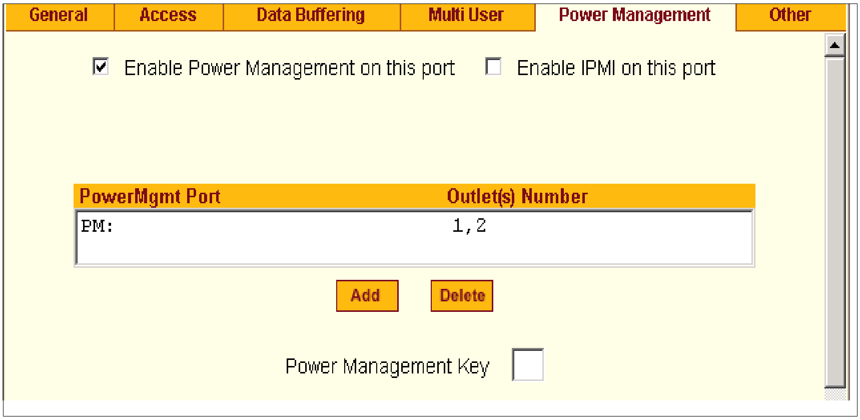
**c.** Enable the "Notify Users" field, if desired.

**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. The following form appears.



☑ Enable Power Management on this port ☐ Enable IPMI on this port

| PowerMgmt Port | Outlet(s) Number |
|---|---|
| PM: | 1,2 |

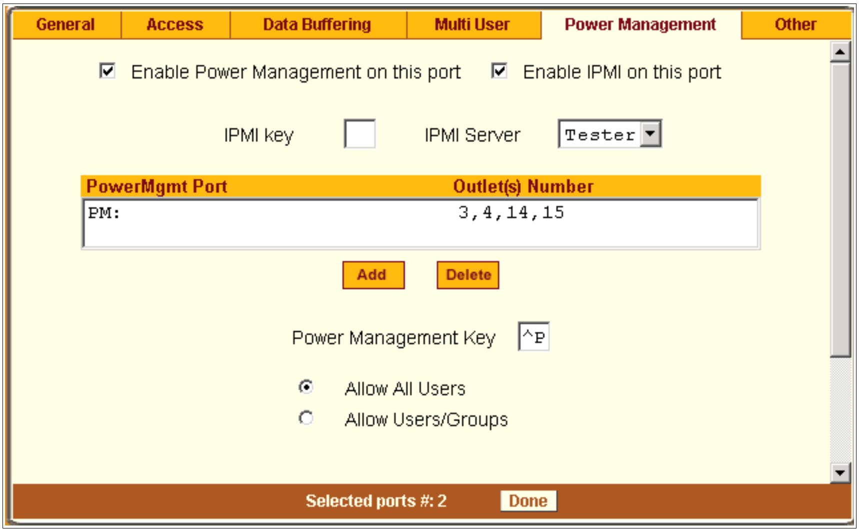
Power Management Key □

**Figure 10-26:**Expert > Ports > Physical Ports > Power Management

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 brings up a power management menu or dialog box by entering a hot key.

**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, as shown in the following figure.



☑ Enable Power Management on this port ☑ Enable IPMI on this port

IPMI key □ IPMI Server Tester

| PowerMgmt Port | Outlet(s) Number |
|---|---|
| PM: | 3,4,14,15 |

Power Management Key ^P

● Allow All Users

○ Allow Users/Groups

Selected ports #: 2

**Figure 10-27:** Expert > Ports > Physical Ports > Power Management

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

**Table 10-11:** 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). |

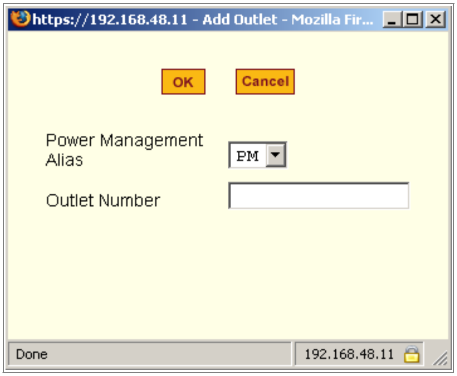
| Field Name | Definition |
|---|---|
| **Enable IPMI on this port** | Check mark to enable IPMI on the selected port(s). |
| **IPMI Key** (available only if IPMI is enabled) | The key sequence which the authorized user(s) can use to perform IPMI power management.<br>The default for IPMI power management 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.<br>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. |
| **New User/Group**<br>(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 CS is plugged into an AlterPath PM IPDU and is configured for power management.
- The device connected to CS 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, as shown in the following figure. In this dialog box, you can specify the AlterPath PM IPDU and the outlet number(s) into which the device is plugged.



https://192.168.48.11 - Add Outlet - Mozilla Fir...

OK Cancel

Power Management Alias: PM

Outlet Number:

Done 192.168.48.11

**Figure 10-28:** Expert > Ports > Physical Ports > Power Management > Add Outlets Dialog Box

The “PM” on the “Power Management Alias” pull-down menu in the example figure indicates that a serial port is configured for power management, and an IPDU is connected to the configured port. Entered outlet numbers are separated by commas. You would specify outlet number 1,2,3,4 as shown in the figure.

### ▼ *To Configure a Serial Port for IPDU or IPMI Power Management*

1. Go to Ports > Physical Ports, select a port or ports to modify, 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." and perform the following steps.

   a. Select the name of a port configured for power management and click the "Add" button.

      The "Add Outlet" dialog box appears.

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

   c. Click OK.

      The power management port and the specified outlet numbers display on the PowerMgmt Port list.

   d. Enter the power management hot key in the "Power Management Key" field.

      Enter a caret (`^`) for the escape key, as in `^p`. The caret stands for the `Ctrl` key.

   - If you want to configure IPMI power management on this port, continue to Step 3.
   - If you are done, go to Step 4.

3. To enable IPMI Power Management of an IPMI device connected to the currently selected port, do the following steps.

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

   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 hot key to bring up the IPMI power management screen.

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

4. Click “Done.”

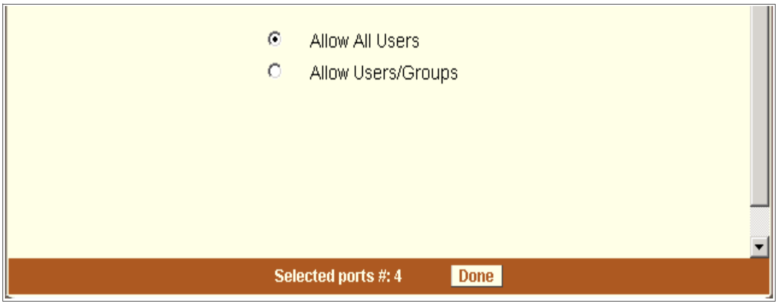
5. Click “apply changes.”

### ▼ *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 CS’s serial ports.

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

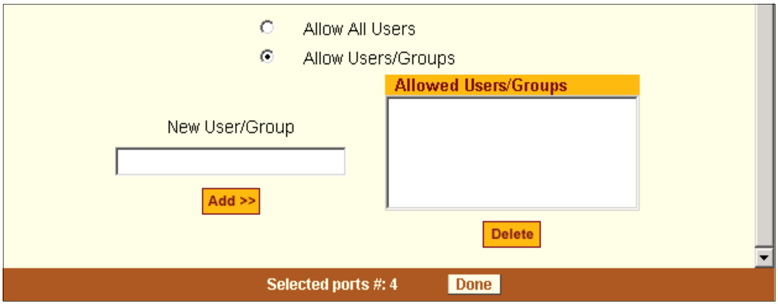
2. To permit everyone to perform power management on this port, click the “Allow All Users” radio button.



● Allow All Users
○ Allow Users/Groups

**Figure 10-29:** Expert > Ports > Physical Ports > Power Management>Allow All Users

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



○ Allow All Users
● Allow Users/Groups

**Figure 10-30:** Expert > Ports > Physical Ports >Power Management >Allow Users/ Groups

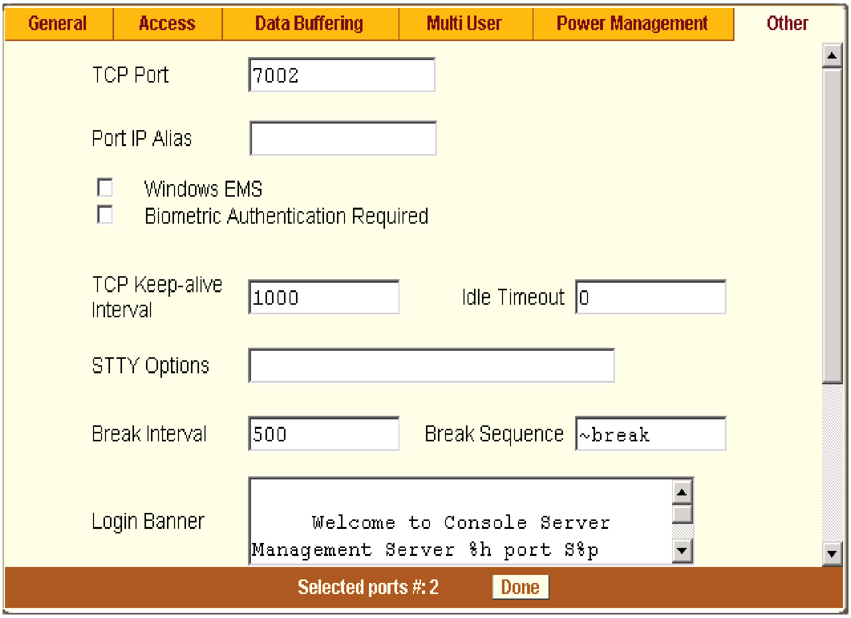
4. Enter a valid username or groupname in the “New User/Group” field, and click “Add.”

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 the Modify Port(s), you can select the Other form from the tabbed menu to configure other options. The following form appears.



TCP Port: 7002

Port IP Alias:

□ Windows EMS

□ Biometric Authentication Required

TCP Keep-alive Interval: 1000

Idle Timeout: 0

STTY Options:

Break Interval: 500

Break Sequence: ~break

Login Banner:

```
     Welcome to Console Server
Management Server %h port S%p
```

Selected ports #: 2

**Figure 10-31:**Expert > Ports > Physical Ports > Other Form

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 10-12:** Expert > Ports > Physical Ports > 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 CS unit has. For example, an CS unit with 8 serial ports have TCP port numbers 7001 through 7008. |
| **Port IP Alias** | A name (alias) for the IP of the selected port. A port IP alias field 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” drop-down menu on the General form. |
| **Biometric Authentication Required** | Adds another layer of security by using the AlterPath Bio authentication scanner. This option is available when a “Console (SSH)”, or a “Console (TelnetSSH) 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. |

| Field Name | Definition |
|---|---|
| **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 (Ctrl-b) |
| **Login Banner** | Enter the text you wish to appear as a login banner when logging into a terminal. |
| **Host to Connect** | This field should be populated with the IP address of the device you are connecting to. The field is displayed when a terminal server (TS) profile is selected from the “Connection Protocol” drop-down menu on the General form. |
| **Terminal Type** | This field should be populated with the terminal type when connecting to a host system. The field is displayed when a terminal server (TS) profile is selected from the “Connection Protocol” drop-down menu on the General form. |

### ▼ *To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console*

1. Go to Ports > Physical Ports in Expert mode, and select a port or ports to modify.
2. Select the “Other” tab.

3. To change the port number for the serial port, enter another number in the “TCP Port” field.
4. To assign a name to the port’s IP address, enter an alias in the “Port IP Alias” field. (Console connection protocol only)
5. 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)
6. If using AlterPath Bio for an additional layer of security, enable “Biometric Authentication Required” field. (Console SSH 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*

Do this procedure if you have connected a computer terminal to a serial port.

