# Table of Contents

## CPS and Power Management
- Configuring Power Management .......................... 18
- Configuring Ports for Power Management by Authorized Users ... 20
- Configuring Ports for Power Management Using the CLI ..... 20

## Options for Managing Power
- Power Management Through the Web Manager ............. 21
- Power Management from the CPS Command Line ............ 21

## Chapter 2: Installation and Configuration

### Shipping Box Contents ........................................ 23
### Important Pre-installation Requirements .................. 25
- Java Plug-In Requirement for Serial Port Access ........... 25

### Basic Installation Procedures .............................. 27
- Installing the CPS ........................................... 28
- Making an Ethernet Connection ............................. 28
- Connecting Servers and Other Devices to CPS .......... 29
- Making a Direct Connection to Configure the Network Parameters ........................................ 29
- Applying Power to the CPS and the Connected Devices ... 30
- Configuring the Network Parameters ....................... 31
  - Performing Basic Network Configuration Using the wiz Command 31
  - Selecting A Security Profile Using the Web Manager .... 34
- Adding Users and Configuring Ports Using the Web Manager ................................................... 35
  - Enabling Ports and Assigning Users .................... 35

### Other Methods of Accessing the Web Manager .......... 36
- Using a Dynamic IP Address to Access the Web Manager ... 36
- Using the Default IP Address to Access the Web Manager ... 36

### Installing PCMCIA Cards .................................. 37

### Connecting APC Switched Rack PDUs (rPDUs) ........... 38

## Chapter 3: Web Manager for Regular Users

### Using the Web Management Interface (WMI) ............. 39
### Features of Regular User Forms ............................ 41

### Connect ..................................................... 42
- Connect to CPS ............................................. 42
- Connect to Serial Ports .................................... 44

### Port Access Requirements ................................ 44
Chapter 4: Web Manager for Administrators 53

APC Web Manager ......................................................... 53
  Prerequisites for Using the Web Manager ....................... 54
Common Tasks for CPS Administrators .............................. 54
Common Features of Administrator Forms ............................ 56
  Buttons and CPS Information ......................................... 56
Logging Into the Web Manager ........................................ 58
Overview of Administrative Modes .................................... 61
  Wizard Mode ............................................................ 61
  Expert Mode ............................................................ 62

Chapter 5: Configuring CPS in Wizard Mode 64

Step 1: Security Profile ................................................ 64
  Serial Port Settings and Security Profiles ........................ 66
  Selecting or Configuring a Security Profile ....................... 68
Step 2: Network Settings ............................................... 71
  Configuring the Network Settings .................................. 73
Step 3: Port Profile .................................................... 74
  Setting Parameters for All Serial Ports ......................... 76
Step 4: Access .......................................................... 77
  Adding a User ........................................................ 79
  Deleting a User ....................................................... 80
  Changing a Password ................................................ 81
Step 5: Data Buffering .................................................. 81
  Configuring Data Buffering .......................................... 85
Step 6: System Log ...................................................... 86
  Adding a Syslog Server .............................................. 87
  Deleting a Syslog Server ............................................ 88
Chapter 6: Configuring the CPS in Expert Mode 89

Overview of Menus and Forms ................................................. 90
Mapping of the Expert Mode Menus and Forms ...................... 91
Description of Forms in Expert Mode ...................................... 92

Chapter 7: Applications Menu and Form 97

Applications ........................................................................... 98
Connect .................................................................................. 98
  Connecting to the CPS ......................................................... 101
  Connecting to a Device Through a Serial Port ....................... 101
rPDU Power Mgmt. ................................................................. 101
  Outlets Manager ............................................................... 102
  View rPDUs Info ............................................................... 105
    Users Manager .............................................................. 107
    Configuration ............................................................... 109
rPDU Multi-Outlet Ctrl. ............................................................. 110
  Prerequisites for Multi-Outlet Control ................................. 112
  Power Management Icons .................................................. 112
IPMI Power Management ....................................................... 114
Terminal Profile Menu ........................................................... 121

Chapter 8: Network Menu and Forms 124

Network .................................................................................... 125
  Host Settings ....................................................................... 125
  Configuring Host Settings [Expert] ....................................... 128
  Syslog .................................................................................. 130
  Configuring Syslogging for Serial Ports and Specifying Message Filtering .............................................. 131
PCMCIA Management ............................................................... 132
  Configuring a Modem PCMCIA Card ................................. 135
  Configuring an ISDN PCMCIA Card ................................. 137
  Configuring a GSM PCMCIA Card .................................... 139
  Configuring an Ethernet PCMCIA Card ............................ 142
  Configuring a PCMCIA Compact Flash Card or a PCMCIA Hard Disk Drive .............................................. 143
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Wireless LAN PCMCIA Card</td>
<td>144</td>
</tr>
<tr>
<td>Configuring a CDMA PCMCIA Card</td>
<td>146</td>
</tr>
<tr>
<td>Ejecting a PCMCIA Card</td>
<td>148</td>
</tr>
<tr>
<td>VPN Connections</td>
<td>149</td>
</tr>
<tr>
<td>SNMP</td>
<td>153</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>158</td>
</tr>
<tr>
<td>Host Table</td>
<td>172</td>
</tr>
<tr>
<td>Static Routes</td>
<td>173</td>
</tr>
<tr>
<td>Chapter 9: Security Menu and Forms</td>
<td>177</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>177</td>
</tr>
<tr>
<td>Adding a User</td>
<td>179</td>
</tr>
<tr>
<td>Adding a Group</td>
<td>180</td>
</tr>
<tr>
<td>Active Ports Sessions</td>
<td>182</td>
</tr>
<tr>
<td>Authentication</td>
<td>184</td>
</tr>
<tr>
<td>Configuring Authentication for CPS Logins</td>
<td>185</td>
</tr>
<tr>
<td>Configuring Authentication Servers for Logins to CPS and Connected Devices</td>
<td>185</td>
</tr>
<tr>
<td>User Authorization on TACACS+</td>
<td>189</td>
</tr>
<tr>
<td>Security Profiles</td>
<td>194</td>
</tr>
<tr>
<td>Serial Port Settings and Security Profiles</td>
<td>197</td>
</tr>
<tr>
<td>To Select or Configure a Security Profile</td>
<td>199</td>
</tr>
<tr>
<td>Chapter 10: Ports Menu and Forms</td>
<td>203</td>
</tr>
<tr>
<td>Physical Ports</td>
<td>205</td>
</tr>
<tr>
<td>General</td>
<td>208</td>
</tr>
<tr>
<td>Connection Profiles</td>
<td>208</td>
</tr>
<tr>
<td>Console Access Server (CAS) Profile Connection Protocols</td>
<td>209</td>
</tr>
<tr>
<td>Terminal Server (TS) Profile Connection Protocols</td>
<td>209</td>
</tr>
<tr>
<td>Bidirectional Telnet Protocol</td>
<td>211</td>
</tr>
<tr>
<td>Modem and Power Management Connection Protocols</td>
<td>212</td>
</tr>
<tr>
<td>Access</td>
<td>224</td>
</tr>
<tr>
<td>Authentication Methods and Fallback Mechanism</td>
<td>226</td>
</tr>
<tr>
<td>Data Buffering</td>
<td>228</td>
</tr>
<tr>
<td>Multi User</td>
<td>232</td>
</tr>
<tr>
<td>Power Management</td>
<td>235</td>
</tr>
<tr>
<td>Other</td>
<td>240</td>
</tr>
<tr>
<td>Virtual Ports</td>
<td>244</td>
</tr>
<tr>
<td>Ports Status</td>
<td>250</td>
</tr>
<tr>
<td>Ports Statistics</td>
<td>251</td>
</tr>
</tbody>
</table>
Chapter 11: Administration Menu and Forms

System Information ................................................. 255
Notifications .......................................................... 257
  Email Notifications Entry ........................................ 259
  Pager Notifications Entry ....................................... 261
  SNMP Trap Notifications Entry ................................ 263
  Serial Ports Alarm Notification ................................. 265
Time/Date ............................................................... 266
  Setting Time and Date with NTP ............................... 267
Boot Configuration .................................................. 268
Backup Configuration .............................................. 271
Upgrade Firmware .................................................. 274
Reboot ................................................................. 277
Online Help ........................................................... 278

Appendix A: Technical Specifications 279
Appendix B: Safety, Regulatory, and Compliance Information 280
Glossary 286
Index 301
Before You Begin

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

Audience

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

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

Document Organization

The document contains the following chapters:

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

Chapter 2: Installation and Configuration—A list of tasks for installing and configuring the APC Console Port Server and connecting devices, with pointers to the needed background information and procedures.

Chapter 3: Web Manager for Regular Users—Describes how authorized users use the Web Manager to access devices that are connected to ports on the CPS.

Chapter 4: Web Manager for Administrators—Explains how the CPS administrator uses the Web Manager to add and delete users, define port access, and perform other common administration tasks.

Chapter 5: Configuring CPS in Wizard Mode—Describes the 6-step procedure to configure the APC Console Port 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.

Chapter 6: Configuring the CPS 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.

Chapter 7: Applications Menu and Form—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.

Chapter 8: Network Menu and 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.

Chapter 9: Security Menu and 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.

Chapter 10: Ports Menu and 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.

Chapter 11: Administration Menu and 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.

Appendix A: Technical Specifications—Provides hardware specifications.

Appendix B: Safety, Regulatory, and Compliance Information—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

Additional documents regarding the APC CPS are on the Documentation CD shipped with the product and are also available at: http://www.apc.com/search by searching under the product’s name.

- APC Console Port Server Command Reference Guide
- APC Console Port Server Installation, Administration, and User’s Guide

Updated versions of the documentation will be posted on the downloads section of the APC web site in the “APC Console Port Server” section when APC releases new versions of the software.

A hard-copy version of this document can be ordered through your APC sales representative.

Typographic and Other Conventions

The following table describes the typographic conventions used in APC manuals.

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links</td>
<td>Hypertext links or URLs</td>
<td>See <a href="http://www.apc.com">http://www.apc.com</a>.</td>
</tr>
<tr>
<td>Emphasis</td>
<td>• Titles</td>
<td>See the APC Console Port Server</td>
</tr>
<tr>
<td></td>
<td>• Emphasized words or terms</td>
<td>Quick Start Guide.</td>
</tr>
<tr>
<td></td>
<td>• New words or terms</td>
<td></td>
</tr>
<tr>
<td>Filename or</td>
<td>Names of commands, files, and</td>
<td>Edit the pslave.conf file.</td>
</tr>
<tr>
<td>Command</td>
<td>directories; on-screen computer output.</td>
<td></td>
</tr>
<tr>
<td>User type</td>
<td>What you type in an example,</td>
<td>[root] ifconfig eth0</td>
</tr>
<tr>
<td></td>
<td>compared to what the computer displays</td>
<td></td>
</tr>
</tbody>
</table>
The following table describes other terms and conventions.

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

<table>
<thead>
<tr>
<th>Term or Convention</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot keys</td>
<td>When hot keys are shown with a plus (+) between two or three keys means that they must be pressed at the same time.</td>
<td>Pressing Ctrl+p brings up the IPMI power management.</td>
</tr>
<tr>
<td>Navigation shortcuts</td>
<td>Shortcuts use the “greater than” symbol (&gt;) to indicate how to navigate to Web Manager forms.</td>
<td>Select Port&gt;Physical Ports&gt;Modify Selected Ports&gt;Power Management</td>
</tr>
</tbody>
</table>

**Additional Resources**

APC offers technical training and firmware upgrades.

For all APC related online services including documentation, training, and technical support, visit the APC Web site, [www.apc.com](http://www.apc.com), and enter the product model or product family into the search engine to access more information.

For firmware upgrades for your CPS, visit the APC Software/Firmware Downloads Web page, [www.apc.com/tools/download/](http://www.apc.com/tools/download/) and enter the product model or product family into the search engine.
Chapter 1: Introduction

This chapter introduces the APC Console Port Server family of 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
APC Console Port Server Models and Configurations
Connectors on the APC Console Port Server
Methods of Accessing CPS and Connected Devices
Web Manager
Prerequisites for Using the Web Manager
Types of Users
Security Features
Authentication
VPN
Packet Filtering
SNMP
Notifications, Alarms, and Data Buffering
Administering Users of Connected Devices
Power Management
Overview

Each product in the APC Console Port Server family is a 1U device that serves as a single access point for using and administering servers and other devices. The following figures show the front of the CPS.

Figure 1-1: CPS Models AP9301 and AP9302 Front Panel

Figure 1-2: CPS Model AP9303 Front Panel

The following figure shows the back of an AP9302 with its Serial, Ethernet, and Console ports.

Figure 1-3: CPS 16-port Back with Connectors
Product Models and Configurations

Table 1-1: Model Numbers and Configuration Options

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Serial Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP9301</td>
<td>8</td>
</tr>
<tr>
<td>AP9302</td>
<td>16</td>
</tr>
<tr>
<td>AP9303</td>
<td>32</td>
</tr>
</tbody>
</table>

See Appendix A for hardware specifications.

The following figures illustrate the APC Console Port Server family of console servers.

**Figure 1-4:** 8-port Console Port Server (AP9301)

**Figure 1-5:** 16-port Console Port Server (AP9302)

**Figure 1-6:** 32-port Console Port Server (AP9303)
Connectors on the CPS

The following figure depicts the connectors on the back of a CPS AP9301.

![CPS Connectors](image)

**Figure 1-7:** CPS Connectors (AP9301 8-port unit shown)

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

**Accessing CPS and Connected Devices**

You can access CPS 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 CPS’s serial ports.
- By connecting a computer running a terminal emulation program, an CPS administrator can log into the CPS box and enter commands in the CPS 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” can either 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.
Web Manager

CPS 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 CPS.

The CPS 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 the Web Manager using one of the following methods:

- Through the IP Network.
- Through a dial-in or callback connection with one of the following devices:
  - 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 CPS so the Web Manager can be launched over the network.
  
  See “Performing Basic Network Configuration Using the wiz Command” on page 31.

- The IP address of the CPS must be known.

  When DHCP is enabled, a leased IP address is assigned to the CPS. The leased IP address may change every time the CPS reboots. You must know the dynamically-assigned IP address to access the Web Manager through the browser. Determine the dynamically-assigned IP address in one of the following ways:

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

CPS supports the following user account types:

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

  Note: For secure access to the connected servers or devices, change the default password “apc” before setting up the CPS.

• 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 for which they are authorized. Regular users have limited access to the Web Manager features.

Security

The APC Console Port Server includes a set of security profiles that consists of predefined parameters to control access to CPS 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.

The following table shows the available security profiles and the active services under each profile. See “Security Profiles” on page 194 for detailed information and procedures.

Table 1-2: Enabled services to access the CPS under each security profile.

<table>
<thead>
<tr>
<th>Access to CPS</th>
<th>Secure</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSHv1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Table 1-3: Enabled services to access the serial ports under each profile.

<table>
<thead>
<tr>
<th>Access to Serial Ports</th>
<th>Secure</th>
<th>Moderate</th>
<th>Open</th>
<th>Default(^1)</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console (Telnet)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Console (SSH)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Console (Raw)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Serial Port Authentication</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bidirect (Dynamic Mode Support)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

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

Table 1-4: Enabled protocols for each profile shown with a check mark.

<table>
<thead>
<tr>
<th>Other Services</th>
<th>Secure</th>
<th>Moderate</th>
<th>Open</th>
<th>Default(^1)</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPC</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1—The Default security profile parameters are the same as Moderate profile parameters.
Authentication

The CPS 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; the CPS follows an alternate defined rule when the authentication server is down or does not authenticate the user.

The following table lists the supported authentication methods.