1. Select the port and choose a terminal server (TS) profile from the “Connection Protocol” drop-down menu on General form.
2. Select the “Other” tab.

   The Other form appears.

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

## *Virtual Ports*

When Virtual Ports is selected under Ports > Virtual Ports in Expert mode, the following form appears.

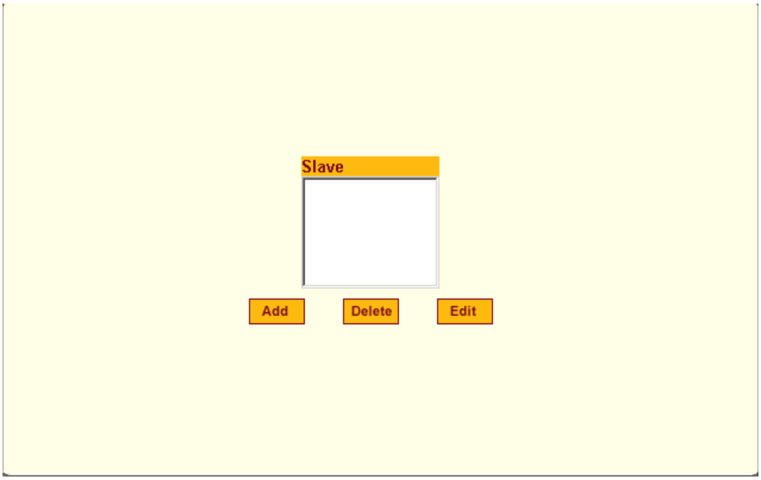


**Figure 10-32:** Expert > Ports > Virtual Ports

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

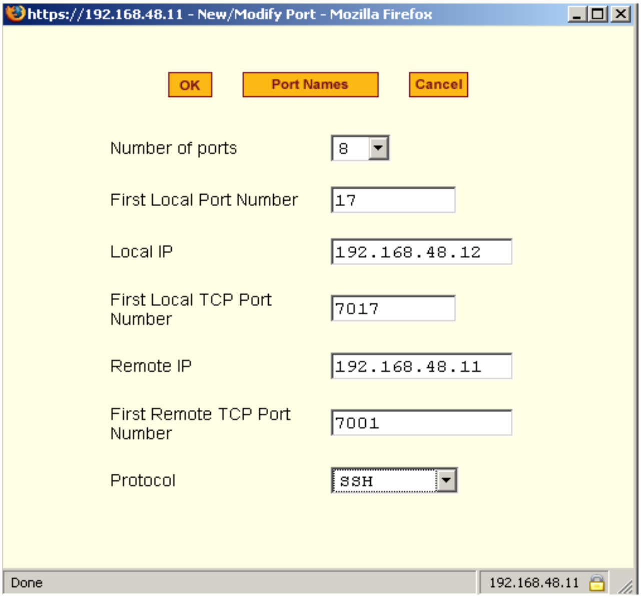
**Note:** Clustering only works for ports that are configured as CAS profile.

You can use one CS as the “master” unit to control other CS units as “slaves”. The ports on the slave unit(s) appears as if they are part of the master unit.

**Note:** Multiple IPDUs should only be connected and daisy-chained through the serial port of the master CS unit when you are configuring a cluster.

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

When you click the “Add” or “Edit” button on the Ports > Virtual Ports form, the following dialog box appears.



Number of ports: 8

First Local Port Number: 17

Local IP: 192.168.48.12

First Local TCP Port Number: 7017

Remote IP: 192.168.48.11

First Remote TCP Port Number: 7001

Protocol: SSH

**Figure 10-33:** Expert > Ports > Virtual Ports > New/Modify Port Dialog Box

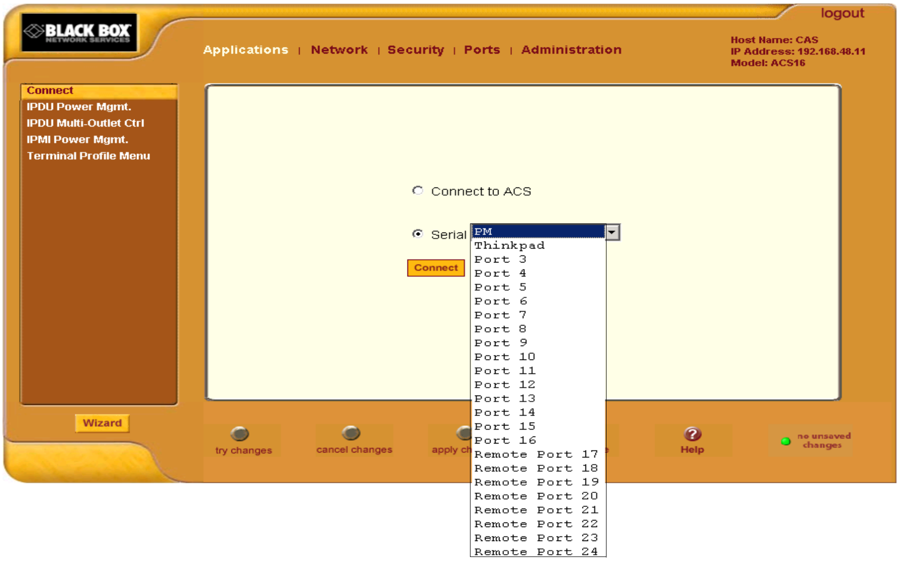
The following table describes the fields available in the Virtual Ports New/ Modify Port dialog box.

**Table 10-13:** Expert > New/Modify Port Dialog Box Fields

| Field Name | Definition |
|---|---|
| **Number of Ports** | Number of ports on each slave unit. Choices are 1, 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 CS or it can be the global IP address of the cluster in the network. |

| Field Name | Definition |
|---|---|
| **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. |
| **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” CS unit and defined the cluster parameters, the slave serial ports and the connected devices are accessible from the master CS unit under Applications > Connect > Serial pull-down menu as shown in the following figure.



Host Name: CAS
IP Address: 192.168.48.11
Model: ACS16

○ Connect to ACS

● Serial PM

**Figure 10-34:** Expert > Applications > Connect > Serial pull-down menu

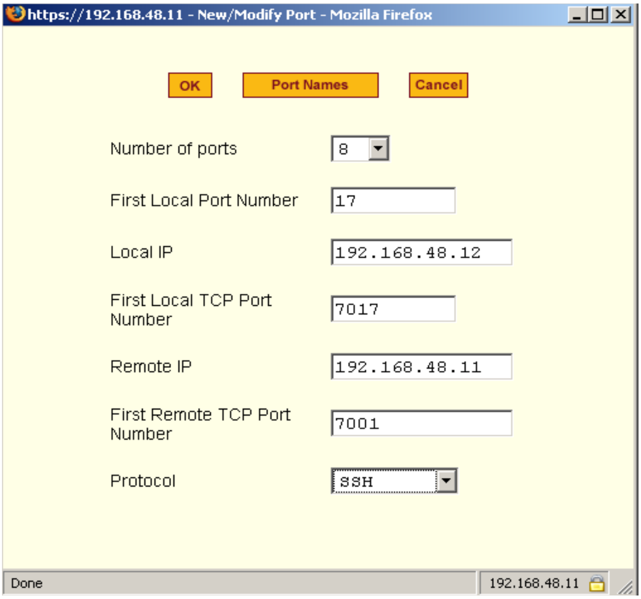
### ▼ *To Cluster CS Units or Modify Cluster Configuration*

Use this procedure if you want to cluster CS units and add or modify ports.

**Note:** CS boxes should be connected individually to an IP network. The units should not be cascaded.

1. Go to Ports > Virtual Ports in Expert mode, and click the “Add” button to add new slave ports, or click the “Edit” button to edit a slave port.

   The New/Modify Port dialog box appears.



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

Number of ports: 8

First Local Port Number: 17

Local IP: 192.168.48.12

First Local TCP Port Number: 7017

Remote IP: 192.168.48.11

First Remote TCP Port Number: 7001

Protocol: SSH

Done | 192.168.48.11

**Figure 10-35:** Expert > Ports > Virtual Ports > New/Modify Port Dialog Box

2. From the drop-down menu select the number of ports that you want to assign as slaves.

   Choices are 1, 4, 8, 16, 32 and 48.

3. Enter the “First Local Port Number”.

This is the first port number on the master, after the last 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, after the last 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”.

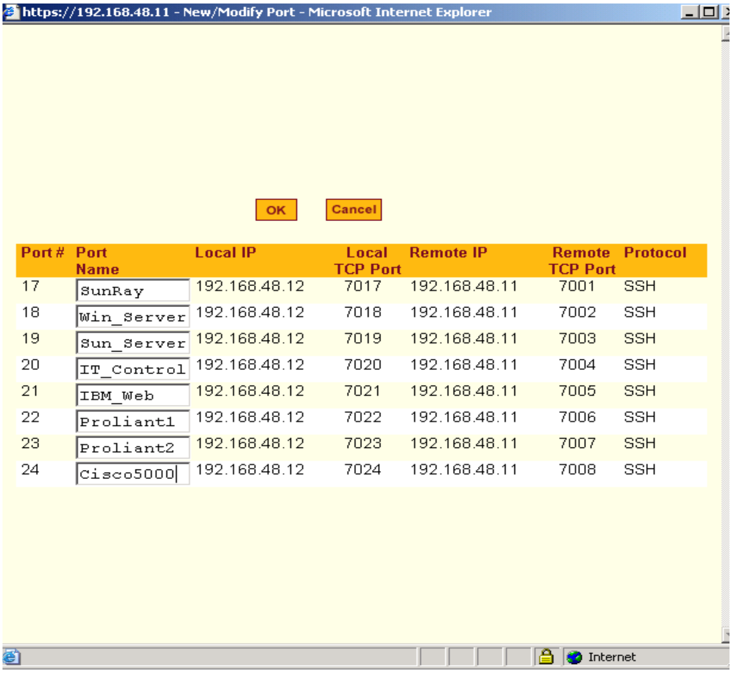
   This is the first TCP port number of the slave. The default is 7001.

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*

Pressing the “Port Names” button on the New/Modify Port dialog box, brings up the form shown in the following figure.


https://192.168.48.11 - New/Modify Port - Microsoft Internet Explorer
OK
Cancel
Internet

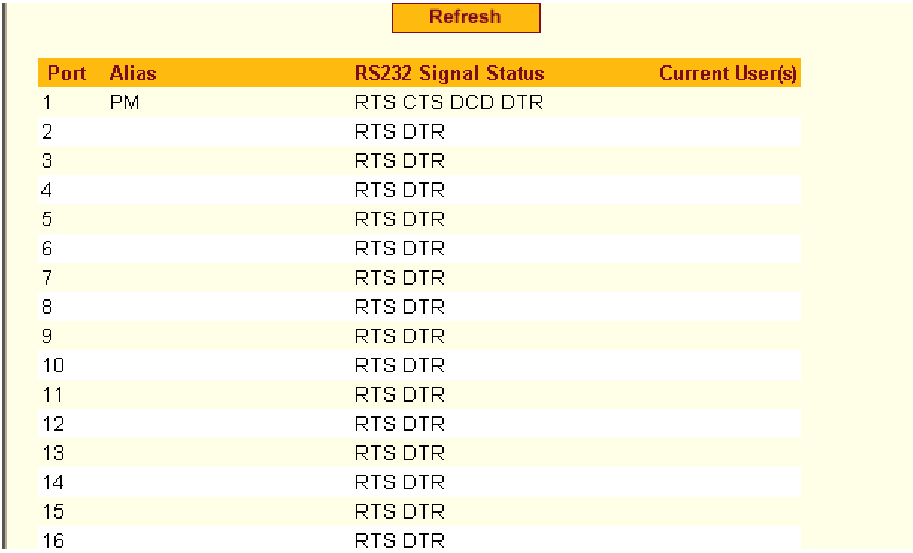
| Port # | Port Name | Local IP | Local TCP Port | Remote IP | Remote TCP Port | Protocol |
|---|---|---|---|---|---|---|
| 17 | SunRay | 192.168.48.12 | 7017 | 192.168.48.11 | 7001 | SSH |
| 18 | Win_Server | 192.168.48.12 | 7018 | 192.168.48.11 | 7002 | SSH |
| 19 | Sun_Server | 192.168.48.12 | 7019 | 192.168.48.11 | 7003 | SSH |
| 20 | IT_Control | 192.168.48.12 | 7020 | 192.168.48.11 | 7004 | SSH |
| 21 | IBM_Web | 192.168.48.12 | 7021 | 192.168.48.11 | 7005 | SSH |
| 22 | Proliant1 | 192.168.48.12 | 7022 | 192.168.48.11 | 7006 | SSH |
| 23 | Proliant2 | 192.168.48.12 | 7023 | 192.168.48.11 | 7007 | SSH |
| 24 | Cisco5000 | 192.168.48.12 | 7024 | 192.168.48.11 | 7008 | SSH |

**Figure 10-36:** Expert > Ports > Virtual Ports > New/Modify > Port Names Dialog box

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

## Ports Status

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



| Port | Alias | RS232 Signal Status | Current User(s) |
|---|---|---|---|
| 1 | PM | RTS CTS DCD DTR | |
| 2 | | RTS DTR | |
| 3 | | RTS DTR | |
| 4 | | RTS DTR | |
| 5 | | RTS DTR | |
| 6 | | RTS DTR | |
| 7 | | RTS DTR | |
| 8 | | RTS DTR | |
| 9 | | RTS DTR | |
| 10 | | RTS DTR | |
| 11 | | RTS DTR | |
| 12 | | RTS DTR | |
| 13 | | RTS DTR | |
| 14 | | RTS DTR | |
| 15 | | RTS DTR | |
| 16 | | RTS DTR | |

**Figure 10-37:** Expert > Ports > Ports Status (Read-Only)

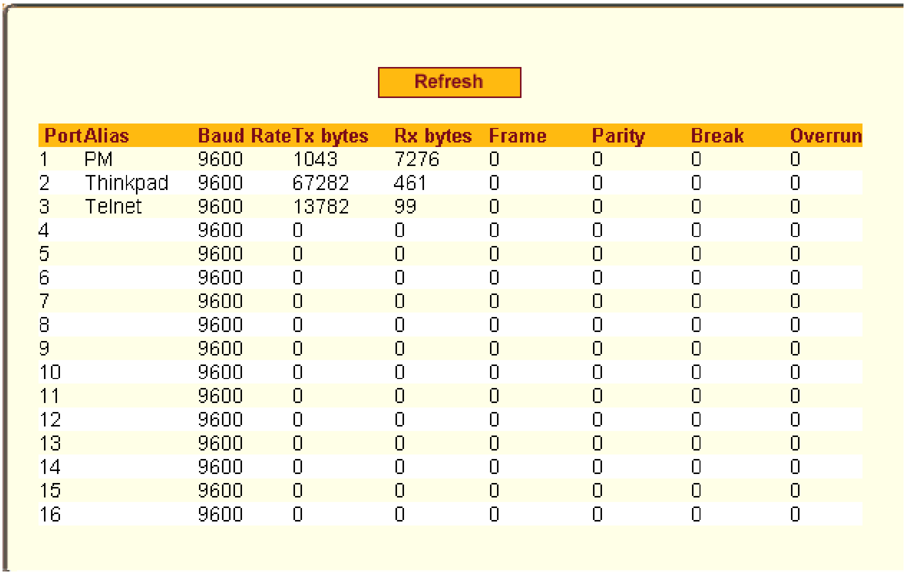
The information in the following table is available in the Ports Status read-only form. All users have access to this form. The information on this page gets updated when you click the “Refresh” button.

**Table 10-14:** Expert > Port Status Read-Only Form

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

## *Ports Statistics*

Selecting Ports > Port Statistics in Expert mode, brings up the following read-only form.



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

**Figure 10-38:** Expert > Ports > Port Statistics (Read-Only)

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

**Table 10-15:** 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. |

| Column Name | Description |
|---|---|
| **Parity** | Error checking bit appended to a data packet.<br>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. |

# Chapter 11
# Administration Menu & Forms

This Chapter describes the “Administration” menu and the related forms. The following table provides a description of the left menu panel links to the detailed information and procedures.

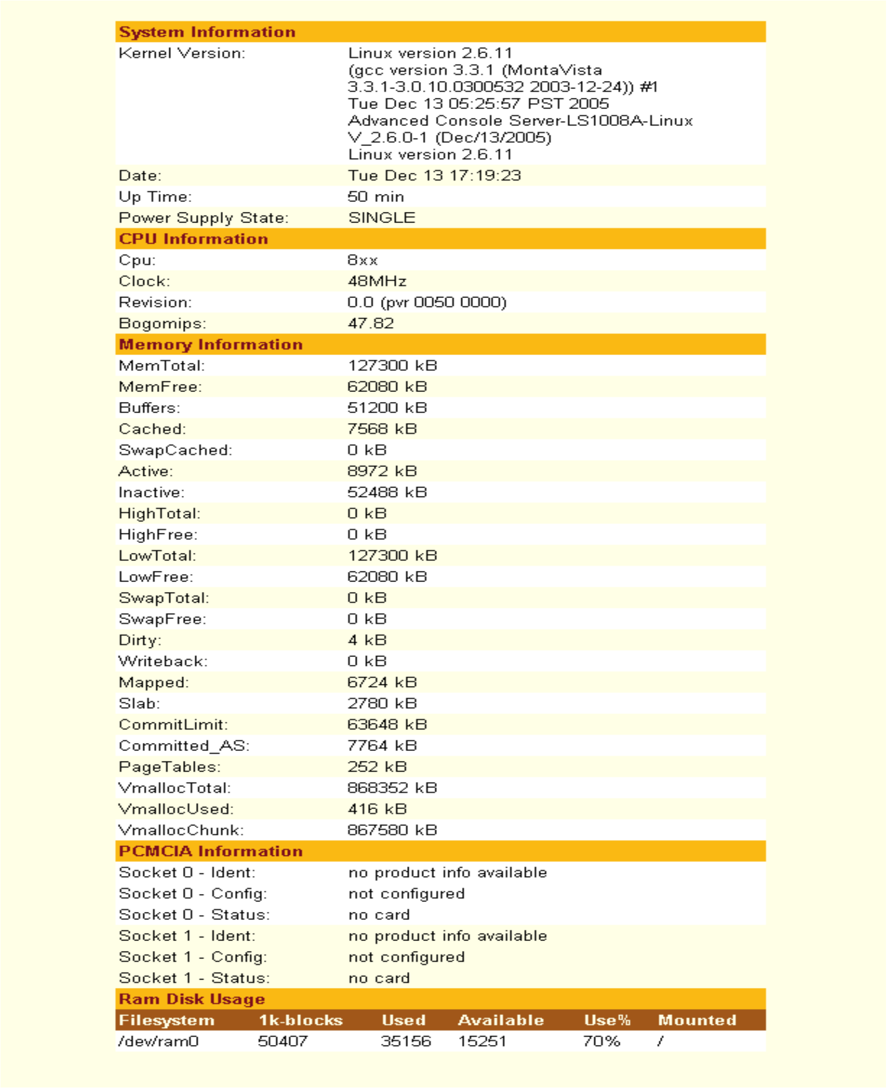
**Table 11-1:** Expert > Administration Menu

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **System Information** | View information on the system hardware, version, file system and PCMCIA cards loaded. | Page 292 |
| **Notifications** | Configure the alarm strings and the destination of the notification. CS can send notification by email, pager or SNMP trap in the occurrence of any system warnings and alarms. | Page 295 |
| **Time/Date** | Set the timezone and configure the system’s date and time manually, or use Network Time Protocol (NTP). | Page 305 |

| Menu Selection | Use this menu to: | Where Documented |
|---|---|---|
| **Boot Configuration** | Configure CS to boot from its internal firmware or from the network.<br>This section defines the settings for loading the operating system in the event that the CS fails to boot successfully. CS can boot from its internal firmware or from the network. | Page 307 |
| **Backup Config** | Configure an FTP server to save and retrieve your CS configuration, or choose a storage device to store your configuration. | Page 310 |
| **Upgrade Firmware** | Upload or upgrade to a new firmware. | Page 313 |
| **Reboot** | Reboot the CS. | Page 316 |
| **Online Help** | Configure a path to a local server for storing the online help files. | Page 317 |

## *System Information*

Selecting Administration > System information in Expert mode brings up the following information form.



| System Information | |
|---|---|
| Kernel Version: | Linux version 2.6.11<br>(gcc version 3.3.1 (MontaVista<br>3.3.1-3.0.10.0300532 2003-12-24)) #1<br>Tue Dec 13 05:25:57 PST 2005<br>Advanced Console Server-LS1008A-Linux<br>V_2.6.0-1 (Dec/13/2005)<br>Linux version 2.6.11 |
| Date: | Tue Dec 13 17:19:23 |
| Up Time: | 50 min |
| Power Supply State: | SINGLE |
| **CPU Information** | |
| Cpu: | 8xx |
| Clock: | 48MHz |
| Revision: | 0.0 (pvr 0050 0000) |
| Bogomips: | 47.82 |
| **Memory Information** | |
| MemTotal: | 127300 kB |
| MemFree: | 62080 kB |
| Buffers: | 51200 kB |
| Cached: | 7568 kB |
| SwapCached: | 0 kB |
| Active: | 8972 kB |
| Inactive: | 52488 kB |
| HighTotal: | 0 kB |
| HighFree: | 0 kB |
| LowTotal: | 127300 kB |
| LowFree: | 62080 kB |
| SwapTotal: | 0 kB |
| SwapFree: | 0 kB |
| Dirty: | 4 kB |
| Writeback: | 0 kB |
| Mapped: | 6724 kB |
| Slab: | 2780 kB |
| CommitLimit: | 63648 kB |
| Committed_AS: | 7764 kB |
| PageTables: | 252 kB |
| VmallocTotal: | 868352 kB |
| VmallocUsed: | 416 kB |
| VmallocChunk: | 867580 kB |
| **PCMCIA Information** | |
| Socket 0 - Ident: | no product info available |
| Socket 0 - Config: | not configured |
| Socket 0 - Status: | no card |
| Socket 1 - Ident: | no product info available |
| Socket 1 - Config: | not configured |
| Socket 1 - Status: | no card |

**Ram Disk Usage**

| Filesystem | 1k-blocks | Used | Available | Use% | Mounted |
|---|---|---|---|---|---|
| /dev/ram0 | 50407 | 35156 | 15251 | 70% | / |

**Figure 11-1:** Expert > Administration > System Information

You can use the form to view the information shown in the following table.