Table 1-5: CPS Supported Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No authentication.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Authentication is performed using a Kerberos server.</td>
</tr>
<tr>
<td>Kerberos/Local</td>
<td>Kerberos authentication is tried first, switching to Local authentication if unsuccessful.</td>
</tr>
<tr>
<td>KerberosDownLocal</td>
<td>Local authentication is performed only when the Kerberos server is down.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Authentication is performed against an LDAP database using an LDAP server.</td>
</tr>
<tr>
<td>LDAP/Local</td>
<td>LDAP authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>LDAPDownLocal</td>
<td>Local authentication is performed only when the LDAP server is down.</td>
</tr>
<tr>
<td>Local</td>
<td>Authentication is performed locally. For example using the /etc/passwd file.</td>
</tr>
</tbody>
</table>

1-The Default security profile parameters are the same as Moderate profile parameters.
### Authentication Type Definition

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local/Radius</td>
<td>Authentication is performed locally first, switching to Radius if unsuccessful.</td>
</tr>
<tr>
<td>Local/TACACS+</td>
<td>Authentication is performed locally first, switching to TACACS+ if unsuccessful.</td>
</tr>
<tr>
<td>Local/NIS</td>
<td>Authentication is performed locally first, switching to NIS if unsuccessful.</td>
</tr>
<tr>
<td>NIS</td>
<td>NIS authentication is performed.</td>
</tr>
<tr>
<td>NIS/Local</td>
<td>NIS authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>NISDownLocal</td>
<td>Local authentication is performed only when the NIS server is down.</td>
</tr>
<tr>
<td>Radius</td>
<td>Authentication is performed using a Radius authentication server.</td>
</tr>
<tr>
<td>Radius/Local</td>
<td>Radius authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>RadiusDownLocal</td>
<td>Local authentication is performed only when the Radius server is down.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Authentication is performed using a TACACS+ authentication server.</td>
</tr>
<tr>
<td>TACACS+/Local</td>
<td>TACACS+ authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>TACACS+DownLocal</td>
<td>Local authentication is tried only when the TACACS+ server is down.</td>
</tr>
</tbody>
</table>

**VPN**

The CPS administrator can set up VPN connections to establish encrypted communications between the CPS and a host on a remote network. The encryption creates a security tunnel for dedicated communications.
You can use the VPN features of the CPS to create the following types of connections:

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

To set up a security gateway, 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 or to configure a VPN connection, see “VPN Connections” on page 149.

Packet Filtering on CPS

The CPS 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 CPS filter table contains a number of built-in chains. The CPS 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 CPS.
- 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, the default action for that chain is applied.

Administrators can specify packet filtering by completing the following tasks:

- 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>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP and Mask</td>
<td>If you specify a source IP address, incoming packets are filtered for the specified IP address. If you specify a destination IP address, outgoing packets are filtered for the specified IP address. 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.</td>
</tr>
<tr>
<td>Destination IP and Mask</td>
<td></td>
</tr>
</tbody>
</table>
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, packets that arrive from a source IP address other than the one specified are dropped.

**Numeric Protocol Options**

If you select Numeric as the protocol when specifying a rule, you must specify the number.

**TCP Protocol Options**

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

<table>
<thead>
<tr>
<th>Field/Menu Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Port</strong></td>
<td>Specify a source or destination port number for filtering. You can also</td>
</tr>
<tr>
<td>- OR -</td>
<td>specify a range, so that TCP packets are filtered for any port number</td>
</tr>
<tr>
<td><strong>Destination Port</strong></td>
<td>within the range.</td>
</tr>
</tbody>
</table>
When you select UDP as a protocol when specifying a rule, you can select the UDP options defined in the following table.

**Table 1-6: UDP Protocol Packet Filtering Options**

<table>
<thead>
<tr>
<th>Field/Menu Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Port</strong></td>
<td>Specify a source or destination port number for filtering. 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.</td>
</tr>
</tbody>
</table>

**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.
Options for the “LOG” Target:

Table 1-7: LOG Target Action Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Level</strong></td>
<td>emerg, alert, crit, err, warning, notice, info, debug</td>
</tr>
</tbody>
</table>

- **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.

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

To define packet filtering using the Web Manager, see the following pages:

- To Add a Chain: Page 170
- To Edit a Chain: Page 170
- To Add a Rule: Page 171
- To Edit a Rule: Page 172
SNMP

The CPS administrator can activate the Simple Network Management Protocol (SNMP) agent that resides on the CPS. The SNMP agent sends notifications about significant events or traps to an SNMP management application.

The CPS SNMP agent supports SNMPv1/v2 and SNMPv3.

To configure SNMP, see “To Configure SNMP” on page 156. To configure one or more serial ports to send SNMP traps, see “SNMP Trap Notifications Entry” on page 263.

Notifications, Alarms, and Data Buffering

The CPS administrator can set up logging, notifications, and alarms to alert administrators about problems. System generated messages on CPS 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 CPS’s flash memory, or remotely (either on an NFS server or a syslog server).

Syslog Servers

Messages about the CPS 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, ensure that the syslog server is pre-configured with a public IP address, and that it is accessible from CPS. 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 CPS.
  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 (Local0 to Local7). The administrator of the syslog server can assign the facility numbers to different devices, or to groups of devices at different locations.

An Example of Using Facility Numbers

The syslog system administrator sets up a server called “syslogger” to handle log messages from two CPS boxes. One CPS is located in St. Louis, Missouri, and the other CPS is in West Kingston, Rhode Island. The syslog server’s administrator wants to aggregate messages from the St. Louis CPS into the local1 facility, and to aggregate messages from West Kingston CPS 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/stl-config file and the messages from the local2 facility to the /var/log/wk-config file. If you were in Chicago 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

The CPS administrator can perform the following tasks to enable access to connected servers, rPDUs, or other devices.

Planning Access to Connected Devices

Perform the following tasks to minimize issues that may arise during software configuration.

• 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 rPDUs and the users who need to access them.
Configuring Access to Connected Devices

While installing the CPS, connect the servers, devices, and any rPDUs to the serial ports. During software configuration, perform the following tasks:

**Table 1-8:** Tasks for Configuring Access to Connected Devices

<table>
<thead>
<tr>
<th>Task</th>
<th>Where documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a serial port connection protocol for a console connection</td>
<td>Page 212</td>
</tr>
<tr>
<td>Configure user access to serial ports</td>
<td>Page 225</td>
</tr>
<tr>
<td>Configure a serial port for rPDU or IPMI power management</td>
<td>Page 238</td>
</tr>
<tr>
<td>Configure a user for rPDU power management</td>
<td>Page 239</td>
</tr>
</tbody>
</table>

**CPS and Power Management**

CPS enables users with power management permissions to power off, power on, and reboot devices. The CPS offers the following power management options:

- Remote power management of servers that have IPMI controllers. The CPS'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 CPS because their IPMI controllers respond to out-of-band IPMI commands. Authorized users can also perform IPMI power management of serially-connected devices. The CPS uses IPMI V1.5.

- Remote power management of devices that are plugged into an rPDU that is connected to CPS
• The rack power distribution unit (rPDU) can be connected to any serial port.
• The diagram below shows a typical setup of the CPS and an rPDU.

Figure 1-8: rPDU Integration With CPS
Configuring Power Management

Administrators can perform power management through the Web Manager, assign power management permissions to users, configure IPMI devices, and configure ports for power management. The following table lists the tasks for power management and where they are described.

**Table 1-9: Tasks for Configuring Power Management**

<table>
<thead>
<tr>
<th>Task</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure users to manage power on rPDUs</td>
<td>“To Configure a User for rPDU Power Management While Connected To a Serial Port” on page 239</td>
</tr>
<tr>
<td>Identify servers for IPMI power management</td>
<td>“To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management” on page 117</td>
</tr>
<tr>
<td>Configure ports for power management by authorized users</td>
<td>“To Configure a Serial Port for rPDU or IPMI Power Management” on page 118</td>
</tr>
</tbody>
</table>

**Configuring Ports for Power Management by Authorized Users**

Administrators of connected devices who have power management permissions can manage power while connected by using a “hot key” to bring up a power management screen.

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

**Configuring Ports for Power Management Using the CLI**

CPS administrators can use the CLI command with the `config ipmi` options to manage power on IPMI devices while logged into the CPS. The `ipmitool` command is documented in the *APC Console Port Server Command Reference Guide*. 

---

**CPS and Power Management**

**20 APC Console Port Server Installation, Administration, and User’s Guide**
Options for Managing Power

Authorized users can perform power management through CPS in three ways:

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

An authorized user with administrative privileges can perform rPDU and IPMI power management. A Regular User with permissions to the connected devices can perform rPDU power management.

Power Management Through the Web Manager

Users with power management permissions can perform power management through the two options available on the Web Manager.

Table 1-10: Power Management Options in the Web Manager

<table>
<thead>
<tr>
<th>Form Name</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>rPDU Power Mgmt</td>
<td>• “rPDU Power Mgmt.” on page 101</td>
</tr>
<tr>
<td></td>
<td>• “To View Status, Lock, Unlock, Rename, or Cycle Power Outlets” on page 104</td>
</tr>
<tr>
<td>IPMI Power Mgmt</td>
<td>• “IPMI Power Management” on page 114</td>
</tr>
<tr>
<td></td>
<td>• “To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management” on page 117</td>
</tr>
<tr>
<td></td>
<td>• “To Manage Power on an IPMI Device” on page 118</td>
</tr>
</tbody>
</table>

Power Management from the CPS Command Line

CPS administrators can use the ipmitool command to manage power on IPMI devices while logged into the CPS. The ipmitool command is documented in the *APC Console Port Server Command Reference Guide*. 

introduction
Chapter 2: Installation and Configuration

This chapter covers the topics listed in the following table.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shipping Box Contents</td>
<td>23</td>
</tr>
<tr>
<td>Important Pre-Installation Requirements</td>
<td>25</td>
</tr>
<tr>
<td>Basic Installation Procedures</td>
<td>27</td>
</tr>
<tr>
<td>Other Methods of Accessing the Web Manager</td>
<td>36</td>
</tr>
<tr>
<td>Installing PCMCIA Cards</td>
<td>37</td>
</tr>
<tr>
<td>Connecting PM rPDUs</td>
<td>38</td>
</tr>
</tbody>
</table>
The following figure illustrates an example of an CPS configured with connected devices.

![CPS Setup Example](image)

**Figure 2-1**: CPS Setup Example
Shipping Box Contents

The shipping box contains the CPS along with the items described in Table 2-1. The entry for each part provides its part number, description, and purpose.

Table 2-1: Shipping Box Contents for CPS8—CPS32

<table>
<thead>
<tr>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation CD</td>
<td>PDF copies of this guide, the Console Port Server Quick-Reference Guide, and the Console Port Server Command Reference Guide.</td>
</tr>
<tr>
<td>CPS Installation and Configuration sheet</td>
<td>Basic installation guide in printed format.</td>
</tr>
<tr>
<td>Power cable.</td>
<td>Connect the CPS to a power source. The destination country defines the type of cord that is shipped, based on the country’s standard power outlet. Contact APC Customer Support if you have special requirements.</td>
</tr>
<tr>
<td>• One cable is included with the single power supply CPSs (AP9301, AP9302)</td>
<td></td>
</tr>
<tr>
<td>• Two cables are included with the dual power supply CPS (AP9303).</td>
<td></td>
</tr>
<tr>
<td>Declaration of Conformity</td>
<td>Regulatory information for line voltage products with a microprocessor.</td>
</tr>
<tr>
<td>Product Registration</td>
<td>Product registration form.</td>
</tr>
<tr>
<td>RJ45 to DB25M straight-thru cable (APC part number AP9308)</td>
<td>Use for modems and other DCE devices.</td>
</tr>
<tr>
<td>Mounting brackets (2) Screws (8)</td>
<td>Use to mount the CPS to a rack or cabinet. Brackets for wall mounting are available.</td>
</tr>
</tbody>
</table>
Important Pre-installation Requirements

Before installing and configuring CPS, 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 CPS, and the machine to which the CPS is connected.
- A Web browser that supports the CPS Web Manager (e.g., Netscape, Internet Explorer 6.0, or Mozilla Firefox).
- Java 2 Runtime Environment (JRE) version 1.4.2 or later. (J2RE is available for download 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

- To check Internet Explorer on Windows:
  a. Go to Tools > Internet Options > Advanced
  b. Scroll to the Java section, with a check box that says “Use Java 2 v1.4.2...”.

If an option similar to the above figure does not appear, JRE is not installed on your system. If the option appears, but the checkbox is not enabled, your browser is not activated to use the Java plug-in that came with JRE. Mark the checkbox to enable the Java plug-in.

- To check Netscape or Mozilla on Windows:
  a. Go to Edit > Preferences >Advanced.
  b. Check the “Enable Java” checkbox.
c. To see what version of the Java plug-in is registered:
   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.
   Download the JRE from [http://java.com](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 for Java Plug-in.
   c. Test your browser to see if the correct Java Plug-in is being used.

---

**Basic Installation Procedures**

**Table 2-2: CPS Basic Installation Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount the CPS</td>
<td>“Installing the CPS” on page 28</td>
</tr>
<tr>
<td>Make an Ethernet connection</td>
<td>“Making an Ethernet Connection” on page 28</td>
</tr>
<tr>
<td>Connect servers and other devices to be managed through the CPS</td>
<td>“Connecting Servers and Other Devices to CPS” on page 29</td>
</tr>
<tr>
<td>Make a direct connection to prepare CPS for basic network configuration</td>
<td>“Making a Direct Connection to Configure the Network Parameters” on page 29</td>
</tr>
<tr>
<td>Apply power to the CPS and the connected devices</td>
<td>“Applying Power to the CPS and the Connected Devices” on page 30</td>
</tr>
<tr>
<td>Perform basic network configuration</td>
<td>“Performing Basic Network Configuration Using the wiz Command” on page 31</td>
</tr>
<tr>
<td>Select a security profile using the Web Manager</td>
<td>“Selecting A Security Profile Using the Web Manager” on page 34</td>
</tr>
</tbody>
</table>
Installing the CPS

You will need a hex screwdriver, and nuts and bolts to secure the CPS in the rack.

1. Install the brackets on to the front or back edges of the box using a screwdriver and the provided screws.

2. Install the CPS in a secure position using the nuts and bolts (not provided).

Note: To ensure safety, see Appendix B: Safety Guidelines.

Making an Ethernet Connection

Note: 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.

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

Connecting Servers and Other Devices to CPS

Before connecting servers or devices to the CPS, complete the following tasks:

- Make sure the configuration of servers or devices to be connected is complete.
- 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 will use remote authentication, make sure that the authentication servers are installed and fully configured
• The server’s administrator has provided the IP address and other method-specific information which you need to configure the authentication server on the CPS.

To Connect Devices to Serial Ports

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

---

**Note:** After the CPS is installed, specify the authentication method to the CPS and the serial ports to which each device is connected. See “Authentication” on page 184 for more information on configuring authentication to CPS, and “Physical Ports” on page 205 for detailed 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 CPS. This procedure assumes you know how to use a terminal or terminal emulation program.

On a PC, ensure that a terminal emulation program such as HyperTerminal 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 CPS directly through your PC’s COM port.

2. Open HyperTerminal. **Path:** 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
Basic Installation Procedures

- Data bits: 8 bits
- Parity: None
- Stop bit: 1
- Flow control: None

Applying Power to the CPS and the Connected Devices

To avoid problems with components on connected devices, complete the following procedures in order.

To Apply Power to the CPS

1. Make sure the CPS’s power switch is off.
2. Plug in the power cable.
3. Turn the CPS’s power switch on.

**Note:** If your CPS model is equipped with dual power supplies, make sure you turn both power switches on. After system initialization, an audible alarm may activate if one of the power supplies is off.