**Table 11-2:** System Information

| **Information** | Parameters |
|---|---|
| **System** | • Kernel Version<br>• Current Date<br>• Up Time<br>• Power Supply State |
| **CPU** | • CPU Type<br>• Clock Speed<br>• Revision<br>• Bogomips |
| **Memory** | • MemTotal<br>• MemFree<br>• Buffers<br>• Cached<br>• SwapCached<br>• Active<br>• Inactive<br>• HighTotal<br>• HighFree<br>• LowTotal<br>• LowFree<br>• SwapTotal<br>• SwapFree<br>• Dirty<br>• Writeback<br>• Mapped<br>• Slab<br>• CommitLimit<br>• Committed_AS<br>• PageTables<br>• VmallocTotal<br>• VmallocUsed<br>• VmallocChunk |

**Table 11-2:** System Information

| **Information** | Parameters |
|---|---|
| **PCMCIA** | Socket 0 and Socket 1<br>Identification, Configuration, and Status |
| **RAMDisk Usage** | • Filesystem<br>• 1k-blocks<br>• Used<br>• Available<br>• Use%<br>• Mounted |

### ▼ *To View System Information*

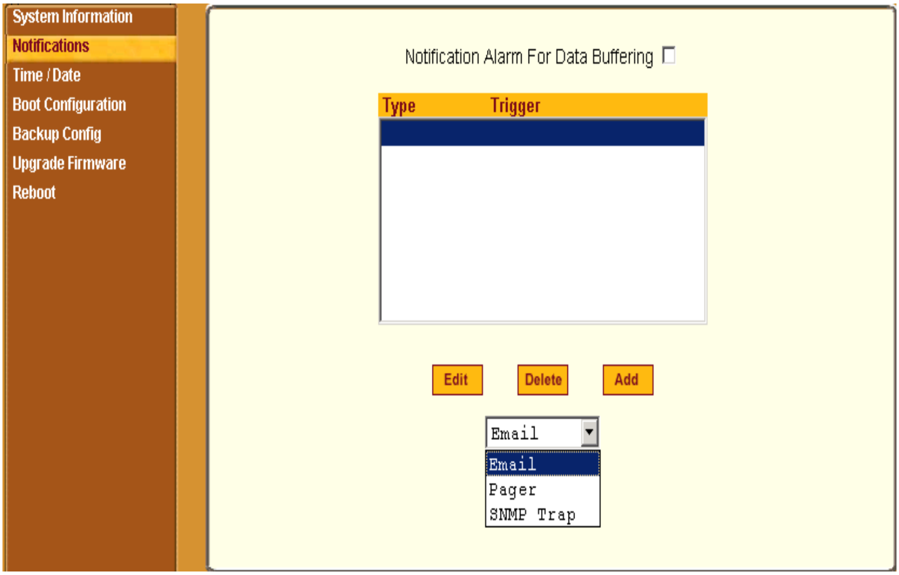
1. Go to Administration > System Information in Expert mode.

   The System Information form appears.

2. To view all the information scroll down the form.

## *Notifications*

Selecting Administration > Notifications in Expert mode brings up the following form.



Notification Alarm For Data Buffering □

Email

**Figure 11-2:** Expert > Administration > Notifications

You can use this form to set up alarm notifications about system issues, problems, or other events of interest that occur on the devices that are 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 11-3:** Expert > 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 and clicking the Edit button brings up 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*

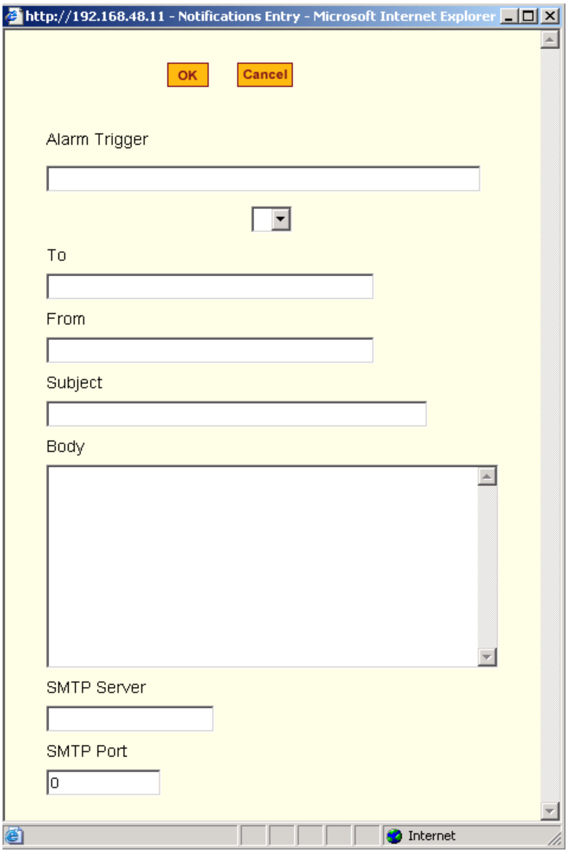
1. Go to Administration > Notifications in Expert mode.

   The Notifications form appears.

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.
6. Depending on your notification method selection, go to one of the following sections.
   - Email Notifications Entry
   - Pager Notifications Entry
   - SNMP Trap Notifications Entry
   - Serial Ports Alarm Notification

## Email Notifications Entry

When you go to Administration > Notifications, select “Email” from the pull-down menu, and click on “Add” or “Edit” button the following dialog box appears.


http://192.168.48.11 - Notifications Entry - Microsoft Internet Explorer
OK
Cancel
Alarm Trigger
To
From
Subject
Body
SMTP Server
Internet

SMTP Port

0

**Figure 11-3:** Expert > Administration > Notifications > Email > Add/Edit Dialog box

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

**Table 11-4:** Expert > Email Notifications Dialog Box Fields

| Field Name | Definition |
|---|---|
| **Alarm Trigger** | The trigger expression used to generate an alarm. |

| Field Name | Definition |
|---|---|
| **[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*

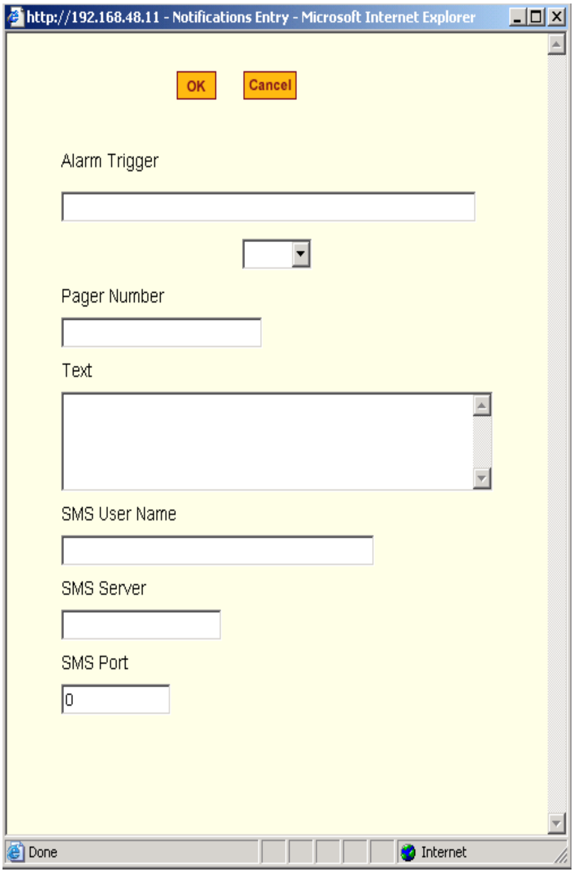
1. Go to Administration > Notifications in Expert mode, and select Email from the pull-down menu. If desired, enable “Notification Alarm for Data Buffering” for an alarm to sound when the trigger action occurs; and click either “Add” or “Edit”.

   The “Notifications Entry” dialog box appears.

2. Specify the event you want to trigger a notification in the “Alarm Trigger” field.
3. If you need to edit an existing notification select it from the drop-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 following dialog box appears.



http://192.168.48.11 - Notifications Entry - Microsoft Internet Explorer

Alarm Trigger

Pager Number

Text

SMS User Name

SMS Server

SMS Port

0

**Figure 11-4:** Expert > Administration > Notifications > Pager > Add/Edit Dialog box

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

**Table 11-5:** Expert > Pager Notifications Dialog Box

| 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”.

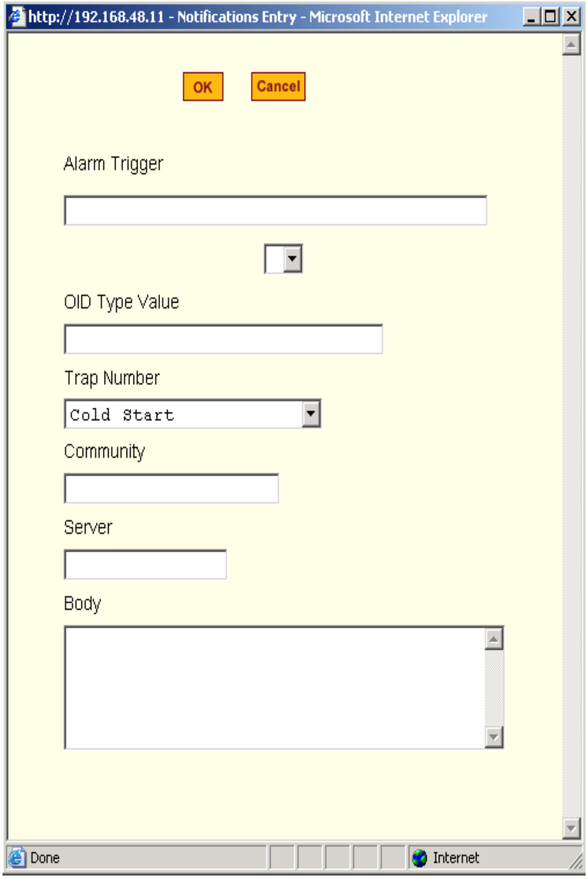
   The “Notifications Entry” dialog box appears.