To Turn Power On Connected Devices

- Complete the physical connection of the devices to the CPS before you turn on the power switches of the connected devices.

Configuring the Network Parameters

Obtain the following information from the system administrator:

- Hostname
- An IP address for the CPS
- Domain name
- DNS IP address
- Gateway IP address
- Network mask
- IP address of the NTP server (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 CPS’s console port and the COM port of a computer.

To Log Into the CPS Through the Console

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

CPS login: root
Password: apc

Note: For secure access to the connected servers or devices, change the default password (apc) before setting up the CPS.

To Change the Root Password

1. Enter the passwd command.

   [root@CAS root]# passwd

2. Enter a new password when prompted.

   New password: new_password
   Re-enter new password: new_password
   Password changed

A Security Advisory appears the first time CPS receives power, or when the unit is reset to factory default parameters.

To Use the wiz Command to Configure Network Parameters

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

   [root@CAS root]# wiz

2. The system runs the configuration wizard. At the prompt, enter n to change the defaults.

   Set to defaults (y/n) [n]: n
3. Enter your hostname, or press Enter to accept the default hostname.

   Hostname [CAS]: branch_CPS

4. Press Enter to keep DHCP enabled, or press n to specify a static IP address for CPS. By default, the CPS uses the IP address provided by the DHCP server. If your network does not use DHCP, the CPS uses the default IP address 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]: CPS_IP_address

6. Enter the domain name.

   Domain name[apc.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

10. The network configuration parameters appear. Enter y after the prompts shown in the following screen example.

    Are all these parameters correct? (y/n) [n]: y
11. To confirm the configuration, enter the `ifconfig` command.

12. After the initial configuration, select a security profile using the Web Manager.

   **Note:** The first time you login to the Web Manager, you must select a Security Profile.

---

### Selecting A Security Profile Using the Web Manager

**Note:** Ask your system administrator for the IP address of the CPS. By default, the CPS uses the IP address provided by the DHCP server. If your network does not use DHCP, the default CPS IP address is 192.168.160.10.

After the initial configuration, connect to the Web Manager by entering the IP address of the CPS in a supported browser.

#### 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 194.
The administrator can perform the following tasks using the Web Manager.

- Administer CPS 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:** By default, all serial ports of the CPS are 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 “Chapter 9: Security Menu and Forms” on page 177 and “Chapter 10: Ports Menu and Forms” on page 203.

For additional configuration and administration options, and related information, see the chapters listed in the following table.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Regular Users - How to use the Web Manager to access servers and connected devices.</td>
<td>“Chapter 3: Web Manager for Regular Users” on page 39</td>
</tr>
<tr>
<td>Web Manager in Wizard Mode.</td>
<td>“Chapter 5: Configuring CPS in Wizard Mode” on page 64</td>
</tr>
<tr>
<td>Web Manager in Expert Mode.</td>
<td>“Chapter 6: Configuring the CPS in Expert Mode” on page 89</td>
</tr>
</tbody>
</table>
Other Methods of Accessing the Web Manager

You can access the Web Manager using either DHCP or the default IP address. These methods require additional setup and configuration which could be specific to the network configuration of your site.

Using 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 CPS.

1. Install the CPS.
2. Connect computers and other devices to be managed through the CPS.
3. Apply power to the CPS and connected devices.
4. Obtain the CPS’s current IP address.
5. Enter the CPS’s IP address in the browser’s address window.
6. Log in to the CPS and finish configuring users and other settings using the Web Manager.

Using the Default IP Address to Access the Web Manager

The default IP address for the CPS 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 CPS.

1. On a computer that resides on the same subnet as the CPS, change the network portion of the IP address of that computer to 192.168.160.
   
   For example, 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. Open a browser on the computer whose address you changed, enter the CPS’s default IP address, http://192.168.160.10 to open the Web Manager, and log in.
Installing PCMCIA Cards

The front panel of the CPS has two PCMCIA card slots. You can insert and configure one card in each of the slots.

To see a list of supported PCMCIA cards, see the APC Web site, www.apc.com.

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.
2. Physically remove the card from the slot.

To Configure a PCMCIA Card

See “To Configure a PCMCIA Card” on page 133, and then see the sections related to the type of card you need to configure.

Connecting APC Switched Rack PDUs (rPDUs)

Connect APC Switched Rack Power Distribution Units (rPDUs) to the serial ports on the CPS by purchasing an RG-45 to RG-12 cable (APC part number AP9317).

**Note:** To use the integrated power features in the CPS to manage an APC rPDU, the rPDU must have firmware version 2.7.3 or higher. The latest firmware version is available at the APC Software/Firmware Downloads Web page, http://www.apcc.com/tools/download/
The following table lists the tasks for connecting rPDU units and managing power.

**Table 2-3: Tasks Related to Connecting rPDUs**

<table>
<thead>
<tr>
<th>Task</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure serial ports for power management protocol.</td>
<td>“To Configure a Serial Port for rPDU or IPMI Power Management” on page 118</td>
</tr>
<tr>
<td>How the administrators perform rPDU power management using the Web Manager</td>
<td>“rPDU Power Mgmt.” on page 101</td>
</tr>
<tr>
<td>How the regular users manager power outlets using the Web Manager</td>
<td>“To Close an SSH Session” on page 45</td>
</tr>
<tr>
<td>Configure users for rPDU power management</td>
<td>“To Configure Users to Manage Power Outlets on rPDUs” on page 108</td>
</tr>
<tr>
<td>Configure servers for IPMI power management while connected.</td>
<td>“To Delete, Add, or Edit an IPMI Device to Enable or Disable IPMI Power Management” on page 117</td>
</tr>
</tbody>
</table>
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 CPS 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 CPS.
- Perform rPDU power management.
- Change their current password.

This chapter contains the following topics:

- Using the Web Manager page 39
- Features of Regular User Forms page 41
- Connect Form page 42
- rPDU Power Management page 46
- rPDU Multi-Outlet Control page 50
- Security page 52

Using the Web Management Interface (WMI)

CPS users perform most tasks through the APC Web Management Interface (WMI). The WMI runs in a browser and provides a real-time view of all the equipment that is connected to the CPS.

The CPS administrator can use the WMI to configure users and ports. An authorized user can access connected devices through the WMI to troubleshoot, maintain, recycle power, and reboot connected devices.
Logging into the WMI

1. Connect your Web browser to CPS by typing in the Console Access Server’s IP address, provided to you by your system administrator, into the browser’s address field (e.g., 192.168.10.10).

   **Note:** See Chapter 2 for the requirements to use the Web Manager Interface.

2. Press **Enter**.

   The system brings up the CPS WMI Login form.

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

   ![Log On Form](image)

   **Figure 3-1:** Regular User > WMI Login form
Features of Regular User Forms

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

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

<table>
<thead>
<tr>
<th>Form Area</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Off</td>
<td>Click this button to log out.</td>
</tr>
<tr>
<td>Host Name: tomr</td>
<td></td>
</tr>
<tr>
<td>IP Address: 192.168.51.3</td>
<td>Displays the hostname and IP address assigned during initial configuration, and the model number of the CPS.</td>
</tr>
<tr>
<td>Model: AP9303</td>
<td></td>
</tr>
</tbody>
</table>
Connect

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

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

- “Connect to CPS” on page 42
- “Connect to Serial Ports” on page 44

Permission to access a port or perform power management is granted by the CPS 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 CPS

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

---

Table 3-1: Common Screen Information (Continued)

<table>
<thead>
<tr>
<th>Form Area</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Help Button" /></td>
<td>Brings up the online help.</td>
</tr>
</tbody>
</table>

---

Figure 3-3: Regular User > Connect Form
The following table describes the available buttons in the Java applet:

**Table 3-2: Java Applet Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SendBreak</td>
<td>To send a break to the terminal</td>
</tr>
<tr>
<td>Disconnect</td>
<td>To disconnect from the Java applet</td>
</tr>
<tr>
<td><img src="image" alt="left_icon" /> <img src="image" alt="right_icon" /></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 your CPS 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 CPS is required. Your system administrator can help with authorization to a specific CPS ports to which your server or device is connected.

Note: If an authentication server is set up in your network, an authentication method and the related parameters should be set up to allow access to the connected devices. 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 at the top of the screen shows the IP address of the CPS, 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 CPS administrator can choose for the serial ports.

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Access Server (CAS)</td>
<td>Telnet, SSH, Telnet&amp;SSH, Raw</td>
</tr>
<tr>
<td>Terminal Server (TS)</td>
<td>Telnet, SSHv1, SSHv2, Local Terminal, Raw Socket</td>
</tr>
<tr>
<td>Dial-up</td>
<td>PPP-No Auth., PPP, SLIP, CSLIP</td>
</tr>
<tr>
<td>Other</td>
<td>Power Management, Bi-directional Telnet</td>
</tr>
</tbody>
</table>
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 CPS unit has. For example, a CPS with eight serial ports have TCP ports 7001 through 7008. The CPS 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 CPS 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 CPS or its IP address.

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

  ssh -l username:TCP_port_number CPS_IP_address

To Close an SSH Session

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

Note: Make sure you enter the escape character followed by a period at the beginning of a line to close the SSH session.
**rPDU Power Mgmt.**

rPDU or “Rack Power Distribution Units” management allows you to manage the power outlets on the PM products. If you have permission to manage outlets on an rPDU, then when you select the “rPDU Power Mgmt.” option, two tabs appear at the top of the form, as shown in the following figure, “Outlets Manager” and “View rPDUs Info”.

![Regular User > rPDU Power Mgmt. Forms](image)

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

You can access the forms under the rPDU Power Mgmt. menu to manage outlets or view rPDUs information.
Outlets Manager

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

- You do not have permission to manage power on any of the rPDU outlets.
- The CPS cannot detect an rPDU configured for power management.

If you see this message, contact the CPS administrator for help.

![Regular User > Outlets Manager (no permissions)](image)

**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.

![Regular User > Outlets Manager (with permissions)](image)

**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 rPDUs 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 30 seconds.

- Cycle—Turn power briefly off and on again.
- Turn the power On/Off to the outlet.

The following table describes the buttons that correspond to the operations described above:

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Opens a dialog box to Edit an Outlet name, and the Power Up Interval.</td>
</tr>
<tr>
<td><img src="image" alt="Reboot" /></td>
<td>Turn power briefly off and then on again.</td>
</tr>
<tr>
<td><img src="image" alt="Turn" /></td>
<td>Turn power On/Off.</td>
</tr>
</tbody>
</table>

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

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

![Figure 3-8: Regular User > View rPDUs Info](image)

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

**Table 3-5:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Either a default name or administrator-configured name.</td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td>Informs whether syslogging has been configured for messages from this rPDU.</td>
</tr>
<tr>
<td><strong>Buzzer</strong></td>
<td>Whether a buzzer has been configured to sound when a specified alarm threshold is exceeded.</td>
</tr>
<tr>
<td><strong>Number of Outlets</strong></td>
<td>Total number of outlets on a connected rPDU.</td>
</tr>
<tr>
<td><strong>Over Current Protection</strong></td>
<td>Informs whether over-current protection is enabled (to prevent outlets from being turned on if the current on the rPDU exceeds the specified threshold).</td>
</tr>
</tbody>
</table>
rPDU Multi-Outlet Ctrl

Selecting rPDU 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 rPDU Multi-Outlet Ctrl form, Figure 3-9 appears if the following statements are true:

1. There is no multi-outlet device defined.
2. Power Management is not enabled for the serial port the device is connected to.
3. CPS cannot detect an rPDU configured for power management.

Contact the CPS administrator for help if you see this message.

---

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>rPDU model number</td>
</tr>
<tr>
<td></td>
<td>PM8 15A</td>
</tr>
<tr>
<td>Software Version</td>
<td>rPDU firmware version</td>
</tr>
<tr>
<td></td>
<td>1.5.0</td>
</tr>
<tr>
<td>Alarm Threshold</td>
<td>Number of amperes, when reached, that will trigger an alarm or syslog message</td>
</tr>
<tr>
<td></td>
<td>15.0A</td>
</tr>
<tr>
<td>Current</td>
<td>Current level (in amperes) on the rPDU</td>
</tr>
<tr>
<td></td>
<td>0.0A</td>
</tr>
</tbody>
</table>
Figure 3-9: Regular User > rPDU 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.

Figure 3-10: Regular User > rPDU 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 3-7: Regular User > rPDU Multi-Outlet Ctrl. Form Icons

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>A grey light bulb icon indicates that the group is off. A yellow light bulb indicates that the group is on. Clicking the light bulb icon changes the power status of all of the outlets in the group.</td>
</tr>
<tr>
<td><img src="image" alt="Reboot" /></td>
<td>Turn power briefly off and on again</td>
</tr>
</tbody>
</table>

**Note:** Only one outlet needs to be powered on for the entire group to be considered on. In this case, it takes two clicks to turn the power off 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 so that all the outlets are in the same state; the second click turns all of the outlets off.

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 rPDU Power Mgmt. form. See “To Close an SSH Session” on page 45.
Chapter 4: Web Manager for Administrators

This chapter is for system administrators who use the Web Manager to configure the CPS, and for CPS users. For information on how to configure CPS using VI or the Command Line Interface (CLI), see the *APC Console Port Server Command Reference Guide*.

The CPS 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” on page 39.

The sections listed in the following table provides background information related to CPS 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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>APC Web Manager</td>
<td>53</td>
</tr>
<tr>
<td>Common Tasks for CPS Administrators</td>
<td>54</td>
</tr>
<tr>
<td>Common Features of Administrators’ forms</td>
<td>56</td>
</tr>
<tr>
<td>Logging into the Web Manager</td>
<td>58</td>
</tr>
<tr>
<td>Overview of Administrative Modes</td>
<td>61</td>
</tr>
</tbody>
</table>

**APC Web Manager**

CPS administrators perform most tasks through the APC 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 CPS.

The CPS 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 CPS so the Web Manager can be launched over the network.
- The IP address of the CPS must be known.

**Note**: If DHCP is enabled on CPS, the IP address is not fixed. Anyone wanting to access the CPS 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 CPS, 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 CPS 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up users and groups to access connected devices.</td>
<td>“Users and Groups” on page 177</td>
</tr>
<tr>
<td>Task</td>
<td>Where Documented</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set up user authentication to access serial ports.</td>
<td>“Access” on page 224</td>
</tr>
<tr>
<td>Configure serial ports for power management.</td>
<td>“To Configure a Power Management Protocol for an rPDU” on page 219</td>
</tr>
<tr>
<td>Assign users permissions to manage outlets on connected rPDUs.</td>
<td>“To Configure Users to Manage Power Outlets on rPDUs” on page 108</td>
</tr>
<tr>
<td>Set up local or remote data buffering, and specify alarms for one or more serial ports.</td>
<td>“To Configure Data Buffering for Serial Ports” on page 231</td>
</tr>
<tr>
<td></td>
<td>“To Choose a Method for Sending Notifications for Serial Port Data Buffering Events” on page 258</td>
</tr>
<tr>
<td>Set up logging of system messages to a syslog server.</td>
<td>“To Specify Names, Alarms, Syslogging, and Over Current Protection for rPDUs” on page 109</td>
</tr>
<tr>
<td></td>
<td>“Configuring Syslogging for Serial Ports and Specifying Message Filtering” on page 131</td>
</tr>
<tr>
<td>Configure devices for IPMI power management.</td>
<td>“IPMI Power Management” on page 114</td>
</tr>
<tr>
<td>Select an authentication method for accessing connected devices.</td>
<td>“Authentication” on page 184</td>
</tr>
<tr>
<td>Configure packet filtering.</td>
<td>“Firewall Configuration” on page 158</td>
</tr>
</tbody>
</table>
Common Features of Administrator Forms

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

- Buttons and CPS Information
- Getting more information

Buttons and CPS 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](image)

The following table describes the uses for each control button.