2. Specify the event you want to trigger a notification in the “Alarm Trigger” field.
3. If you need to edit an existing notification select it from the drop-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, select “SNMP Trap” from the pull-down menu, and click on “Add” or “Edit” button the following dialog box appears.



Trap Number: Cold Start

**Figure 11-5:** Expert > Administration > Notifications > SNMP Trap > Add/ Edit Dialog box

SNMP traps are event notifications that are sent to a list of responsible parties that are 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). The trap definition varies with the SNMPv1 and SNMPv2, which defines the messaging format.

The following table describes the available fields in the SNMP trap notification entry dialog box.

**Table 11-6:** Expert > SNMP Trap Notifications Dialog Box

| 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. |
| **Trap Number** | The trap type defined in the Management Information Base (MIB). The choices are:<br>• Cold Start<br>• Warm Start<br>• Link Down<br>• Link Up<br>• Authentication Failure<br>• EGP Neighbor Loss<br>• 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 appears
2. Specify the event you want to trigger a notification in the “Alarm Trigger” field.
3. If you need to edit an existing notification select it from the drop-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, such that the system will generate an alarm in any of the following events.

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

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

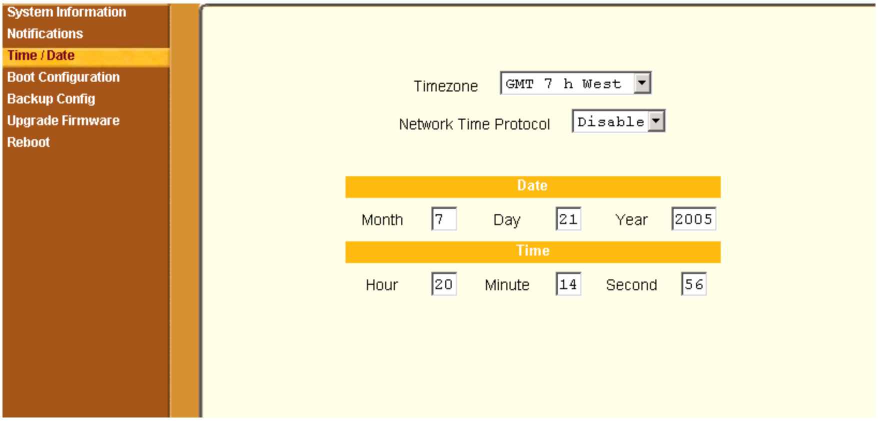
### ▼ *To Configure a Trigger for Serial Port Alarm Notification*

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, Email, Pager, or SNMP Trap. See “Notifications” on page 295.
7. Click “OK.”
8. Click “apply Changes.”

## Time/Date

Selecting Administration > Time/Date in Expert mode brings up the form shown in the following figure.



Timezone: GMT 7 h West

Network Time Protocol: Disable

Month: 7 Day: 21 Year: 2005

Hour: 20 Minute: 14 Second: 56

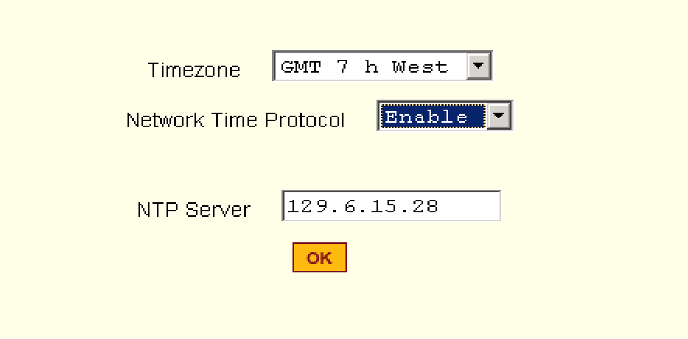
**Figure 11-6:** Expert > Administration > Time/Date

You can use the Time/Date form in Expert mode to set the CS’s time and date in one of the following two methods.

- Manual configuration by entering the time and date in the form
- Set up using the NTP server

  Enabling Network Time Protocol (NTP) synchronizes the CS’s system clock with an NTP server, which maintains the true time (the average of many high-accuracy clocks around the world).

If you enable the “Network Time Protocol”, the following form appears.



Timezone GMT 7 h West

Network Time Protocol Enable

NTP Server 129.6.15.28

**Figure 11-7:** Expert > Administration > Time/Date > NTP Enable

## Setting Time and Date with NTP

NTP (Network Time Protocol) is an Internet standard protocol which enables your system clock to be synchronized with the *true time*, defined as the average of many high-accuracy clocks around the world. NTP is disabled by default.

### ▼ *To Manually Set the Time and Date*

**1.** Go to Administration > Time/Date in Expert mode.

The Time/Date form appears.

**2.** Select a timezone from the “Timezone” pull-down list.

**3.** Select “Disable” from the “Network Time Protocol” menu.

**4.** Type the date and time in the fields provided.

**5.** Click “apply changes.”

### ▼ *To Configure Time and Date Using an NTP Server*

**1.** Go to Administration > Time/Date in Expert mode.

The Time/Date form appears.

**2.** Select a timezone from the “Timezone” pull-down list.

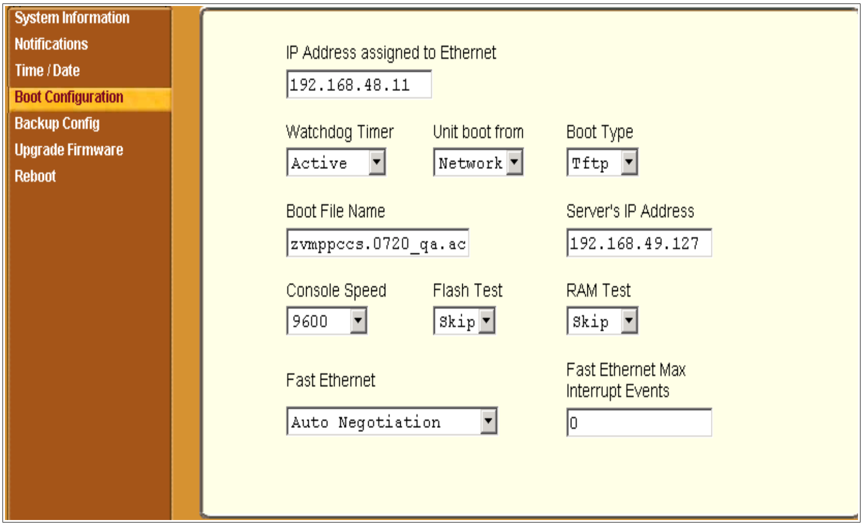
**3.** Select “Enable” from the “Network Time Protocol” pull-down menu.

The “NTP Server” field appears.

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

## Boot Configuration

Selecting Administration > Boot Configuration in Expert mode brings up the form shown in the following figure.



IP Address assigned to Ethernet: 192.168.48.11

Watchdog Timer: Active
Unit boot from: Network
Boot Type: Tftp

Boot File Name: zvmppccs.0720_qa.ac
Server's IP Address: 192.168.49.127

Console Speed: 9600
Flash Test: Skip
RAM Test: Skip

Fast Ethernet: Auto Negotiation
Fast Ethernet Max Interrupt Events: 0

**Figure 11-8:** Expert > Administration > Boot Configuration

Boot configuration defines the location from where CS loads the operating system. The CS can boot from its internal firmware or from the network. By default, CS boots from flash memory.

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 CS boot image file must be available on the TFTP or BOOTP server.
- CS 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 11-7:** Expert > Boot Configuration Form Fields

| Field Name | Definition |
|---|---|
| **IP Address assigned to Ethernet** | A fixed IP address or a DHCP assigned IP address to the CS unit. |
| **Watchdog Timer** | Whether the watchdog timer is active or Inactive. If the watchdog timer is active, the CS reboots if the software crashes. |
| **Unit boot from** | Specify whether to boot CS 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. |
| **Fast Ethernet** | The speed of the Ethernet connection. Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value)<br>100BaseT Half-Duplex<br>100BaseT Full-Duplex<br>10BaseT Half-Duplex<br>10BaseT Full-Duplex |

**Table 11-7:** Expert > Boot Configuration Form Fields

| Field Name | Definition |
|---|---|
| **Fast Ethernet Max. Interrupt Events** | The maximum number of packets that the CPU handles before an interrupt (0 is the default). |

### ▼ *To Configure CS Boot*

1. Go to Administration > Boot Configuration in Expert mode.

   The Boot Configuration form appears.

2. Enter the IP address of the CS in the “IP Address assigned to Ethernet” field.
3. Accept or change the selected option in the “Watchdog Timer” field.
4. Select to boot from “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, do 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 CS.

   **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.

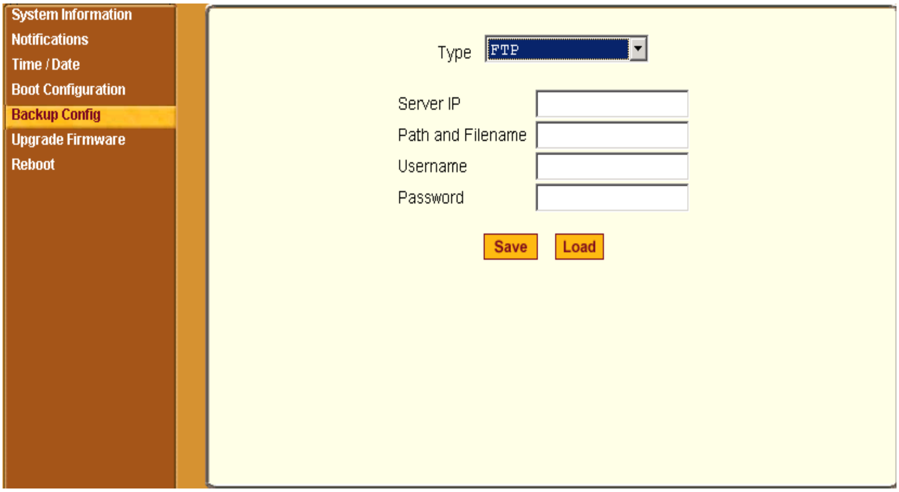
   **e.** Choose an Ethernet speed from the “Fast Ethernet” pull-down menu.

   **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 brings up the form shown in the following figure.



Type: FTP

Server IP:

Path and Filename:

Username:

Password:

**Figure 11-9:** Expert > Administration > Backup Config

The “Type” pull-down menu options on this form are “FTP” and “Storage Device.” The storage device can be either a compact flash or an IDE PCMCIA drive.

- Use an FTP server to save and retrieve your CS configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from CS by pinging the FTP server.
- Use a storage device such as a compact flash or an IDE PCMCIA drive to save your configuration.

The following table describes the available fields and buttons in the “Backup Config” form if “FTP” is selected.

**Table 11-8:** Expert > Backup Config Type FTP Form Fields and Buttons

| Field | Definition |
|---|---|
| Server IP | IP address of an FTP server on the same subnet as the CS. (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 want to save the file under another name. For example, to save the configuration file `zvmppcbb.0720.bb` in a directory called “/`upload`” on the FTP server, you would enter the following in the “Path and Filename” field:<br>/`upload/zvmppcbb.0720.bb` |
| Username and Password | Obtain the username 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. |

When “Storage Device” is selected from the “Type” pull-down menu , the following form appears.