<table>
<thead>
<tr>
<th>Button Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>back</td>
<td>Only appears in Wizard mode. Returns the previous form.</td>
</tr>
<tr>
<td>try changes</td>
<td>Tests the changes entered on the current form without saving them.</td>
</tr>
<tr>
<td>cancel changes</td>
<td>Cancels all unsaved changes.</td>
</tr>
<tr>
<td>apply changes</td>
<td>Applies all unsaved changes.</td>
</tr>
<tr>
<td>reload page</td>
<td>Reloads the page.</td>
</tr>
<tr>
<td>Help</td>
<td>Brings up the online help.</td>
</tr>
<tr>
<td>next</td>
<td>Only appears in Wizard mode. Goes to the next form.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>try changes</td>
<td>Click the “try changes” button.</td>
<td>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.</td>
</tr>
<tr>
<td>cancel changes</td>
<td>Click the “cancel changes” button.</td>
<td>Restores the configuration files from the backup that was created the last time changes were applied.</td>
</tr>
<tr>
<td>apply changes</td>
<td>Click the “apply changes” button.</td>
<td>If “try changes” has not been previously clicked, updates the appropriate configuration files. Overwrites the backed-up copy of the configuration files.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Form Area</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Off</td>
<td>Click this button to log out.</td>
</tr>
</tbody>
</table>
| Host Name: tomr  
  IP Address: 192.168.51.3  
  Model: AP9303 | Displays the hostname, IP address assigned during initial configuration, and the model number of the APC Console Port 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 CPS.

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

**Note:** Devices such as the CPS 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. To find a dynamically-assigned IP address, you must make an inquiry to the DHCP server using the MAC address (a 12-digit hexadecimal number, which is on a label on the CPS). Check with the system administrator who configured the basic network parameters to find the assigned IP address. If there is no DHCP server, use the CPS’s default static IP address: 192.168.160.10.

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

**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.

**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 CPS is accessed. Disable the pop-up blocker of your browser to enable this dialog box to appear.
Figure 4-4: Administrator > Security Advisory Message
Overview of Administrative Modes

The CPS Web Manager operates in two modes, Wizard Mode and Expert Mode.

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 CPS 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 CPS web interface in Wizard Mode. The user entry form varies depending on the selected menu item.

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 CPS. 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 CPS 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.

![Figure 4-6: Example of Web Manager Form in Expert Mode](image-url)
The 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 > CPS Configuration and Expert Menus Chapters**

<table>
<thead>
<tr>
<th>Configuring the CPS in Wizard Mode</th>
<th>“Chapter 5: Configuring CPS in Wizard Mode”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the CPS in Expert Mode</td>
<td>“Chapter 6: Configuring the CPS in Expert Mode”</td>
</tr>
<tr>
<td>Applications Menu [Expert]</td>
<td>“Chapter 7: Applications Menu and Form”</td>
</tr>
<tr>
<td>Network Menu [Expert]</td>
<td>“Chapter 8: Network Menu and Forms”</td>
</tr>
<tr>
<td>Administration Menu [Expert]</td>
<td>“Chapter 11: Administration Menu and Forms”</td>
</tr>
</tbody>
</table>
Chapter 5: Configuring CPS 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 in this manual.

<table>
<thead>
<tr>
<th>Step 1: Security Profile</th>
<th>Page 64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2: Network Settings</td>
<td>Page 71</td>
</tr>
<tr>
<td>Step 3: Port Profile</td>
<td>Page 74</td>
</tr>
<tr>
<td>Step 4: Access</td>
<td>Page 77</td>
</tr>
<tr>
<td>Step 5: Data Buffering</td>
<td>Page 81</td>
</tr>
<tr>
<td>Step 6: System Log</td>
<td>Page 86</td>
</tr>
</tbody>
</table>

**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. There are three pre-defined security profiles, *Secured, Moderate, Open*, and an option to configure a *Custom* profile. A fifth option, *Default* sets the parameters to the same as *Moderate*.

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 CPS box for each security profile.

<table>
<thead>
<tr>
<th>Access to CPS</th>
<th>Secured</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SSHv1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SSHv2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Step 1: Security Profile

#### Table 5-2: Wizard > Enabled services to access the serial ports for each profile.

<table>
<thead>
<tr>
<th>Access to CPS</th>
<th>Secured</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SSH root access</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTPS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP redirection to HTTPS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Other Services</th>
<th>Secured</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPC</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 1: Security Profile

The first step in configuring your APC Console Port Server is to select a Security Profile. One of the following situations is applicable when you start the CPS unit.

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

   In this situation when you boot CPS 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, CPS Web Manager restarts for the security configuration to take effect.

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

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

3. CPS is restarting normally.

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

Serial Port Settings and Security Profiles

All serial ports on CPS units shipped from the factory are disabled by default. The administrator can enable ports individually or collectively and assign specific users to individual ports.
Step 1: Security Profile

The following figure shows the default factory settings of serial ports:

**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 Step 2: Network Setting.

**Figure 5-2:** Security and Serial Ports Configuration Alert
Step 1: Security Profile

Selecting or Configuring a Security Profile

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

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

   The following security warning dialog box appears.

   ![Figure 5-3: Security Advisory Dialog Box](image)

   **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.

**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.

![Custom Security Profile Dialog Box](image)

**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

See Table 5-1 on page 64 and the subsequent tables for a comparison of the available services in each security profile. See the Glossary for a definition of the available services.
Step 2: Network Settings

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.

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

   The following dialog box appears.

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

   The CPS 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 CPS, the administrator configures the basic network settings that are 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 CPS
- 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 DHCP is disabled, the form appears as shown in the following figure.

**Figure 5-6**: Wizard > Step 2: Network Settings - DHCP disabled.
If DHCP is enabled, the form appears as shown in the following figure.

![Figure 5-7: Wizard > Step 2: Network Settings - DHCP enabled.](image)

**Configuring 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 CPS 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 (CAP). The protocol used to access the serial ports can be configured in this form.

![Wizard > Step 3: Port Profile](Image)

**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:** 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>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Protocol</strong></td>
<td>Console (Telnet) [Default]</td>
<td>Sets the protocol to be used to connect to devices that are connected to serial ports.</td>
</tr>
<tr>
<td></td>
<td>Console (SSH)</td>
<td>Console (SSH) encrypts data and authentication information.</td>
</tr>
<tr>
<td></td>
<td>Console (TelnetSSH)</td>
<td>Console (TelnetSSH) allows users to connect using either protocol.</td>
</tr>
<tr>
<td></td>
<td>Console (Raw)</td>
<td>Console (Raw) is for unnegotiated plain socket connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use Expert mode if you want to specify any of several other connection protocols that are listed under Ports&gt;Physical Ports&gt;Modify&gt;General.</td>
</tr>
<tr>
<td><strong>Flow Control</strong></td>
<td>None [Default]</td>
<td>Must match the flow control method of the devices connected to all serial ports.</td>
</tr>
<tr>
<td></td>
<td>Hardware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software</td>
<td></td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>None [Default]</td>
<td>Must match the parity used by the devices connected to all serial ports.</td>
</tr>
<tr>
<td></td>
<td>Odd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Even</td>
<td></td>
</tr>
<tr>
<td><strong>Baud Rate (Kbps)</strong></td>
<td>9600 [Default]</td>
<td>Must match the baud rates of the devices connected to all serial ports.</td>
</tr>
<tr>
<td></td>
<td>Options range from 2400–921600 Kbps</td>
<td></td>
</tr>
<tr>
<td><strong>Data Size</strong></td>
<td>8 [Default]</td>
<td>Must match the number of data bits used by the devices connected to all ports.</td>
</tr>
<tr>
<td></td>
<td>Options range from 5–8</td>
<td></td>
</tr>
<tr>
<td><strong>Stop Bits</strong></td>
<td>1 [Default]</td>
<td>Must match the number of stop bits used by the devices connected to all ports.</td>
</tr>
<tr>
<td></td>
<td>Options are either 1 or 2</td>
<td></td>
</tr>
</tbody>
</table>
Step 3: Port Profile

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 and Forms” on page 203.

### Setting 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 CPS 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 and Forms” on page 203 for more detail.

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

   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**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Required</td>
<td>Check for enabled. Unchecked for disabled.</td>
<td>If the “Authentication Required” is enabled, user authentication is enforced using the local passwd database. To specify other authentication methods such as RADIUS, TACACS+, LDAP, Kerberos, or NIS go to Expert mode and select Security&gt;Authentication.</td>
</tr>
</tbody>
</table>

Parameter Options Description
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. Additionally, 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 CPS. By default, any user can access any port as long as they have a valid user ID and password.

![Figure 5-9: Wizard > Step 4: Access](image)
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 CPS.

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

![Add User Dialog Box](https://example.com/figure.png)

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

The following table defines the information required in the fields.

**Table 5-4:** Wizard > Add User Dialog: Field Names and Definitions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong></td>
<td>The username for the account being added.</td>
</tr>
<tr>
<td><strong>Password and Repeat Password</strong></td>
<td>The password for the account.</td>
</tr>
</tbody>
</table>
Table 5-4: Wizard > Add User Dialog: Field Names and Definitions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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 a Bio (biometric authentication). |
| 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.

![Change Password Dialog Box](https://example.com)

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

**Adding a User**

1. Select “Step 3: Access”  
   
The Access form displays.
2. Click Add.

The “Add User” dialog box appears.

3. Enter the username and password in the “User Name” and “Password” fields, and enter the password again in the “Repeat Password” field.

4. Select from the “Group” menu options.

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

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

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

5. 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 APC Bio (biometric authentication).

6. Enter the default shell in the “Shell” field (optional).

7. Enter comments to identify the user’s role or configuration in the “Comments” field (optional).

8. Click OK.

9. Click the “apply changes” button.

**Deleting 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.”
Changing a Password

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

![Figure 5-12: Wizard > Step 5: Data Buffering [Inactive]](image-url)
Once data buffering is enabled, the form displays a number of fields. The displayed fields depend 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 CPS’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”.

![Data Buffering Form]

**Figure 5-13:** Wizard > Step 5: Data Buffering [Local]
The following figure shows the form when data buffering is set to “Destination Remote”:

![Wizard > Step 5: Data Buffering](image)

**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 5-5:** Wizard > Data Buffering Field Names and Definitions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Where the buffer files should be stored. Local, for example, flash, or Remote on a server.</td>
</tr>
<tr>
<td>Mode</td>
<td>For Local Destination - Select Linear for sequential files, or Circular for non-sequential format.</td>
</tr>
<tr>
<td></td>
<td>Local data buffering stores data in circular or linear mode.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Step 5: Data Buffering

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

**Field Name Definition**

- **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 CPS’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.

**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.
Configuring 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. Configure the destination.
   a. If the destination is local, perform the following steps:
      i. From the “Mode” pull-down menu, select “Circular” or “Linear” data buffering.
      ii. Type a file size in bytes into the “File Size (Bytes)” field. The file size should be greater than zero.
Step 6: System Log

b. If the destination is remote, perform the following steps:

i. 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 `<server name or IP address>:<remote path>`, enter `<server name or IP address>:<remote path>` 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 CPS.

ii. 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”.

iii. 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.”

5. 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 CPS’ serial ports. Syslogging for rPDUs is also possible, if rPDU power management is configured. See “Chapter 7: Applications Menu and Form” on page 97.
The form appears as shown in the following figure.

![Figure 5-15: Wizard > Step 6: System Log](image)

**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 CPS. 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 CPS.

See “Syslog Servers” on page 16 for information about how facility numbers are used.

## Adding 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 CPS

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.)

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

5. Click “apply changes.”

Deleting 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 chapters shown below describe the Expert configuration mode in detail, introduce the menu elements in the “Expert” mode, and describe the procedures.

Table 5-6: CPS Configuration and Expert Menus Chapters

<table>
<thead>
<tr>
<th>Menu Element</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the CPS in Expert Mode</td>
<td>6: Configuring the CPS in Expert Mode</td>
</tr>
<tr>
<td>Applications Menu [Expert]</td>
<td>7: Applications Menu and Form</td>
</tr>
<tr>
<td>Network Menu [Expert]</td>
<td>8: Network Menu and Forms</td>
</tr>
<tr>
<td>Ports Menu [Expert]</td>
<td>10: Ports Menu and Forms</td>
</tr>
<tr>
<td>Administration Menu [Expert]</td>
<td>11: Administration Menu and Forms</td>
</tr>
</tbody>
</table>
Chapter 6: Configuring the CPS in Expert Mode

This chapter provides an overview of configuring the CPS Web Manager in Expert Mode. The following chapters introduce the Expert mode forms and functionality.

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

This chapter includes the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Menus and Forms</td>
<td>90</td>
</tr>
<tr>
<td>Mapping of the Expert Mode Menus and Form</td>
<td>91</td>
</tr>
<tr>
<td>A Description on Forms and a Reference to Where the Details are Documented.</td>
<td>92</td>
</tr>
</tbody>
</table>
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](image)

**Note:** Procedures in this manual use shortcuts to tell how to get to Web Manager forms. For example, a step telling the user to access the “Outlets Manager” form uses this convention: “In Expert mode, go to Applications> rPDU 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 highlighted in **blue** to go to the section where the form is described.

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

<table>
<thead>
<tr>
<th>Applications</th>
<th>Network</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Connect</td>
<td>— Host Settings</td>
<td>— Users and Groups</td>
</tr>
<tr>
<td>— rPDU Power Mgmt.</td>
<td>— Syslog</td>
<td>— Active Ports Sessions</td>
</tr>
<tr>
<td>— Outlets Manager</td>
<td>— PCMCIA Management</td>
<td>— Authentication</td>
</tr>
<tr>
<td>— View rPDUs Info</td>
<td>— VPN Connections</td>
<td>— Auth Type</td>
</tr>
<tr>
<td>— Users Manager</td>
<td>— SNMP</td>
<td>— RADIUS</td>
</tr>
<tr>
<td>— Configuration</td>
<td>— Firewall Configuration</td>
<td>— Tacacs+</td>
</tr>
<tr>
<td>— rPDU Multi-Outlet Ctrl</td>
<td>— Host Table</td>
<td>— Ldap</td>
</tr>
<tr>
<td>— IPMI Power Management</td>
<td>— Static Routes</td>
<td>— Kerberos</td>
</tr>
<tr>
<td>— Terminal Profile Menu</td>
<td></td>
<td>— NIS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Security Profiles</td>
</tr>
<tr>
<td>Ports</td>
<td>Administration</td>
<td></td>
</tr>
<tr>
<td>— Physical Ports</td>
<td>— System Information</td>
<td></td>
</tr>
<tr>
<td>— Modify Selected/All Ports</td>
<td>— Notifications</td>
<td></td>
</tr>
<tr>
<td>— General</td>
<td>— Time/Date</td>
<td></td>
</tr>
<tr>
<td>— Access</td>
<td>— Boot Configuration</td>
<td></td>
</tr>
<tr>
<td>— Data Buffering</td>
<td>— Backup Configuration</td>
<td></td>
</tr>
<tr>
<td>— Multi User</td>
<td>— Upgrade Firmware</td>
<td></td>
</tr>
<tr>
<td>— Power Management</td>
<td>— Reboot</td>
<td></td>
</tr>
<tr>
<td>— Other</td>
<td>— Online Help</td>
<td></td>
</tr>
<tr>
<td>— Virtual Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>— Ports Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>— Ports Statistics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Description of Forms in Expert Mode

The following table briefly describes the functionality of each menu and the related forms. For detailed procedures, see the section of the manual listed under *Where Documented*.