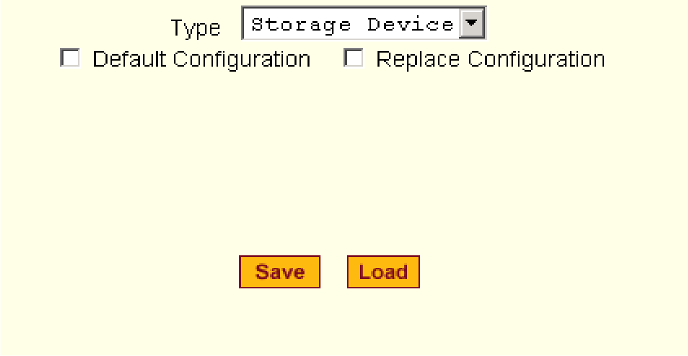


**Figure 11-10:** Expert > Administration > Backup Config > Storage Device

The following table describes the available fields when “Storage Device” is selected from the “Type” drop-down menu.

**Table 11-9:** Expert > Backup Config Type Storage Device Form

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

### ▼ *To Back Up or Restore the Configuration Files using an FTP Server*

1. Go to Administration > Backup Config in Expert mode.

   The Backup Config form appears.

2. Select “FTP” from the “Type” pull-down menu.
3. Enter the IP address of the FTP server in the “Server IP” field.
4. Enter the directory path on the FTP server where you have write permissions in the “Path and Filename” field. Enter the filename after the

directory path. For example, /`upload/zvmppccs.0720_qa.cs-k26.`

5. Enter the username and password provided by your system administrator for the FTP server.
6. To backup a copy of the current configuration files, press the “Save” button.
7. To download a previously saved copy of the configuration files, press the “Load” button.

### ▼ *To Back Up or Restore the Configuration Files using a Storage Device*

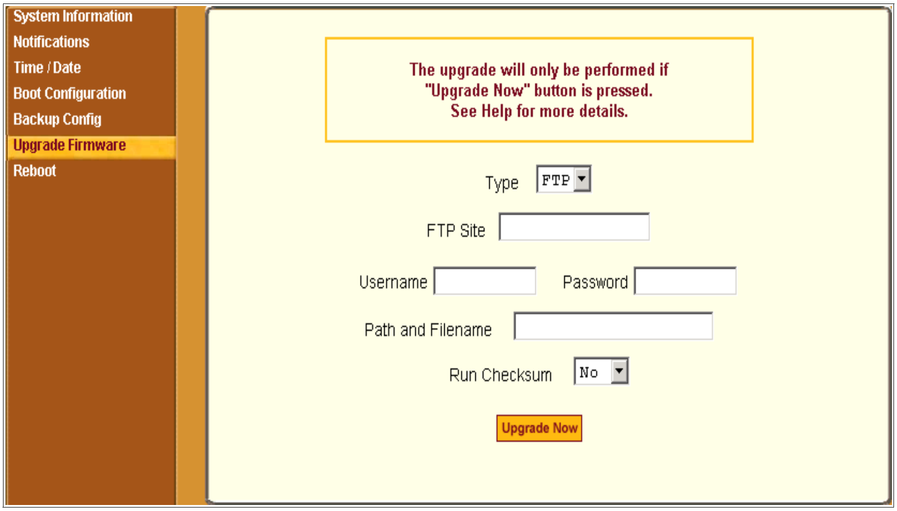
1. Go to Administration > Backup Config in Expert mode.

   The Backup Config form appears.

1. Select “Storage Device” from the “Type” pull-down menu.
2. To backup a copy of the current configuration files, select “Default Configuration” and press the “Save” button.
3. To restore a copy of the configuration files saved on the storage device without replacing the internal flash configuration, select “Default Configuration” and press the “Load” button.
4. Click “apply changes”
5. Reboot the system. See Administration > Reboot for details, if needed.
6. To replace the configuration saved on the storage device previously, select “Replace Configuration” and press the “Save” button.
7. To restore a copy of the configuration files saved on the storage device, and replace the internal flash configuration, select “Replace Configuration” and press the “Load” button.
8. Click “apply changes”
9. Reboot the system. See Administration > Reboot for details, if needed.

## Upgrade Firmware

Selecting Administration > Upgrade Firmware in Expert mode brings up the form shown in the following figure.



The upgrade will only be performed if
"Upgrade Now" button is pressed.
See Help for more details.

Type FTP

FTP Site

Username Password

Path and Filename

Run Checksum No

**Figure 11-11:** Expert > Administration > Upgrade Firmware

You can use this form to configure an automated upgrade of the CS’s firmware which includes the Kernel, applications, and configuration files. The firmware is upgradeable using an FTP server. You can upgrade the firmware directly through BLACK BOX®’ FTP site at ftp://ftp.blackbox.com/lan/Term-Servers/, or download the new firmware to a local FTP server and upgrade from there.

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

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

**Table 11-10:** Expert > Upgrade Firmware Form Fields

| Field/Menu Name | Definition |
|---|---|
| **Type** | FTP is the only supported type. |

| Field/Menu Name | Definition |
|---|---|
| **FTP Site** | The URL of the FTP server where the firmware is located. This can be a local FTP server, or the BLACK BOX®' FTP site at<br>ftp://ftp.blackbox.com/lan/Term-Servers/ |
| **Username** | Username recognized by the ftp server. |
| **Password** | Password associated with the username for the ftp server. |
| **Path and File Name** | The pathname of the firmware on the ftp server.<br>For example, `/blackbox/lan/Term-Servers/LS1016A_LS1032A/v230/zvmppcbb.v230` |
| **Run Checksum** | Runs the checksum program to verify the accuracy of the uploaded data. |

### ▼ *To Upgrade the CS's firmware*

This procedure is for upgrading the latest release of the CS's firmware. The upgrade installs the software on the flash memory.

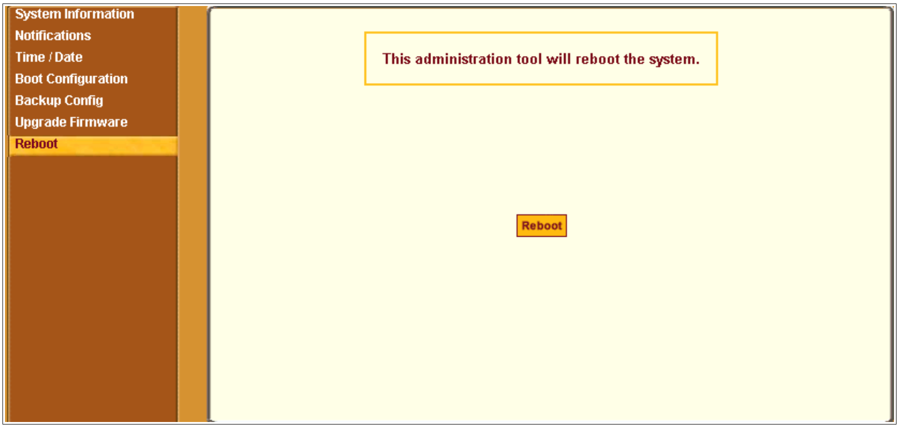
1. Go to Administration > Upgrade Firmware.

   The Upgrade Firmware form appears.

2. Choose FTP from the Type menu. (FTP is the only supported type).
3. Enter the URL of the ftp server in the “FTP Site” field.
4. Enter the username recognized by the ftp server in the “Username” field.
5. Enter the password associated with the username on the ftp server in the “Password” field.
6. Enter the pathname of the file on the ftp server in the “Path and Filename” field.
7. Click.the “Upgrade Now” button.
8. Click “cancel changes” if you need to restore the backed up configuration files.

## Reboot

Selecting Administration > Reboot in Expert mode brings up the form shown in the following figure.



This administration tool will reboot the system.

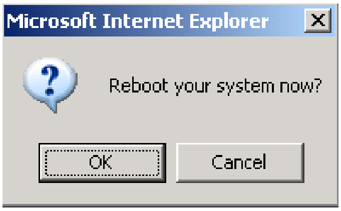
**Figure 11-12:** Expert > Administration > Reboot

Clicking the “Reboot” button reboots the CS.

### ▼ *To Reboot the CS*

1. Go to Administration > Reboot in Expert mode.
2. Click the “Reboot” button.

   A confirmation dialog box appears.

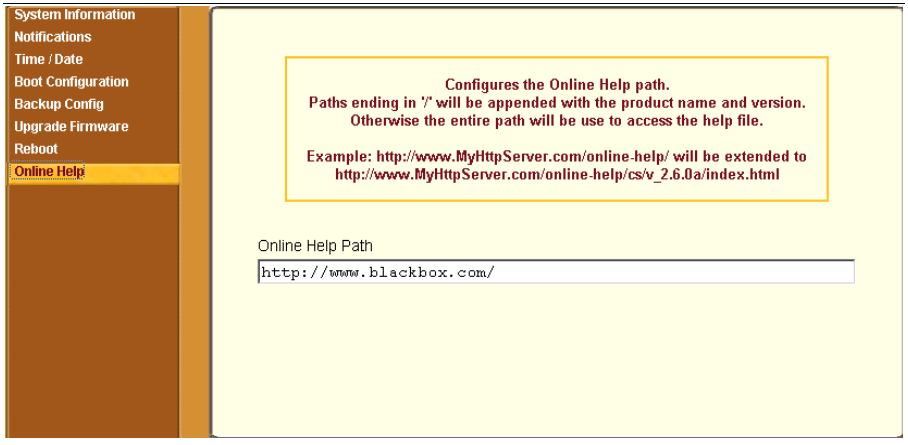


Reboot your system now?

3. Click OK.

# Online Help

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



Configures the Online Help path.
Paths ending in '/' will be appended with the product name and version.
Otherwise the entire path will be use to access the help file.

Example: http://www.MyHttpServer.com/online-help/ will be extended to
http://www.MyHttpServer.com/online-help/cs/v_2.6.0a/index.html

Online Help Path

`http://www.blackbox.com/`

**Figure 11-13:**Expert > Administration > Online Help

BLACK BOX® host the online-help on an FTP server accessible from the Internet. The path to the BLACK BOX® FTP server is configured by default on CS and is viewable in the "Online Help Path" field as http://www.blackbox.com/.

From any form in the Web Manager; pressing the "Help" button opens a new window and redirect its content to the configured path for the online help documentation.

The CS administrator can download the online help, and reconfigure the path to a local server where the online help can be stored. The CS firmware stores the new link in flash and accesses the online help files whenever the help button is clicked.

## ▼ To Configure the Online Help Path

1. Using an FTP tool navigate to the FTP site where the online help is stored and download the desired version of the online help files.
2. In the CS Web Manager navigate to Administration > Online Help in Expert mode.