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

<table>
<thead>
<tr>
<th>Form</th>
<th>Use This Form To</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Connect to the CPS shell through a secure SSH session, or connect to a specific serial port.</td>
<td>Chapter 7, “Connect”</td>
</tr>
<tr>
<td>rPDU Power Mgmt.</td>
<td>Manage power outlets on the PM family of Rack 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.</td>
<td>Chapter 7, “rPDU Power Mgmt.”</td>
</tr>
<tr>
<td>rPDU Multi-Outlet Ctrl</td>
<td>Manage all power outlets of a multi-outlet device connected to the PM family of Rack Power Distribution Units in one single operation.</td>
<td>Chapter 7, “rPDU Multi-Outlet Ctrl”</td>
</tr>
<tr>
<td>Terminal Profile Menu</td>
<td>Configure a menu of commands that will be presented to the user when they power on their computer terminal and login to the CPS. This is a special application used only when the CPS is being used as a server with terminals attached.</td>
<td>Chapter 7, “Terminal Profile Menu”</td>
</tr>
</tbody>
</table>
### Table 6-3: Expert > Network

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Settings</strong></td>
<td>Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.</td>
<td>Chapter 8, “Host Settings”</td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td>Configure how CPS will handle its syslog messages. CPS generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit and control purposes.</td>
<td>Chapter 8, “Syslog”</td>
</tr>
<tr>
<td><strong>PCMCIA Management</strong></td>
<td>Configure the optional PCMCIA cards. CPS supports several PCMCIA cards including modem, ISDN, wireless and wired NICs, Compact Flash and IDE drives for data buffer storage.</td>
<td>Chapter 8, “PCMCIA Management”</td>
</tr>
<tr>
<td><strong>VPN Connections</strong></td>
<td>Configure one or more VPN connections to other systems or CPS attached devices.</td>
<td>Chapter 8, “VPN Connections”</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>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.</td>
<td>Chapter 8, “SNMP”</td>
</tr>
<tr>
<td><strong>Firewall Configuration</strong></td>
<td>Configure static IP tables, and how packets should be filtered.</td>
<td>Chapter 8, “Firewall Configuration”</td>
</tr>
<tr>
<td><strong>Host Table</strong></td>
<td>View information about the local network environment. View table of hosts; create, edit, and delete hosts.</td>
<td>Chapter 8, “Host Table”</td>
</tr>
</tbody>
</table>
**Static Routes**

To add routes manually. Static routes are a very quick and effective way to route data from one subnet to different subnets.

![Chapter 8, “Static Routes”](image)

---

**Users and Groups**

Create or edit users and groups, establish or change their passwords, access rights and privileges.

![Chapter 9, “Users and Groups”](image)

---

**Active Port Sessions**

Show the active sessions, as well as their identifications, features and usage statistics.

![Chapter 9, “Active Ports Sessions”](image)

---

**Authentication**

Enter the authentication method used to access CPS.

![Chapter 9, “Authentication”](image)

---

**Security Profiles**

Select a pre-defined Security Profile, or choose Custom Profile to configure individual settings.

![Chapter 9, “Security Profiles”](image)

---

**Physical Ports**

Activates or deactivates serial ports. Set the parameters for each or all ports. Configure specific parameters for the serial ports where rPDU devices are connected.

![Chapter 10, “Physical Ports”](image)
Description of Forms in Expert Mode

Table 6-5: Expert > Ports

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Ports</td>
<td>Perform Clustering. One CPS can be used as a Master to control other CPS (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.</td>
<td>Chapter 10, “Virtual Ports”</td>
</tr>
<tr>
<td>Port Status</td>
<td>View the current status of each port. The information provided here are: RS232 Signal Status and user connected to each port.</td>
<td>Chapter 10, “Ports Status”</td>
</tr>
<tr>
<td>Ports Statistics</td>
<td>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.</td>
<td>Chapter 10, “Ports Statistics”</td>
</tr>
</tbody>
</table>

Table 6-6: Administration

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>View information on the system hardware, version, file system and PCMCIA cards loaded</td>
<td>Chapter 11, “System Information”</td>
</tr>
<tr>
<td>Notifications</td>
<td>Configure the alarm strings and the destination of the notification. CPS can send notification by email, pager or SNMP trap in the occurrence of any system warnings and alarms.</td>
<td>Chapter 11, “Notifications”</td>
</tr>
</tbody>
</table>
### Table 6-6: Administration

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time/Date</strong></td>
<td>Set the time zone and configure the system’s Date and Time. Network Time Protocol (NTP) can also be used.</td>
<td>Chapter 11, “Time/Date”</td>
</tr>
<tr>
<td><strong>Boot Configuration</strong></td>
<td>Configure CPS to boot from its internal firmware or from the network. Defines the settings for loading the operating system in the event that the CPS fails to boot successfully. The CPS can boot from its internal firmware or from the network. This section configures the required parameters.</td>
<td>Chapter 11, “Boot Configuration”</td>
</tr>
<tr>
<td><strong>Backup Configuration</strong></td>
<td>Use a FTP server to save and retrieve your CPS configuration; use a storage device to store your configuration.</td>
<td>Chapter 11, “Backup Configuration”</td>
</tr>
<tr>
<td><strong>Upgrade Firmware</strong></td>
<td>Upload/upgrade new firmware.</td>
<td>Chapter 11, “Upgrade Firmware”</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td>Reboot the CPS system.</td>
<td>Chapter 11, “Reboot”</td>
</tr>
<tr>
<td><strong>Online Help</strong></td>
<td>Configure a path to a local server for storing the online help files.</td>
<td>Chapter 11, “Online Help”</td>
</tr>
</tbody>
</table>
Chapter 7: Applications Menu and Form

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

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Connect to the CPS shell via a secure SSH session or connect to the serial ports.</td>
<td>Page 98</td>
</tr>
<tr>
<td>rPDU Power Mgmt.</td>
<td>Manage power outlets on the PM family of Rack 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.</td>
<td>Page 101</td>
</tr>
<tr>
<td>rPDU Multi-Outlet Ctrl</td>
<td>Manage all power outlets of a multi-outlet server or device connected to the PM in one single operation.</td>
<td>Page 110</td>
</tr>
<tr>
<td>IPMI Power Mgmt.</td>
<td>Manage IPMI (Intelligent Platform Management Interface) devices. Power on/off remote machines and check their current status.</td>
<td>Page 114</td>
</tr>
<tr>
<td>Terminal Profile Menu</td>
<td>Configure a menu of commands that will be presented to the user when they power on their computer terminal and login to the CPS. This is a special application used only when the CPS is being used as server with terminals attached.</td>
<td>Page 121</td>
</tr>
</tbody>
</table>
Applications

Under “Applications” in Expert mode, five options appear in the left menu panel as shown in the following figure. The options are Connect, rPDU Power Mgmt., rPDU Multi Outlet Ctrl, IPMI Power Mgmt., and Terminal Profile Menu.

![Figure 7-1: Expert > Applications Menu Options](image)

Connect

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

![Figure 7-2: Expert > Applications > Connect Form](image)
Using the “Connect” form, you can connect directly to CPS, or to the devices that are connected to the serial ports.

- Connect to CPS

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

![Image of ssh session Java Applet](https://example.com/ssh_session.png)

**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 and Forms” on page 177.

• 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.

![Figure 7-4: Expert > Serial Port Java Applet](image)

Note the difference between “Connect to CPS” 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 must supply a username and password to log into the device.

**Connecting to the CPS**

This procedure logs you into the CPS as a “Regular User” in a ssh session.

1. In Expert mode, go to Applications > Connect.
2. Click the “Connect to CPS” 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”.

**Connecting 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.

**rPDU Power Mgmt.**

Selecting “rPDU Power Mgmt.” brings up the five tabs shown in the following figure. Using the rPDU power management forms you can manage the power to the connected devices only if a serial port is configured for power management.
For the procedure, see “To Configure a Serial Port for rPDU or IPMI Power Management” on page 118.

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

<table>
<thead>
<tr>
<th>Form</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlets Manager</td>
<td>102</td>
</tr>
<tr>
<td>View rPDUs Info</td>
<td>105</td>
</tr>
<tr>
<td>Users Manager</td>
<td>107</td>
</tr>
<tr>
<td>Configuration</td>
<td>109</td>
</tr>
</tbody>
</table>

**Outlets Manager**

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

- 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:

![Outlets Manager Form]

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

The following table illustrates what each icon indicates.

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Yellow bulbs]</td>
<td>Yellow bulbs indicate an outlet is switched on. Gray indicates an outlet is switched off.</td>
</tr>
<tr>
<td>![Reboot]</td>
<td>An orange “Reboot” button is active next to each outlet that is on.</td>
</tr>
</tbody>
</table>
Clicking the Edit button brings up the following dialog box.

![Edit Outlet Dialog Box](https://example.com/edit-outlet.png)

**Figure 7-7:** 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 > rPDU 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 rPDUs Info

Select Applications > rPDU Power Mgmt. > View rPDUs Info tab. The following form appears.

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

The following table describes the information viewable on the “View rPDUs 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 rPDUs General Information

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Either a default name or administrator-</td>
</tr>
<tr>
<td></td>
<td>configured name appears.</td>
</tr>
<tr>
<td>Buzzer</td>
<td>Whether a buzzer has been configured to</td>
</tr>
<tr>
<td></td>
<td>sound when a specified alarm threshold has</td>
</tr>
<tr>
<td></td>
<td>reached.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Whether syslogging has been configured for</td>
</tr>
<tr>
<td></td>
<td>messages from this rPDU.</td>
</tr>
<tr>
<td>Over Current Protection</td>
<td>Whether over current protection is enabled.</td>
</tr>
<tr>
<td></td>
<td>“Over Current Protection” is to prevent</td>
</tr>
<tr>
<td></td>
<td>outlets from being turned on, if the current</td>
</tr>
<tr>
<td></td>
<td>on the rPDU exceeds the specified threshold.</td>
</tr>
</tbody>
</table>

View the following information about each rPDU that is configured through a serial port:

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Model number</td>
</tr>
<tr>
<td></td>
<td>[Model No.]</td>
</tr>
<tr>
<td></td>
<td>15A</td>
</tr>
<tr>
<td>Software Version</td>
<td>Firmware version</td>
</tr>
<tr>
<td></td>
<td>2.6.0</td>
</tr>
<tr>
<td>Alarm Threshold</td>
<td>Number of amperes that triggers an alarm or</td>
</tr>
<tr>
<td></td>
<td>syslog message if it is reached</td>
</tr>
<tr>
<td></td>
<td>15.0 A</td>
</tr>
<tr>
<td>Current</td>
<td>Current level on the rPDU</td>
</tr>
<tr>
<td></td>
<td>0.0 A</td>
</tr>
<tr>
<td>Maximum Detected</td>
<td>Maximum current detected</td>
</tr>
<tr>
<td></td>
<td>0.4 A</td>
</tr>
<tr>
<td>Temperature</td>
<td>Temperature on the rPDU (Displayed if</td>
</tr>
<tr>
<td></td>
<td>equipped with a temperature sensor.)</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Maximum Detected</td>
<td>Maximum temperature detected on the rPDU</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
To View and Reset rPDU Information

1. Go to Applications > rPDU Power Mgmt. > View rPDUs Info.
   The “View rPDUs 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 > rPDU Power Mgmt., you can assign users to outlets.

The following figure shows the form with two users listed for an rPDU. The rPDU is connected to serial port 1 configured for power management.

![Figure 7-9: rPDU Power Mgmt> Users Manager](image)

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

![Add/Edit User x Outlets dialog box](image)

**Figure 7-10:** Expert > rPDU 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 2: Users Information](image)

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

**To Configure Users to Manage Power Outlets on rPDUs**

1. Go to Applications > rPDU 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 > rPDU Power Mgmt., you can specify the following:
- An alias for the rPDU
- A threshold current between 1 and xx amperes. (The maximum current depends on the rPDU model. Refer to View rPDUs Info section to determine your rPDU model.
- Any of the following actions to occur if the threshold current is exceeded on the rPDU.
   - Over-current protection. If enabled, the outlets on the rPDU cannot be turned on, when the current on the rPDU 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 PM rPDU connected to, and is configured for power management.

To Specify Names, Alarms, Syslogging, and Over Current Protection for rPDUs

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 rPDU.
1. Go to Applications > rPDU Power Mgmt. > Configuration.
2. The Configuration form displays entries for all ports configured for power management. Perform the following steps for each rPDU.
rPDU Multi-Outlet Ctrl

a. Assign a name to the rPDU in the “Name” field, if desired.

b. For each rPDU, 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 rPDU.

c. If enabling over-current protection, a buzzer, or alarm notification, select an Alarm Threshold from the pull-down menu.

3. Click “apply changes.”

rPDU Multi-Outlet Ctrl

Selecting Applications > rPDU 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.

![Figure 7-12: Expert > Applications > rPDU Multi-Outlet Ctrl](image)

Whether the power supplies are connected to the same rPDU 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 rPDU or IPMI Power Management” on page 118.

Figure 7-13: Expert > Applications > Multi-Outlet Ctrl [not configured]
Prerequisites for Multi-Outlet Control

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

• An rPDU 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 rPDU.
• The rPDU 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 next to the individual outlets is used to display the status of the outlet but cannot be used to control the outlet.

Figure 7-14: Expert > Applications > Multi-Outlet Control Icons
The icons in the first line of each group are described in the following table.

**Table 7-4: Expert > rPDU Multi-Outlet Ctrl form icons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="light_bulb.png" alt="Light Bulb" /></td>
<td>A grey light bulb icon indicates that the group is off. A yellow light bulb indicates that the group is on. Clicking the light bulb icon once changes the power status of all of the outlets in the group.</td>
</tr>
<tr>
<td><img src="reboot.png" alt="Reboot" /></td>
<td>Turn power briefly off and then on again</td>
</tr>
</tbody>
</table>

**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, you must click the light bulb icon twice to turn the power off or to lock the entire group. (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 > rPDU 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 in the same state.

1. Go to Applications > rPDU Multi-Outlet Ctrl.
2. To apply power to the group of outlets in OFF state, click the grey light bulb adjacent to the group name.
3. To remove power from the group of outlets in ON state, 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 > rPDU Multi-Outlet Ctrl.

2. To power on the group, click the yellow light bulb adjacent to the group name.
   All of the outlets turn 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 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 > rPDU Multi-Outlet Ctrl.

2. Make sure that all of the outlets are turned on
   For information about turning on all outlets, see “To Power On or Power Off a Group of Outlets in the Same Power State” on page 113.

3. 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.

![Add Button](image)

**Figure 7-15:** Expert > Applications > IPMI Power Mgmt.

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

![Add/Edit Form](image)

**Figure 7-16:** 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 Power Management

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 CPS information must be obtained from the IPMI device’s administrator.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Alias</td>
<td>Optional</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device on the network</td>
</tr>
<tr>
<td>Authentication type</td>
<td>None, Straight Password, MD5, MD2</td>
</tr>
<tr>
<td>Access Level</td>
<td>(User/Operator/Administrator) Default is User.</td>
</tr>
<tr>
<td>Username</td>
<td>Default is NULL user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for administering the remote device</td>
</tr>
</tbody>
</table>

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.
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 rPDU 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. Note that you will need to use a “Console” connection protocol to activate the Power Management tab.

3. To enable Power Management of a device connected to the current port and plugged into a connected rPDU, click “Enable Power Management on this port.”.
The following form appears.

4. Click the “Add” button

The “Add Outlet” dialog box appears.

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

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 rPDU 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 CPS’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.”

![Figure 7-20: Expert > Serial Port > Power Management > User Permissions (Detail)](image)

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.

![Figure 7-21: Expert > Serial Port > Power Management > Enable IPMI](image)
2. Enter an IPMI hot key.
   A device user 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 ^ (e.g., ^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 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 CPS with access to the Linux commands on the CPS unless you configure a menu here. The following figure shows an empty menu.

![Figure 7-22: Expert > Applications > Terminal Profile Menu](image)
The menu can contain any command recognized by the Linux operating system on the CPS. 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.

![Add Option Dialog Box](image)

**Figure 7-23:** 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.

![Terminal Profile Menu Example](image)

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

The command menu appears when the terminal receives power.
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 and 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

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Settings</td>
<td>Configure the network parameters such as Host Name, IP addresses, DNS services, Gateway, and Bonding</td>
<td>Page 125</td>
</tr>
<tr>
<td>Syslog</td>
<td>Configure how the CPS will handle its syslog messages. The CPS generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit and control purposes.</td>
<td>Page 130</td>
</tr>
<tr>
<td>PCMCIA Management</td>
<td>Configure the optional PCMCIA cards. CPS supports several PCMCIA cards including modem, ISDN, GSM, CDMA, wireless LAN, Ethernet LAN, Compact Flash, and IDE drives for data buffer storage.</td>
<td>Page 132</td>
</tr>
<tr>
<td>VPN Connections</td>
<td>Configure one or more VPN connections to other systems or CPS attached devices.</td>
<td>Page 149</td>
</tr>
<tr>
<td>SNMP</td>
<td>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.</td>
<td>Page 153</td>
</tr>
<tr>
<td>Menu Selection</td>
<td>Use this menu to:</td>
<td>Where Documented</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>Configure static IP tables, and how packets should be filtered.</td>
<td>Page 158</td>
</tr>
<tr>
<td>Host Tables</td>
<td>View information about the local network environment. View table of hosts; create, edit, and delete hosts.</td>
<td>Page 172</td>
</tr>
<tr>
<td>Static Routes</td>
<td>To manually add routes. Static routes are a very quick and effective way to route data from one subnet to different subnets.</td>
<td>Page 173</td>
</tr>
</tbody>
</table>

**Network**

**Host Settings**

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

![Host Settings Form](image)

**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.

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

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

<table>
<thead>
<tr>
<th>Filed Name</th>
<th>Field Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The fully qualified domain name identifying the specific host computer on the network.</td>
</tr>
<tr>
<td>Console Banner</td>
<td>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.</td>
</tr>
<tr>
<td>Filed Name</td>
<td>Field Definition</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary IP</td>
<td>IP address of the CPS unit.</td>
</tr>
<tr>
<td>Secondary IP</td>
<td>The secondary IP address of the CPS unit. By configuring a second IP address, the unit will be available for more than one network.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for a subnet.</td>
</tr>
<tr>
<td>Secondary Network Mask</td>
<td>Optional.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit used by the TCP protocol.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Address of the Domain Name Server.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>Address of the backup Domain Name Server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The name that identifies the domain, for example, domainname.com.</td>
</tr>
<tr>
<td>Gateway IP</td>
<td>The IP address to the gateway on the subnet.</td>
</tr>
<tr>
<td>Bonding</td>
<td>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.</td>
</tr>
</tbody>
</table>

If bonding is enabled, the following values should be set.

- **Miimon**: The interval in which the active interface is checked to see if it is still communicating (in milliseconds).
- **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 the APC Console Port Server Command Reference Guide for more information.

Configuring 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 CPS 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 CPS in the “Primary IP” field.
   
   b. Enter the netmask in the “Network Mask” field.
   
   c. If the CPS has a second Ethernet card in a PCMCIA slot, enter the CPS’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 check mark 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 you select Network > Syslog, the form shown in the following figure appears.

![Figure 8-3: Expert > Network > Syslog](image)

You can use the Syslog form to configure how the CPS 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 CPS 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:

- Category “CAS log;” “Data Buffering log;” “Web log;” or “System log.”

### Configuring Syslogging for Serial Ports and Specifying 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

The PCMCIA features is available only on the APC 32-port Model AP9303 CPS unit. To expand the capabilities of your AP9303 CPS, use the following procedures to use PCMCIA cards with the unit.

When Network > PCMCIA Management is selected the following form appears.

![Figure 8-4: Expert > Network > PCMCIA Management](image)

You can use the PCMCIA management form to configure the following types of PCMCIA cards:

- 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.

For a list of the supported PCMCIA cards, see the APC Web site, [http://www.apc.com](http://www.apc.com). Search for “Console Port Server PCMCIA” and select the result that points to the supported PCMCIA cards.
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 CPS and Click the “Insert” button for the slot in which you installed the PCMCIA card.
   The following dialog box appears.

3. Click OK.
   The card information appears under the “Card Type” column as shown in the following figure.

4. Click the Configure button.
5. The Slot dialog box appears. Select the PCMCIA card type to configure from the pull-down menu.

![Slot dialog box with PCMCIA card types]

6. Follow the procedure that corresponds to the type of the PCMCIA card you have installed.

<table>
<thead>
<tr>
<th>Configuration Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Modem PCMCIA Card</td>
<td>137</td>
</tr>
<tr>
<td>Configuring an ISDN PCMCIA Card</td>
<td>138</td>
</tr>
<tr>
<td>Configuring a GSM PCMCIA Card</td>
<td>141</td>
</tr>
<tr>
<td>Configuring an Ethernet PCMCIA Card</td>
<td>142</td>
</tr>
<tr>
<td>Configuring a PCMCIA Compact Flash Card or a PCMCIA Hard Disk Drive</td>
<td>144</td>
</tr>
<tr>
<td>Configuring a Wireless LAN PCMCIA Card</td>
<td>145</td>
</tr>
<tr>
<td>Configuring a CDMA PCMCIA Card</td>
<td>147</td>
</tr>
</tbody>
</table>
Configuring a Modem PCMCIA Card

You can use the “PCMCIA Management” form under “Network” to enable a remote user to call into the CPS 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 PCMCIA Card Configuration Dialog Box](image)

**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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCMCIA Card</td>
<td>Pull-down menu to select the type of PCMCIA card that you are using.</td>
</tr>
<tr>
<td>PPP</td>
<td>Check box to enable point-to-point protocol.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that the CPS uses to call back.</td>
</tr>
</tbody>
</table>
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.

![Figure 8-6: Expert > Modem PCMCIA Card Configuration Dialog Box - PPP](image)

If you enable “Call Back”, the Phone Number field appears on the Slot dialog box, as shown in the following figure.

![Figure 8-7: Expert > Modem PCMCIA Card Configuration Dialog Box - Call Back](image)
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 CPS 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 CPS through an ISDN PCMCIA card.

When you select ISDN from the pull-down menu, the dialog box shown in the following figure appears.
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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select ISDN from the pull-down menu.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that CPS uses to call back.</td>
</tr>
</tbody>
</table>

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 CPS 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 CPS 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 CPS 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 PCMCIA Card Configuration Dialog Box](image)

**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 PCMCIA Card Configuration Dialog Box](image-url)

**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 8-2:** Expert > Form Fields For a GSM Card

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select GSM from the pull-down menu.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Pin Number</td>
<td>The personal identification number associated with the GSM.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that CPS uses to call back.</td>
</tr>
</tbody>
</table>
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 CPS 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 CPS 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.

![Image of Ethernet PCMCIA Card Configuration Dialog Box]

**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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select Ethernet from the Pull-down menu.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The local IP address of the Ethernet.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The network address of the Ethernet.</td>
</tr>
</tbody>
</table>

**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.

![Figure 8-12: Expert > PCMCIA Compact Flash/Hard Disk Configuration Dialog Box](image)

The following table provides a brief description of the fields available in the Compact Flash/Hard Disk dialog box.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select Compact Flash/Hard Disk from the Pull-down menu.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check box to enable the storage device.</td>
</tr>
<tr>
<td>Use for Data Buffering</td>
<td>Check box to use the storage device for data buffering.</td>
</tr>
</tbody>
</table>
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.

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 8-5: Expert > Form Fields for a Wireless LAN Card.**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Pull-down box to select the type of PCMCIA card that you are using.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The local IP address of the Ethernet.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The network address of the Ethernet.</td>
</tr>
<tr>
<td>MyPrivateNet (ESSID)</td>
<td>The unique identifier for the wireless access point.</td>
</tr>
<tr>
<td>Channel</td>
<td>The communication channel with the access point.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The translation of data into code during transmission.</td>
</tr>
<tr>
<td>Key</td>
<td>The key or password to decode the encrypted data.</td>
</tr>
</tbody>
</table>

**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.
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 PCMCIA Configuration Dialog Box](https://example.com/image.png)

**Figure 8-14**: Expert > PCMCIA CDMA Card Configuration Dialog Box

CDMA cards are modem cards that make it possible for CPS 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 8-6**: Expert > Form Fields for a CDMA Card.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Pull-down box to select the type of PCMCIA card that you are using.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the CDMA card used by the ppp connection.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the CDMA card used by the ppp connection.</td>
</tr>
</tbody>
</table>
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 CPS 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.

3. Click “apply changes.”

4. Physically remove the card from the PCMCIA slot on the front of the CPS.
VPN Connections

VPN, or Virtual Private Network enables a secured communication between CPS and a remote network by utilizing a gateway, and creating a secured tunnel between CPS 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.

![Figure 8-15: Expert > Network > VPN Connections](image)

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 which option is selected, “RSA Public Keys” or “Shared Secret”.

---

**Network**
The remote gateway is referred to as the Remote or “Right” host, and the CPS 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 CPS 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 8-7: Expert > Field and Menu Options for Configuring a VPN Connection

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Name</strong></td>
<td>Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN.”</td>
</tr>
<tr>
<td><strong>Authentication Protocol</strong></td>
<td>The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header).</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Authentication method used, either “RSA Public Keys” or “Shared Secret.”</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>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, <a href="mailto:hostname@xyz.com">hostname@xyz.com</a></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td><strong>NextHop</strong></td>
<td>The router through which the CPS (on the left side) or the remote host (on the right side) sends packets to the host on the other side.</td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
<td>The netmask of the subnetwork where the host resides.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td><strong>RSA Key (If RSA Public Keys is selected)</strong></td>
<td>You need to generate a public key for the CPS 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.</td>
</tr>
<tr>
<td><strong>Pre-Shared Secret (If “Shared Secret” is selected)</strong></td>
<td>Pre-shared password between left and right users.</td>
</tr>
</tbody>
</table>
To Configure VPN

To enable VPN, make sure that IPSec is enabled on the Network > Services form.

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 CPS (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.

Field Name | Definition
--- | ---
**Boot Action** | The boot action configured for the host, either Ignore, Add, or Start.

---

To Configure VPN

To enable VPN, make sure that IPSec is enabled on the Network > Services form.

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 CPS (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 CPS SNMP agent supports SNMPv1/v2 and v3. To use SNMP v1 or v2, you must 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.

![Figure 8-17: Expert > Network > SNMP](image)

You can use this form to enable notifications about significant events or traps from CPS 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 8-8: Expert > Fields and Menu Options for SNMP Configuration**

<table>
<thead>
<tr>
<th>Field or Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysContact</td>
<td>The email address of the CPS’s administrator, for example, <a href="mailto:cps_admin@apcc.com">cps_admin@apcc.com</a>.</td>
</tr>
<tr>
<td>SysLocation</td>
<td>The physical location of the CPS.</td>
</tr>
<tr>
<td>Community</td>
<td>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 CPS.</td>
</tr>
<tr>
<td>Source</td>
<td>SNMP v1 and v2 only. Valid entries are “default” or a subnet address, for example, 193.168.44.0/24.</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier. Each managed object has a unique identifier.</td>
</tr>
</tbody>
</table>
| Permission           | “Read Only” access to the entire MIB (Management Information Base) except for SNMP configuration objects.  
“Read/Write” access to the entire MIB except for SNMP configuration objects. |
| User Name and Password | SNMP v3 only. |
Clicking the “Add” or “Edit” buttons under “SNMPv1/SNMPv2 Configuration” brings up the “New/Mod SNMP v1 v2 Configuration” dialog box, as shown in the following figure.

![Figure 8-18: Expert > “New/Mod SNMP v1 v2 Configuration” Dialog Box](image)

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.

![Figure 8-19: Expert > “New/Mod SNMP v3 Configuration” Dialog Box](image)

**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, complete 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 SNMPv1 or SNMPv2 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 SNMPv3 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, complete 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. To configure one or more serial ports to send SNMP traps, see “SNMP Trap Notifications Entry” on page 263.
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.

![Firewall Configuration Form](image)

**Figure 8-20**: Expert > Network > Firewall Configuration

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

Packet filtering relies on defined chains and rules. See “Packet Filtering on CPS” on page 10 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.

![Figure 8-21: Expert > Firewall Configuration “Edit Chain” Dialog Box](image)

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.

![Figure 8-22: Firewall Configuration “User-defined Chain” Message](image)
“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.

![Figure 8-23: Firewall Configuration “Delete Default Chain” Message](image)

“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](image)

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 Form and Buttons](image)

**Figure 8-25:** Firewall Configuration “Edit Rules for chain_name” Form and 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.
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.

![Target Pull-down Menu Options](https://192.168.51.3 - INPUT chain - Add Rule - Microsoft Internet Explorer)

![Figure 8-27: Firewall Configuration “Add Rule” and “Edit Rule” Target Menu Options](https://192.168.51.3 - INPUT chain - Add Rule - Microsoft Internet Explorer)

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 8-28:** 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 8-29:** 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.
Network

Figure 8-30: 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](image)

Figure 8-31: 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 8-9: Expert > TCP Options Fields

<table>
<thead>
<tr>
<th>Field/Menu Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>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 the range of specified IP addresses.</td>
</tr>
<tr>
<td>OR - Destination Port - AND- to</td>
<td></td>
</tr>
<tr>
<td>TCP Flags</td>
<td>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.”</td>
</tr>
</tbody>
</table>
UDP Protocol Fields

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

![UDP Options Section](image)

**Figure 8-32**: Firewall Configuration “Add Rule” and “Edit Rule” UDP Protocol Fields

The following table defines the fields in the UDP Options Section.

**Table 8-10**: Expert > UDP Options Fields

<table>
<thead>
<tr>
<th>Field/Menu Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inverted</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
**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.

![Table 8-11: Expert > Firewall Configuration Input and Output Interface, and Fragments Fields Definitions.](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Interface</strong></td>
<td>The input interface (ethN) for the packet</td>
</tr>
<tr>
<td><strong>Output Interface</strong></td>
<td>The output interface (ethN) for the packet</td>
</tr>
<tr>
<td><strong>Inverted</strong></td>
<td>“Inverting” an item negates the selected rules. Rules will apply to everything except the selected options.</td>
</tr>
<tr>
<td><strong>Fragments</strong></td>
<td>The types of packets to be filtered:</td>
</tr>
<tr>
<td></td>
<td>• All packets</td>
</tr>
<tr>
<td></td>
<td>• 2nd, 3rd... fragmented packets</td>
</tr>
<tr>
<td></td>
<td>• Non-fragmented and 1st fragmented packets</td>
</tr>
</tbody>
</table>

**Figure 8-34:** Firewall Configuration Input and Output Interface Fields and Fragments Menu Options

The following table defines the fields in the above figure.

**Table 8-11:** Expert > Firewall Configuration Input and Output Interface, and Fragments Fields Definitions.
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.

![Figure 8-35: Firewall Configuration “Add Rule” and “Edit Rule” LOG Target Fields](image)

The following table defines the menu options and fields in the “LOG Options Section.”