3. In the “Online Help Path” field configure the path to the location of the documenation on your local server.

**Note:** When a directory path is ended with a “/”, the firmware appends the product name and verison. For example, http://www.myserver.com/online-help/ would be http://www.myserver.com/online-help/cs/<firmware version>

# Appendix A
# Technical Specifications

The following table lists the Advanced Console Server hardware specifications

| | |
|---|---|
| CPU | MPC855T (PowerPC Dual-CPU) |
| Memory | 128MB DIMM SDRAM / 16MB CompactFlash |
| Interfaces | 1 Ethernet 10/100BT on RJ45<br>1 RS232 Console on RJ45<br>RS232 Serial Ports on RJ45<br>PCMCIA slots supporting: Secondary Ethernet, Wireless networking, CDMA, GPRS, GSM, V.90 modems, ISDN. |
| Power | Internal 100-240VAC, 50/60 Hz†<br>Optional Dual entry, redundant power supplies†<br>† -48VDC option available |
| Operating Temperature | 50°F to 112°F (10°C to 44°C) |
| Storage Temperature | -40°F to 185°F (-40°C to 85°C) |
| Humidity | 5% to 90% non-condensating |
| Dimensions | CS1: 6.3 x 4.0 x 1.5 in (16 x 10 x 3.8 cm)<br>CS 4-48: 17 x 8.5 x 1.75 in (43.18 x 21.59 x 4.45 cm) |

| | |
|---|---|
| Certification | FCC Part 15, A<br>EN55022, A (CE)<br>EN55024<br>UL 1950<br>Solaris Ready™ |

# Appendix B
# Safety, Regulatory, and Compliance Information

The following Safety Information for Advanced Console Server are described in this appendix.

## Safety Guidelines for Rack-Mounting the CS

The following considerations should be taken into account when rack-mounting the Advanced Console Server.

### *Temperature*

The manufacturer's maximum recommended ambient temperature for the Advanced Console Server is 122 ºF (50 ºC).

Elevated Operating Ambient Temperature

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

### *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.

### *Mechanical Loading*

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

### *Circuit Overloading*

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

### *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.

## Safety Precautions for Operating the Advanced Console Server

Please read all the following safety guidelines to protect yourself and your Advanced Console Server.

**Caution:** Do not operate your Advanced Console Server with the cover removed.

**Caution:** To avoid shorting out your Advanced 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.

**Caution:** To help prevent electric shock, plug the Advanced 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 adapter 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.

**Caution:** To help protect the 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 CS and that they are not located where they can be stepped on or tripped over. Do not spill food or liquids on CS.

**Caution:** Do not push any objects through the openings of the Advanced Console Server. Doing so can cause fire or electric shock by shorting out interior components.

**Caution:** Keep your Advanced Console Server away from heat sources and do not block host’s cooling vents.

**Caution:** The Advanced Console Server DC-powered models are only intended to be installed in restricted access areas (Dedicated Equipment Rooms, Equipment Closets or the like) in accordance with Articles 110-18, 110-26 and 110-27 of the National Electrical Code, ANSI/NFPA 701, 1999 Edition. Use 18 AWG or

0.75 mm2 or above cable to connect the DC configured unit to the Centralized D.C. Power Systems. Install the required double-pole, single-throw, DC rated UL Listed circuit breaker between the power source and the Advanced Console Server DC version. Minimum Breaker Rating: 2A. Required conductor size: 18 AWG.

# Working inside the Advanced Console Server

Do not attempt to service the CS yourself, except when following instructions from BLACK BOX® Technical Support personnel. In the latter case, first take the following precautions:

1. Turn the CS 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.

# 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.

**Caution:** 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.

# FCC Warning Statement

The 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 & 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 Advanced Console Server Models

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

# Canadian DOC Notice

The 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’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.

# Aviso de Precaución S-Mark Argentina

Por favor de leer todos los avisos de precaución como medida preventiva para el operador y el Advanced Console Server.

**Caution:** No hacer funcionar el Advanced Console Server con la tapa abierta.

**Caution:** Para prevenir un corto circuito en el Advanced Console Server al desconectarlo de la red, primero desconectar el cable del equipo y luego el cable que conecta a la red. Para conectar el equipo a la red, primero conectar el cable a la red y luego al equipo.

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

**Caution:** No empuje ningún tipo de objeto en los compartimientos del Advanced Console Server. Hacer esto podría ocasionar un incendio o causar un corto circuito dentro del equipo.

**Caution:** Mantenga el Advanced Console Server fuera del alcancé de calentadores, y asegurarse de no tapar la ventilación del equipo.

**Caution:** El Advanced Console Server con alimentación de corriente directa (CD) solo debe ser instalado en áreas con restricción y de acuerdo a los artículos 110-18, 110-26, y 110-27 del National Electrical Code, ANSI/NFPA 701, Edición

1999. Para conectar la corriente directa (CD) al sistema, utilice cable de 0.75 mm (18 AWG). Instalar el interruptor corriente directa (CD) aprobado por UL entre la fuente de alimentación y el Advanced Console Server. El limite mínimo del interruptor deberá ser 2 amperes, con conductor de 0.75 mm (18 AWG).

# Trabajar dentro del Advanced Console Server

No intente dar servicio al Advanced Console Server, solo que este bajo la dirección de Soporte Técnico de BLACK BOX®. Si este es el caso, tome las siguientes precauciones:

Apague el Advanced Console Server. Asegurase que este tocando tierra antes de tocar cualquier otra cosa, que puede ser al tocar la parte trasera del equipo.

# Batería

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

# Appendix C
# Supported PCMCIA Cards

BLACK BOX® CS supports the PCMCIA cards listed in the table below. Note that some PCMCIA cards have been discontinued by their manufacturers and are marked accordingly.

**Table C-1:** Supported PCMCIA Cards

| Brand | Model |
|---|---|
| **10BT Ethernet** | |
| 3Com | Megahertz 10Mbps LAN Card Model 3CCE589ET (Discontinued) |
| **10/100BT Ethernet** | |
| Linksys[3] | EtherFast 10/100 PC Card Model PCM100 v2<br>FCC ID: MQ4FE1KMX |
| Linksys[3] | EtherFast 10/100 PC Card Model PCM100 v2<br>FCC ID: MQ4FE1KAX |
| Linksys[3] | EtherFast 10/100 PC Card Model PCM100 v2<br>FCC ID: MQ4FE1500A |
| Linksys[3] | EtherFast 10/100 PC Card Model PCM100 v2<br>FCC ID: MQ4FE1500C |
| Xircom | XE2000NA 10/100 Network PC Card Adaptor |

**Table C-1:** Supported PCMCIA Cards

| Brand | Model |
|---|---|
| **10/100BT Ethernet& V.90 (56k) Modem Combo** | |
| Xircom | XEM5600 10/100BT Ethernet and 56k V.90 modem combination (Discontinued) |
| **802.11b Wireless Ethernet** | |
| Proxim | ORiNOCO 11b Client PC Gold Card - 8410-WD (Discontinued) |
| Linksys | Instant Wireless Network PC Card - WPC11 Ver.3 |
| **Fiber Optic** | |
| Danpex | 1300C FX100BT SC |
| Danpex | 1300C FX100BT ST |
| **V.90 (56k) Modem** | |
| Xircom | XM5600 56K Modem PC Card |
| Zoom | Modem V.92 PC Card Plus Model 3075 |
| **ISDN** | |
| AVM | Fritz! Card v2.0 |
| Sedlbauer | Sedlbauer Speed Star II ISDN card |
| **CDMA** | |
| Growell | iCARD800 CDMA 1XRTT |
| **GSM/GPRS** | |
| Sierra Wireless[1] | AirCard 750 - GSM |
| Sierra Wireless[1] | AirCard 750 - GPRS |
| Novatel Wireless | Merlin G201 (Discontinued) |
| Option Wireless | Globe Trotter Universal Tri-band GSM/GPRS PC Radio Card |

**Table C-1:** Supported PCMCIA Cards

| Brand | Model |
|---|---|
| **Compact Flash**[2] | |
| SanDisk | 64MB CF Memory + Adapter (Discontinued) |
| St. Micro | 128MB CF Memory + Adapter |
| Kingston | 128MB CF Memory + Adapter |
| Kingston | 256MB CF Memory + Adapter |
| Kingston | 512MB CF Memory + Adapter |
| Other | Most other adapters and compact flash should also work but have not been verified by BLACK BOX® |
| **IDE Hard Disk** | |
| Toshiba | MK5002MPL 5GB |

[1] WARNING: Consult your local GSM service provider for coverage areas and support of this card prior to use with the BLACK BOX® CS.

[2] In order to load a Compact Flash card on the BLACK BOX® CS, use a PCMCIA Compact Flash adapter.

[3] Linksys 10/100BT Ethernet Cards - PCM100 v2 & v3 cards have specific FCC ID numbers on the PCMCIA card. The cards with specific FCC ID that are supported are listed above. Note the FCC ID before purchase.

# Glossary

**Authentication** The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.

**Basic In/Out System (BIOS)** Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.

**Baud Rate** The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.

**BogoMips** BogoMips (from "bogus" and MIPS). Unscientific measurement of CPU speed made by the Linux kernel when it boots to calibrate an internal busy-loop.

**Bonding (Linux)** Ability to detect communication failure transparently, and switch from one LAN connection to another. The Linux bonding driver has the ability to detect link failure and reroute network traffic around a failed link in a manner transparent to the application. It also has the ability (with certain network switches) to aggregate network traffic in all working links to achieve higher throughput. The bonding driver accomplishes this by enslaving all of the Ethernet ports in the bond to the same Ethernet MAC address, which ensures the proper routing of packets across the links.

**Boot** To start a computer so that it is ready to run programs for the user. A PC can be booted either by turning its power on, (Cold Boot) or by pressing Ctrl+Alt+Del (Warm Boot).

**Break Signal** A break signal is a logical zero on a TXD or RXD lines for a period of time, usually 250 to 500 milliseconds. Normally a receive or transmit data signal stays at the mark (on=1) voltage until the next character is transferred. A Break is sometimes used to reset the communications line or change the operating mode of communications hardware. Breaks at a serial console port are interpreted by Sun servers as a signal to suspend operation and switch to monitor mode.

**Checksum** A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.

**CIDR Notation** Classless Inter Domain Routing (CIDR) is a method for

assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C.
In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.9.205.22 /18 means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are 8, 16, 24, and 32.

**CLI** Command line interface. An interface that allows use of text commands. Through CLI, individual commands can be given to the computer one at a time using the keyboard. BLACK BOX® products run the Linux operating system. Administrators type "CLI" on the command line of the Linux shell. The BLACK BOX® CLI tool provides many commands and nested parameters in a format called the CLI parameter tree.

**Cluster** A cluster is a group of one or more computers working as a group to execute a certain task. From the user standpoint, a cluster acts as a large computer system.

**Console Access Server (CAS)**

A CAS has an Ethernet LAN connection and many RS-232 serial ports. It connects to the console ports of servers and networking equipment and allows convenient and secure access from a single location.

**Community** The community name acts as a password and is used to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.

**Console**

Terminal used to configure network devices at boot (start-up) time. Also used to refer to the keyboard, video and mouse user interface to a server.

**Console Port**

Most of the equipment in a data center (servers, routers, switches, UPS, PBX, etc.) has a serial console port for out-of-band management purposes.

**DHCP**

*Dynamic Host Configuration Protocol*. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

**DNS Server**

*Domain Name Server.* The computer you use to access the DNS to allow you to contact other computers on the Internet. The server keeps a database of host computers and their IP addresses.