**Table 8-12: Expert > Target LOG Options Selection Fields**

<table>
<thead>
<tr>
<th>Field or Menu Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>One of the options in the pull-down menu:</td>
</tr>
<tr>
<td></td>
<td>![Dropdown menu with options: emerg, alert, crit, err, warning, notice, info, debug]</td>
</tr>
<tr>
<td>Log Prefix</td>
<td>The prefix is included in the log entry.</td>
</tr>
<tr>
<td>TCP Sequence</td>
<td>Includes the TCP sequence in the log.</td>
</tr>
<tr>
<td>TCP Options</td>
<td>Includes TCP options in the log.</td>
</tr>
<tr>
<td>IP Options</td>
<td>Includes IP options in the log.</td>
</tr>
</tbody>
</table>
REJECT Target

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject with</td>
<td>“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.</td>
</tr>
<tr>
<td>icmp-net-unreachable</td>
<td>ICMP network unreachable alias.</td>
</tr>
<tr>
<td>icmp-host-unreachable</td>
<td>ICMP host unreachable alias.</td>
</tr>
<tr>
<td>icmp-port-unreachable</td>
<td>ICMP port unreachable alias.</td>
</tr>
<tr>
<td>icmp-protounreachable</td>
<td>ICMP protocol unreachable alias.</td>
</tr>
<tr>
<td>icmp-net-prohibited</td>
<td>ICMP network prohibited alias.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-host-prohibited</td>
<td>ICMP host prohibited alias.</td>
</tr>
<tr>
<td>echo-reply</td>
<td>Echo reply alias.</td>
</tr>
<tr>
<td>tcp-reset</td>
<td>TCP RST packet alias.</td>
</tr>
</tbody>
</table>

Field Name Definition
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.

   ![Image of warning dialog box](image)

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

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 158.
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 158

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.

---

**Figure 8-37**: Expert > Network > Host Tables
To Define the CPS’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.

![Figure 8-38: Expert > Network > Static Routes](image)

Clicking the “Edit” or “Add” buttons brings up a form shown in the following figure.
Figure 8-39: 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.

Figure 8-40: 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.

![Image of the fields and menus for adding a static route with the “Host” route type selected.]

**Figure 8-41:** Expert > Static Routes “Add” and “Edit” Dialog Boxes—Host Route

**Table 8-13:** Fields to configure when you select a routing type from the “New/Modify Route” dialog boxes:

<table>
<thead>
<tr>
<th>Field or Menu Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Route</strong></td>
<td>Choices are “Default,” “Network,” or “Host.”</td>
</tr>
<tr>
<td><strong>Network IP</strong></td>
<td>Appears only when “Network” route is selected. Type the IP address of the destination network.</td>
</tr>
<tr>
<td><strong>Network Mask</strong></td>
<td>Appears only when “Network” route is selected. Type the netmask of the destination network.</td>
</tr>
<tr>
<td><strong>Host IP</strong></td>
<td>Appears only when “Host” route is selected. Type the IP address of the destination host.</td>
</tr>
<tr>
<td><strong>Go to</strong></td>
<td>Choices are “Gateway” or “Interface.”</td>
</tr>
<tr>
<td><strong>[Adjacent field]</strong></td>
<td>Type the IP address of the gateway or the name of the interface.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Type the number of hops to the destination.</td>
</tr>
</tbody>
</table>
To Configure Static Routes [Expert]

See Table 8-13 on page 175 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, complete 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 and Forms

This chapter describes the “Security” menu and its 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

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users and Groups</td>
<td>Create or edit users and groups, establish or change their passwords, and access rights and privileges.</td>
<td>Page 177</td>
</tr>
<tr>
<td>Active Port Sessions</td>
<td>Show the active sessions, as well as their identifications, features and usage statistics.</td>
<td>Page 182</td>
</tr>
<tr>
<td>Authentication</td>
<td>Enter the authentication method used to access CPS.</td>
<td>Page 184</td>
</tr>
<tr>
<td>Security Profiles</td>
<td></td>
<td>Page 194</td>
</tr>
</tbody>
</table>

Users and Groups

Users and Groups form allows you to do the following tasks:

- Set up user access to the CPS 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 CPS by the administrator. The username is **root**, and the default password is **apc**. For security purposes, change the default password.

Selecting Security > Users & Groups in Expert mode brings up the form shown in the following figure.

![User and Group Form](image)

**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.

![Add User Dialog Box]

**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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of the user to be added.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user name.</td>
</tr>
<tr>
<td>Group</td>
<td>On the Group pull-down menu, select “Regular User [Default]” or “Admin.”</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: To configure a user to be able to perform all administrative functions, select the “Admin” group.</td>
</tr>
<tr>
<td>Shell</td>
<td>Optional. The default shell is /bin/sh when the user makes an SSH or telnet connection.</td>
</tr>
<tr>
<td>Comments</td>
<td>Optional notes about the user’s role or configuration.</td>
</tr>
</tbody>
</table>
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.

![Add Group Dialog Box]

**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.

![Figure 9-4: Expert > Security > Active Ports Sessions](image)

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.

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

**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.

**Figure 9-5**: Expert > Security > Authentication

Use the Authentication forms to complete the following tasks:

- Select a method for authenticating logins to CPS.
- Identify authentication servers that are configured for logins to CPS or to the serial ports.
Configuring Authentication for CPS Logins

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

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

To Configure the CPS 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 CPS, 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 CPS 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.

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

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

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

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

**Table 9-4: Tasks for Setting up Authentication Servers.**

<table>
<thead>
<tr>
<th>Method</th>
<th>Variations</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/Local, or RADIUS/DownLocal</td>
<td>See “To Configure a RADIUS Authentication Server” on page 187</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal</td>
<td>See “To Configure a TACACS+ Authentication Server” on page 187</td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP, LDAP/Local, or LDAP/DownLocal</td>
<td>See “To Configure an LDAP Authentication Server” on page 189</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos, Kerberos/Local, or Kerberos/DownLocal</td>
<td>See “To Configure a Kerberos Authentication Server” on page 191</td>
</tr>
<tr>
<td>NIS</td>
<td>NIS, Local/NIS, NIS/Local, or NIS/DownLocal</td>
<td>See “To Configure a NIS Authentication Server” on page 193</td>
</tr>
</tbody>
</table>
To Configure a RADIUS Authentication Server

Perform the following procedure to configure a RADIUS authentication server when CPS 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.

   ![Figure 9-7: Expert > Security > Authentication > Radius](image)

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 CPS.

To Configure a TACACS+ Authentication Server

Perform the following procedure to configure a TACACS+ authentication server when CPS 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.
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 CPS 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.
Click “apply changes.”

The changes are stored in /etc/tacplus.conf on the CPS.

User 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 CPS 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.

The following table lists the task necessary for enabling authorization to serial ports on the CPS.

To Configure an LDAP Authentication Server

Perform the following procedure to configure an LDAP authentication server when the CPS 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 CPS and the connected devices know the passwords assigned to the accounts:

- An account for “admin”
- If LDAP authentication is specified for the CPS, accounts for all users who need to log into the CPS 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.

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 apc.com, the correct entry is: dc=apc, 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 CPS.

---

**To Configure a Kerberos Authentication Server**

Perform the following procedure to configure a Kerberos authentication server when CPS 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 CPS and connected devices know the passwords assigned to the accounts:

- An account for “admin”
- If Kerberos authentication is specified for CPS, accounts for all users who need to log into the CPS 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 CPS and the Kerberos server exist in the CPS’s `/etc/hosts` file.

   a. Go to Network > Host Table in Expert mode.

      The “Host Table” form appears.

   b. Add an entry for CPS 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 time zone settings are synchronized on the CPS and on the Kerberos server.

**Note:** Kerberos authentication depends on time synchronization. Time and date synchronization can be achieved by setting both CPS 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 267.
   b. To manually set the time and date on the CPS, see “To Manually Set the Time and Date” on page 267.
   c. Work with the Kerberos authentication server administrator to synchronize the time and date between CPS and the Kerberos server.

3. Set the time zone on CPS by going to Administration > Time/Date in Expert mode as per the following figure. The default is GMT.

   ![Figure 9-10: Expert > Administration > Time/Date](image)

The Kerberos form displays as shown in the following figure.

**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 CPS 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.

**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.

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. There are three pre-defined security
profiles, *Secured, Moderate, Open*, and an option to configure a *Custom* profile. A fifth option, *Default* sets the parameters to the same as *Moderate*.

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 CPS box for each security profile.

<table>
<thead>
<tr>
<th>Access to CPS</th>
<th>Secured</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>✔️</td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>SSHv1</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>SSHv2</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Allow SSH root access</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HTTP</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HTTPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HTTP redirection to HTTPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Table 9-6**: Expert > Enabled services to access the serial ports for each profile.

<table>
<thead>
<tr>
<th>Access to Serial Ports</th>
<th>Secured</th>
<th>Moderate</th>
<th>Open</th>
<th>Default</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console (Telnet)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Console (SSH)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Console (Raw)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Serial Port Authentication</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
The first step in configuring your APC Console Port Server is to define a Security Profile. One of the following situations is applicable when you boot up the CPS unit.

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

   In this situation when you boot CPS 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 CPS restarts.

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

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

3. CPS 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 CPS 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.

![Figure 9-14: Expert > Physical Ports Default Factory Settings](image)

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.

![Figure 9-15: Security Profile and Serial Ports Configuration Alert](image)
• 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.

**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 CPS at your site, or you have reset the unit to factory default.

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

   The following security warning dialog box appears.

   **Figure 9-17:** Security Advisory Dialog Box
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.

![Figure 9-18: Wizard > Step 1: Security Profile Form](image)

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.

![Custom Security Profile Dialog Box](image)

**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.

See Table 9-5 on page 195, and the subsequent tables for a comparison of the available services in each security profile. See 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.

5. Once you select a security profile or configure a custom profile and apply the changes, the CPS Web Manager restarts in order for the changes to take effect. The following dialog box appears.

6. Select “apply changes” to save the configuration to Flash. CPS Web Manager restarts.

7. Login after Web Manager restarts.

8. The Web Manager defaults to Ports > Ports Status page. Proceed to the forms and the related tasks outlined in the table below.

**Table 9-8:** Configuring CPS in Expert Mode

- Configure Users and Groups: “Users and Groups” on page 177
- Configure Serial Ports: “Physical Ports” on page 205
- Configure Network Settings: “Host Settings” on page 125
- Configure rPDU Power Management: “rPDU Power Mgmt.” on page 101
Chapter 10: Ports Menu and 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

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Ports</td>
<td>Activate or deactivate the serial ports. Set the parameters for each or all ports. Configure specific parameters for the serial ports where rPDU devices are connected.</td>
<td>Page 205</td>
</tr>
<tr>
<td>Virtual Ports</td>
<td>Perform Clustering. This section shows how to define and configure slaves. One CPS can be used as a Master to control other CPS (slaves) units. All ports of the slave unit appear as if they are part of the master unit.</td>
<td>Page 244</td>
</tr>
<tr>
<td>Port Status</td>
<td>View the current status of each port. The information provided here are RS232 Signal Status and user connected to each port.</td>
<td>Page 250</td>
</tr>
<tr>
<td>Ports Statistics</td>
<td>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.</td>
<td>Page 251</td>
</tr>
</tbody>
</table>
The Ports section of CPS 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.

![Figure 10-1: Expert > Ports](image)

Using the forms described in the following sections, you can perform custom configuration of serial ports.
Physical Ports

In Expert mode, select Ports > Physical Ports to view the following form:

![Physical Ports Form]

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:

![Physical Ports Tab Options]

Figure 10-2: Expert > Ports > Physical Ports

Figure 10-3: Expert > Ports > Physical Ports > “Modify .... Ports ” Tab Options
To Select One or More Serial Ports


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.
   - 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.
3. Go to the desired procedure from the following list.

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Configure a Serial Port Connection Protocol for a Console Connection</td>
<td>212</td>
</tr>
<tr>
<td>To Configure User Access to Serial Ports</td>
<td>225</td>
</tr>
<tr>
<td>To Configure Data Buffering for Serial Ports</td>
<td>231</td>
</tr>
<tr>
<td>To Configure Multiple Sessions and Port Sniffing for One or More Serial Ports</td>
<td>234</td>
</tr>
<tr>
<td>To Configure a Serial Port for rPDU or IPMI Power Management</td>
<td>238</td>
</tr>
<tr>
<td>To Configure a User for rPDU Power Management While Connected To a Serial Port</td>
<td>239</td>
</tr>
<tr>
<td>To Configure TCP Port Number, STTY Options, Break Interval, and the Login Banner for a Serial Port Connected to a Console</td>
<td>243</td>
</tr>
</tbody>
</table>

**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.”
Physical Ports

General

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

![General Form](image)

**Figure 10-4:** Expert > Ports > Physical Ports > General Form

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

<table>
<thead>
<tr>
<th>Connection Profile</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Access Server (CAS)</td>
<td>209</td>
</tr>
<tr>
<td>Terminal Server (TS)</td>
<td>209</td>
</tr>
<tr>
<td>Bidirectional Telnet</td>
<td>211</td>
</tr>
<tr>
<td>Modem (RAS)</td>
<td>212</td>
</tr>
<tr>
<td>Power Management</td>
<td>212</td>
</tr>
</tbody>
</table>
**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 accesses the serial port through the Web Manager, the session automatically uses the specified protocol to connect to the console of the connected device.
- When a user logs in remotely to the serial port, access is allowed only for the selected protocol. If another protocol is used then access is denied. For example, if you specify the “Console (SSH)” protocol, the user can use `ssh` but cannot use `telnet` to access the serial port.

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

**Table 10-2: Expert > Console Connection Protocols**

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console (Telnet)</td>
<td>Authorized users can use <code>telnet</code> to connect to the console of the connected device.</td>
</tr>
<tr>
<td>Console (SSH)</td>
<td>Authorized users can use <code>ssh</code> to connect to the console of the connected device.</td>
</tr>
<tr>
<td>Console (TelnetSSH)</td>
<td>Authorized users can use <code>telnet</code> and/or <code>ssh</code> to connect to the console of the connected device simultaneously. When multiple sessions feature is configured, simultaneous <code>telnet</code> and/or <code>ssh</code> sessions are allowed through the serial port.</td>
</tr>
<tr>
<td>Console (Raw)</td>
<td>Authorized users can make a Raw Socket connection to the console of the connected device.</td>
</tr>
</tbody>
</table>

**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.

---

**Ports Menu & Forms**

209
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 CPS.

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**

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>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, CPS opens a Telnet session on the server. The server’s IP address should be specified on the “Other” form, Ports &gt; Physical Ports &gt; Other.</td>
</tr>
<tr>
<td>SSHv1</td>
<td>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 CPS opens an SSHv1 session on the server. The server’s IP address should be specified on the “Other” form, Ports &gt; Physical Ports &gt; Other.</td>
</tr>
<tr>
<td>SSHv2</td>
<td>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 CPS opens a SSHv2 session on the server. The server’s IP address should be specified on the “Other” form, Ports &gt; Physical Ports &gt; Other.</td>
</tr>
<tr>
<td>Local Terminal</td>
<td>Dedicates a computer terminal that is connected to the selected serial port for connecting to CPS. When the attached terminal is powered on, CPS opens a Telnet session on itself. The user then can use any of the CPS’s Linux commands. You can also create a terminal profile menu, Applications &gt; Terminal Profile Menu that enables the user to quickly launch sessions on any number of remote hosts.</td>
</tr>
</tbody>
</table>
Bidirectional Telnet Protocol

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

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 PM rPDUs connected to the serial ports.