**Domain Name**

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine. For example, the domain names: matisse.net, mail.matisse.net, workshop.matisse.net can all refer to the same machine, but each domain name can refer to no more than one machine. Usually, all of the machines on a given Network will have the same thing as the right-hand portion of their Domain Names (matisse.net in the examples above). It is also possible for a Domain Name to exist but not be connected to an actual machine. This is often done so that a group or business can have an Internet e-mail address without having to establish a real Internet site. In these cases, some real Internet machine must handle the mail on behalf of the listed Domain Name.

**Escape Sequence** A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.

An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one capability, and thus need some way to tell data from commands.

**Ethernet** A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.

**Flash** Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.

**Flow Control** A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.

**FTP** Short for *File Transfer Protocol*. The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring web pages from a server to a user's browser. FTP uses the Internet's TCP/IP protocols to enable data transfer.

**Hot-Swap** Ability to remove and add hardware to a computer system without powering off the system.

**ICMP** *Internet Control Message Protocol* is an Internet protocol sent in response to errors in TCP/IP messages. It is an error reporting protocol between a host and a gateway. ICMP uses Internet Protocol (IP) datagrams (or *packets*), but the messages are processed by the IP software and are not directly apparent to the application user.

**In-band Network Management** In a computer network, when the management data is accessed using the same network that carries the data, this is called “in-band management.”

**IP Address** A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals.

Each address has a network number, an optional sub network number and a host number. The first two numbers are used for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.

**IP packet filtering**

This is a set of facilities in network equipment that allows the filtering of data packets based on source/destination addresses, protocol, TCP port number and other parameters. Packet filtering is one of the main functions of a firewall.

**IPsec**

Short for *IP Security Protocol*, IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as for access and trustwothiness control. IPsec provides similar services as SSL, but it works on a network layer. Through IPsec you can create encrypted tunnels (VPN) or encrypt traffic between two hosts.

**ISDN**

A set of communications standards allowing a single wire or optical fibre to carry voice, digital network services and video. ISDN is intended to eventually replace the plain old telephone system.

**Kerberos**

Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. It works by assigning a unique key called a ticket to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

**LDAP**

*Lightweight Directory Access Protocol*. A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.

LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

**MAC**

*Medium Access Control*. Internationally unique hardware identification address that is assigned to the NIC (Network Interface Card) which interfaces the node to the LAN.

**Masquerading**

Where a system acts on behalf of other systems, such as when an ISP server accesses network services on behalf of a dial-up user.

**MTU**

Short for *Maximum Transmission Unit*, the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

Every network has a different MTU, which is set by the network administrator. On Windows, you can set the MTU of your machine. This defines the maximum size of the packets sent from your computer onto the network. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP, you might want to set your machine's MTU to 576 too. Most Ethernet networks, on the other hand, have an MTU of 1500.

**NEBS**

NEBS (Network Equipment Building Systems) Compliance means that equipment has been tested and proven to meet the NEBS requirements commonly adhered to by several telecommunications carriers. The requirements are in place to ensure that telecommunications equipment poses no risk or safety hazard to people, nearby equipment, or to the physical location where the equipment operates, and that equipment is reliable and dependable during both normal and abnormal conditions. Tests address heat release, surface temperature, fire resistance, electomagnetic compatibility, electrical safety, and manufacturing component characteristics, among other attributes.

**Network Mask**

A 32-bit number used to group IP addresses together or to indicate the range of IP addresses on a single IP network/ subnet/supernet. There is a group of addresses assigned to each network segment. For example, the mask 255.255.255.0 groups together 254 IP addresses. If we have, as another example, a sub-network 192.168.16.64 with mask 255.255.255.224, the addresses we may assign to computers on the sub-network are 192.168.16.65 to 192.168.16.94, with a broadcast address of 192.168.16.95.

A number used by software to separate the local subnet address from the rest of a given Internet protocol address

Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e.

255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.

**NFS** *Network File System* is a protocol suite developed and licensed by Sun Microsystems that allows different makes of computers running different operating systems to share files and disk storage. NFS is implemented using a connectionless protocol (UDP) in order to make it stateless.

**NTP** *Network Time Protocol*. A standard for synchronizing your system clock with the ``true time", defined as the average of many high-accuracy clocks around the world.

**Object Identifiers** (**OID**) The SNMP manager or the management application uses a well-defined naming syntax to specify the variables to the SNMP agent. Object names in this syntax are called Object Identifiers (Object IDs or OIDs). OIDs are series of numbers that uniquely identify an object to an SNMP agent. OIDs are arranged in a hierarchical, inverted tree structure.

The OID tree begins with the root and expands into branches. Each point in the OID tree is called a node and each node will have one or more branches, or will terminate with a leaf node. The format of OID is a sequence of numbers with dots in between.

There are two roots for Object Identifiers, namely iso and ccit. iso starts with.1 and ccit starts with.0. Most Object Identifiers start with.1.3.6.1, where 1=iso, 3=org, 6= dod,

1 = internet. The Internet sub-tree branches into mgmt and private.

To understand the concept of relative and absolute Object Identifiers, let us consider the AdventNet Object Identifier.1.3.6.1.4.1.2162. It specifies the path from the root of the tree. The root does not have a name or a number but the initial 1 in this OID is directly below root. This is called an absolute OID. However, a path to the variable may be specified relative to some node in the OID tree. For example, 2.1.1.7 specifies the sysContact object in the system group, relative to the Internet (.1.3.6.1) node in the OID tree. This is called a relative OID.

**Off-Line Data Buffering** This is a CAS feature that allows capture of console data even when there is no one connected to the port.

**OID** See **Object Identifier**.

**OOBI** Out-of-Band Infrastructure, an integrated systems approach to remote administration. Consists of components that provide secure, alternate path to connect to and manage an organization’s production network remotely.

**Packet** A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.

**Parity** In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.

The following lists the available parity parameters and their meanings:

**Odd -** Parity bit set so that there is an odd number of 1 bits

**Even -** Parity bit set so that there is an even number of 1 bits

**None -** Parity bit is ignored, value is indeterminate

**PCMCIA** *Personal Computer Memory Card International Association*. An organization consisting of some 500 companies that has developed a standard for small, credit card-sized devices, called PC Cards. Originally designed for adding memory to portable computers, the PCMCIA standard has been expanded several times and is now suitable for many types of devices including network cards (NICs).

The PCMCIA 2.1 Standard was published in 1993. As a result, PC users can be assured of standard attachments for any peripheral device that follows the standard.

**Port**

A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a port number may be seen as an address of an application within the computer.

**PPP**

*Point-to-Point Protocol*. This protocol is a way to connect your computer to the Internet over telephone lines. PPP is replacing an older protocol, SLIP, as it is more stable and has more error-checking features.

PPP has been a widely-used Internet standard for sending datagrams over a communications link. The PPP standard is described in RFC 1661 by the Point-to-Point Working Group of the Internet Engineering Task Force (IETF). PPP is commonly used when remote computers call an Internet service provider (ISP) or a corporate server that is configured to receive incoming calls.

**Profile**

Usage setup of the CS either as a Console Access Server (CAS), a Terminal Server, or a Remote Access Server.

**RADIUS**

*Remote Authentication Dial-In User Service* is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

**RISC** *Reduced Instruction Set Computer.* This describes a computer processor architecture that uses a reduced set of instructions (and achieves performance by executing those instructions very fast.) Most UNIX servers (Sun Sparc, HP, IBM RS6000, Compaq Alpha) were designed with a processor using a RISC architecture. The Intel ® x86 architecture.

**Root Access** *Root* is the term for a very highly privileged administrative user (particularly in Unix environments). When an ISP grants you root access, it means you will have full control of the server. With full control, you will be able to install any software and access any file on that server.

**Routing Table** The Routing Table defines which interface should transmit an IP packet based on destination IP information.

**RPC** Short for *Remote Procedure Call*. A type of protocol that allows a program on one computer to execute a program on a server. Using RPC, a system developer do not need to develop specific procedures for the server. The client program sends a message to the server with appropriate arguments and the server returns a message containing the results of the program executed.

**Secure Shell (SSH)** SSH has the same functionality as Telnet (see definition for **Telnet**), but adds security by encrypting data before sending it through the network.

**Server Farm** A collection of servers running in the same location (see **Cluster**).

**SMTP** Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.

**SNMP** Short for *Simple Network Management Protocol,* a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

(Source: Webopedia)

**SNMP Traps**

Notifications or Event Reports are occurrences of Events in a Managed system, sent to a list of managers configured to receive Events for that managed system. These Event Reports are called Traps in SNMP. The Traps provide the value of one or more instances of management information.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

The Trap Definition vary with the SNMP Version (which defines the messaging format), but the information contained in these are essentially identical. The major difference between the two message formats is in identifying the events.

**Stop Bit**

A bit which signals the end of a unit of transmission on a serial line.A stop bit may be transmitted after the end of each byte or character.

**Subnet Mask**

A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.

**SSH (Secure Shell)**

A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

**STTY**

Set the options for a terminal device interface.

This command prints information about your terminal settings. The information printed is the same as if you had typed stty while interacting with a shell.

The stty utility sets or reports on terminal I/O characteristics for the device that is its standard input. Without options or operands specified, it reports the settings of certain characteristics, usually those that differ from implementation-dependent defaults. Otherwise, it modifies the terminal state according to the specified operands.

**TACACS** *Terminal Access Controller Access Control System.*

Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

**TACACS+** *Terminal Access Controller Access Control System Plus*. A protocol that provides remote access authentication, authorization, and related accounting and logging services commonly used in UNIX networks.

**TCP Keep-Alive Interval** The time interval between the periodic polling of all inactive TCP/IP connections, checking that the client processes really are still there. After a certain period of inactivity on an established connection, the server's TCP/IP software will begin to send test packets to the client, which must be acknowledged. After a preset number of 'probe' packets has been ignored by the client, the server assumes the worst and the connection is closed.

The keep-alive timer provides the capability to know if the client's host has either crashed and is down or crashed and rebooted.

**Telnet** A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console

**Terminal Server** A terminal server has one Ethernet LAN port and many

RS-232 serial ports. It is used to connect many terminals to the network. Because they have the same physical interfaces, terminal servers are sometimes used as console access servers.

**TTY**

1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.

**UDP**

*User Datagram Protocol* uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.

**U Rack Height Unit**

A standard computer rack has an internal width of 17 inches. Rack space on a standard rack is measured in units of height (U). One U is 1.75 inches. A device that has a height of 3.5 inches takes 2U of rack space.

**VPN**

*Virtual Private Networking* allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.

**Watchdog Timer**

A watchdog timer (WDT) is a device or electronic card that performs a specific operation after a certain period of time if something goes wrong with an electronic system and the system does not recover on its own.

A common problem is for a machine or operating system to lock up if two parts or programs conflict, or, in an operating system, if memory management trouble occurs. In some cases, the system will eventually recover on its own, but this may take an unknown and perhaps extended length of time.

A watchdog timer can be programmed to perform a warm boot (restarting the system) after a certain number of seconds during which a program or computer fails to respond

following the most recent mouse click or keyboard action.

The timer can also be used for other purposes, for example, to actuate the refresh (or reload) button in a Web browser if a Web site does not fully load after a certain length of time following the entry of a Uniform Resource Locator (URL).

# Index