**Table 10-4:** Expert > Protocols for Serial Ports Connected to Modems or rPDUs

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP-No Auth</td>
<td>Starts a PPP session without interactive authentication required.</td>
</tr>
<tr>
<td></td>
<td>Assumes the specified CPS serial port is connected to an external modem.</td>
</tr>
<tr>
<td>PPP</td>
<td>Starts a PPP session with authentication required.</td>
</tr>
<tr>
<td></td>
<td>Assumes the specified CPS serial port is connected to an external modem.</td>
</tr>
<tr>
<td>SLIP</td>
<td>Starts a SLIP session.</td>
</tr>
<tr>
<td></td>
<td>Assumes the specified CPS serial port is connected to an external modem.</td>
</tr>
<tr>
<td>CSLIP</td>
<td>Starts a CSLIP session.</td>
</tr>
<tr>
<td></td>
<td>Assumes the specified CPS serial port is connected to an external modem.</td>
</tr>
<tr>
<td>Power Management</td>
<td>Configures the serial port for power management.</td>
</tr>
<tr>
<td></td>
<td>Assumes an PM rPDU is connected to the serial port.</td>
</tr>
</tbody>
</table>

**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](image)

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.

![Physical Ports Form](image)

**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).

![Protocol Options](image)

**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 222.
5. To further configure the serial port’s connection protocol:
   • For user access and authentication methods see “Access” on page 224.
   • To specify the TCP Port number, configure modem initialization options, and
     configure PPP options, see “Other” on page 240.

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 211.

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](image)

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.

   ![Figure 10-9: Expert > Ports > Physical Ports > Bidirectional Telnet Connection](image)
3. To change the connection protocol, select Bidirectional Telnet from the “Connection Protocol” pull-down menu.

<table>
<thead>
<tr>
<th>Console (Telnet)</th>
<th>Console (SSH)</th>
<th>Console (Raw)</th>
<th>Console (TelnetSSH)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bidirectional Telnet</strong></td>
<td>Telnet</td>
<td>SSHv1</td>
<td>SSHv2</td>
</tr>
<tr>
<td>Raw Socket</td>
<td>PPP-No Auth</td>
<td>PPP</td>
<td>SLIP</td>
</tr>
<tr>
<td><strong>Power Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 222.

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 121.

**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 209.
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](image1)

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.

![Figure 10-12: Expert > Ports > Physical Ports > Terminal Server Connection](image2)
3. To change the connection protocol, select a Terminal Server connection from the “Connection Protocol” pull-down menu, “Telnet”, “SSHv1”, “SSHv2”, “Local Terminal”, or “Raw Socket”.

4. To configure a terminal to automatically connect to CPS, 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.”

Figure 10-13: Connection Protocols > Terminal Server
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, and 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.

![Expert > Ports > Physical Ports > Modem Connection Active Tabs](image)

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.

![Expert > Ports > Physical Ports > Modem Connection](image)
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](image)

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 222.

5. To further configure the serial port’s connection protocol:
   - For user access and authentication methods, see “Access” on page 224.
   - To specify the TCP Port number, and configure modem initialization and PPP options see “Other” on page 240.

6. If you are finished, click “Done.”

7. Click “apply changes.”

**To Configure a Power Management Protocol for an rPDU**

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

1. In Expert mode, go to Ports > Physical Ports, select a port or ports to modify, and 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](image)
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.

![Figure 10-18: Expert > Ports > Physical Ports > Power Management Connection](image)

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

![Figure 10-19: Connection Protocols > Power Management](image)

4. Enter the name for the rPDU in the “Alias” field.
5. Select an access method to the rPDU 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.

   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 a 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.

![Figure 10-21: Expert > Ports > Physical Ports > Serial Port Settings](image)

**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. (If the rPDU is not connected, you cannot select the Access tab.)

![Expert > Ports > Physical Ports > Access Form](image)

**Figure 10-22:** Expert > Ports > Physical Ports > Access Form

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authorized Users/Groups| Restrict or deny access to a serial port by specifying one or more users or groups.  
  You can deny access to one or more users or groups by entering an exclamation point (!) before the user or group name. For example, to explicitly deny access to a user called “noadmin” and enable access only to a single user called “johnd” you would enter the following:  
  `!noadmin,johnd`  
  **Important:** The names in the example are separated by a comma. |
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 10-5: Expert > Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No authentication.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Authentication is performed using a Kerberos server.</td>
</tr>
<tr>
<td>Kerberos/Local</td>
<td>Kerberos authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>KerberosDownLocal</td>
<td>Local authentication is performed only when the Kerberos server is down.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Authentication is performed against an LDAP database using an LDAP server.</td>
</tr>
<tr>
<td>LDAP/Local</td>
<td>LDAP authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>LDAPDownLocal</td>
<td>Local authentication is performed only when the LDAP server is down.</td>
</tr>
<tr>
<td>Local</td>
<td>Authentication is performed locally. For example, using the /etc/passwd file.</td>
</tr>
<tr>
<td>Local/Radius</td>
<td>Authentication is performed locally first, switching to Radius if unsuccessful.</td>
</tr>
<tr>
<td>Local/TACACS+</td>
<td>Authentication is performed locally first, switching to TACACS+ if unsuccessful.</td>
</tr>
<tr>
<td>Local/NIS</td>
<td>Authentication is performed locally first, switching to NIS if unsuccessful.</td>
</tr>
</tbody>
</table>
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 CPS.

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS</td>
<td>NIS authentication is performed.</td>
</tr>
<tr>
<td>NIS/Local</td>
<td>NIS authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>NISDownLocal</td>
<td>Local authentication is performed only when the NIS server is down.</td>
</tr>
<tr>
<td>Radius</td>
<td>Authentication is performed using a Radius authentication server.</td>
</tr>
<tr>
<td>Radius/Local</td>
<td>Radius authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>RadiusDownLocal</td>
<td>Local authentication is performed only when the Radius server is down.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Authentication is performed using a TACACS+ authentication server.</td>
</tr>
<tr>
<td>TACACS+/Local</td>
<td>TACACS+ authentication is tried first, switching to Local if unsuccessful.</td>
</tr>
<tr>
<td>TACACS+DownLocal</td>
<td>Local authentication is tried only when the TACACS+ server is down.</td>
</tr>
</tbody>
</table>
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 10-6: Expert > Procedures to Configure an Authentication Server**

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos, Kerberos/Local, or Kerberos/DownLocal</td>
<td>“To Configure a Kerberos Authentication Server” on page 191.</td>
</tr>
<tr>
<td>LDAP, LDAP/Local, or LDAP/DownLocal</td>
<td>“To Configure an LDAP Authentication Server” on page 189.</td>
</tr>
<tr>
<td>NIS, Local/NIS, NIS/Local, or NIS/DownLocal</td>
<td>“To Configure a NIS Authentication Server” on page 193.</td>
</tr>
<tr>
<td>RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal</td>
<td>“To Configure a RADIUS Authentication Server” on page 187.</td>
</tr>
<tr>
<td>TACACSPlus, Local/TACACSPlus, TACACSPlus/Local, or TACACSPlusDownLocal</td>
<td>“To Configure a TACACS+ Authentication Server” on page 187.</td>
</tr>
</tbody>
</table>

---

**Data Buffering**

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

![Figure 10-23: Expert > Ports > Physical Ports > Data Buffering](image)
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.

![Data Buffering Form](image)

**Figure 10-24:** Expert > Ports > Physical Ports > Data Buffering

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

**Table 10-7:** Expert > Data Buffering Form Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Location for the data files. Either “Local” or “Remote”</td>
</tr>
</tbody>
</table>
Table 10-7: Expert > Data Buffering Form Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode (Local Destination)</td>
<td><em>circular</em> or <em>linear</em>. 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.</td>
</tr>
<tr>
<td>File Size (Bytes) (Local Destination)</td>
<td>The maximum file size for the data buffer file. The file size must be greater than zero.</td>
</tr>
<tr>
<td>NFS File Path (Remote Destination)</td>
<td>The path for the mount point of the directory where data buffer file is to be stored.</td>
</tr>
<tr>
<td>Note:</td>
<td>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 CPS.</td>
</tr>
<tr>
<td>Record the timestamp...</td>
<td>Save a timestamp with the data in the data buffer file.</td>
</tr>
<tr>
<td>Show Menu</td>
<td>Options for the buffer file.</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>The IP address for the preconfigured Syslog server.</td>
</tr>
<tr>
<td>Facility Number</td>
<td>Choose a facility number to assign to CPS. Obtain the facility number for CPS from the system administrator of the syslog server. The facility number is included in any syslog message generated from CPS. The server’s administrator can use facility numbers to isolate logs from individual devices into individual files. Options range from Local0 to Local7.</td>
</tr>
<tr>
<td>Syslog Buffer Size</td>
<td>Maximum size of the buffer in the Syslog server.</td>
</tr>
<tr>
<td>Buffer SysLog at all times</td>
<td>As indicated.</td>
</tr>
<tr>
<td>Buffer SysLog only when nobody is connected to the port</td>
<td>As indicated.</td>
</tr>
</tbody>
</table>
To Configure Data Buffering for Serial Ports

Perform this procedure if you want to configure data buffering. Obtain the facility number for the CPS 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.

![Multi User Form](image)

**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 10-8: Expert > Multi User Form Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Multiple Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Sniff Mode</td>
<td>Allow sniffing on multiple user connection to a serial port.</td>
</tr>
<tr>
<td>Privilege Users</td>
<td>Users with access rights to a multi user shared session.</td>
</tr>
<tr>
<td>Menu Hotkey</td>
<td>The hotkey for accessing the menu.</td>
</tr>
<tr>
<td>Notify Users</td>
<td>Checkbox to enable notify users of session access.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Do not allow multiple sessions. Only two users can connect to the same port simultaneously. One shared session and one normal session are allowed.</td>
</tr>
<tr>
<td>Yes (show menu)</td>
<td>More than two simultaneous users can connect to the same serial port. A Sniffer menu is presented to the user and they can choose to:</td>
</tr>
<tr>
<td></td>
<td>• Open a sniff session</td>
</tr>
<tr>
<td></td>
<td>• Open a read/write session</td>
</tr>
<tr>
<td></td>
<td>• Cancel a connection</td>
</tr>
<tr>
<td></td>
<td>• Send a message to other users connected to the same serial port.</td>
</tr>
<tr>
<td>Read/Write (do not show menu)</td>
<td>Read/write sessions are opened, and the sniffer menu won’t be presented.</td>
</tr>
</tbody>
</table>
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.”

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadOnly (do not show menu)</td>
<td>Read only sessions are opened, and the sniffer menu won’t be presented.</td>
</tr>
</tbody>
</table>
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.

![Power Management Form](image)

**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 rPDU power management, Applications > rPDU 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.
The following table describes the available fields in the power management form.

**Table 10-9: Expert > Power Management Form Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Power Management on this Port</strong></td>
<td>Check mark to enable Power Management on the selected port(s).</td>
</tr>
<tr>
<td><strong>Enable IPMI on this port</strong></td>
<td>Check mark to enable IPMI on the selected port(s).</td>
</tr>
<tr>
<td><strong>IPMI Key</strong> (available only if IPMI is enabled)</td>
<td>The key sequence which the authorized user(s) can use to perform IPMI power management. The default for IPMI power management is Ctrl+Shift+i (^I)</td>
</tr>
<tr>
<td><strong>IPMI Server</strong> (available only if IPMI is enabled)</td>
<td>Select the device configured for IPMI power management.</td>
</tr>
<tr>
<td><strong>PowerMgmt Port</strong></td>
<td>View listbox for the PM enabled ports and the assigned outlet numbers.</td>
</tr>
</tbody>
</table>
Power management while connected to a port is possible only when one or both of the following conditions are true.

- The device connected to CPS is plugged into an PM rPDU and is configured for power management.
- The device connected to CPS 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.

### Field Name | Definition
--- | ---
Power Management Key | The key sequence which the authorized user(s) can use to perform power management. The default for rPDU 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 | Entry field to add a new user/group (available only if “Allow Users/Groups” radio button is selected)
Allowed Users/Groups | View list box of authorized users or groups. (available only if “Allow Users/Groups” radio button is selected)
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 PM rPDU and the outlet number(s) into which the device is plugged.

![Add Outlet Dialog Box](https://example.com/add-outlet.png)

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 rPDU 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 rPDU 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 rPDU, 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 rPDU 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 CPS’s serial ports.

1. Configure a serial port for rPDU 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.

![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.”

![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.
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 10-10: Expert > Ports > Physical Ports > Other Form Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCP Port</strong></td>
<td>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 CPS unit has. For example, an CPS unit with 8 serial ports have TCP port numbers 7001 through 7008.</td>
</tr>
<tr>
<td><strong>Port IP Alias</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows EMS</td>
<td>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.</td>
</tr>
<tr>
<td>Biometric Authentication Required</td>
<td>Adds another layer of security by using the 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.</td>
</tr>
<tr>
<td>TCP Keep-alive Interval</td>
<td>Specifies the time interval between the periodic polling by the system to check client processes and connectivity.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>The maximum time (in seconds) that a session can be idle before the user is logged off.</td>
</tr>
<tr>
<td>STTY Options</td>
<td>Set terminal options.</td>
</tr>
<tr>
<td>Break Interval</td>
<td>Usually 250 to 500 milliseconds. It’s a logical zero on the TXD or RXD lines to reset the communications line.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>Usually a character sequence ~break (Ctrl-b)</td>
</tr>
<tr>
<td>Login Banner</td>
<td>Enter the text you wish to appear as a login banner when logging into a terminal.</td>
</tr>
<tr>
<td>Host to Connect</td>
<td>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.</td>
</tr>
<tr>
<td>Terminal Type</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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.
Virtual Ports

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](image)

The virtual ports form allows you to perform clustering of CPS units. The CPS 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 CPS as the “master” unit to control other CPS units as “slaves”. The ports on the slave unit(s) appears as if they are part of the master unit.

**Note:** Multiple rPDUs should only be connected through the serial port of the master CPS unit when you are configuring a cluster.

To define and configure slave units:

When you click the “Add” or “Edit” button on the Ports > Virtual Ports form, the following dialog box appears.

![Virtual Ports New/Modify Port Dialog Box](http://192.168.51.3:New/ModifyPort.png)

**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 10-11: Expert > New/Modify Port Dialog Box Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Ports</td>
<td>Number of ports on each slave unit. Choices are 8, 16 and 32.</td>
</tr>
<tr>
<td>First Local Port Number</td>
<td>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.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The IP address for the master CPS or it can be the global IP address of the cluster in the network.</td>
</tr>
<tr>
<td>First Local TCP Port No.</td>
<td>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.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The IP address of the slave.</td>
</tr>
<tr>
<td>First Remote TCP Port Number</td>
<td>The first TCP port number of the slave. The default is 7001.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The communication protocol used by the slave. The options are Telnet or SSH.</td>
</tr>
</tbody>
</table>
Once you have configured the slave CPS unit and defined the cluster parameters, the slave serial ports and the connected devices are accessible from the master CPS unit under Applications > Connect > Serial pull-down menu as shown in the following figure.

**Figure 10-34:** Expert > Applications > Connect > Serial pull-down menu

**To Cluster CPS Units or Modify Cluster Configuration**

Use this procedure if you want to cluster CPS units and add or modify ports.

**Note:** CPS 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.
2. From the drop-down menu select the number of ports that you want to assign as slaves. Choices are 8, 16 and 32.

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.

![Figure 10-36: Expert > Ports > Virtual Ports > New/Modify > Port Names Dialog box](image)

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 CPS 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.

![Figure 10-37: Expert > Ports > Ports Status (Read-Only)](image)

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 10-12: Expert > Port Status Read-Only Form**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The serial port number.</td>
</tr>
<tr>
<td>Alias</td>
<td>Displays the name (alias) for the serial port if one is assigned by the administrator.</td>
</tr>
<tr>
<td>RS232 Signal Status</td>
<td>Serial Communication Signal Status</td>
</tr>
<tr>
<td>Current User(s)</td>
<td>Displays the user(s) connected to each serial port.</td>
</tr>
</tbody>
</table>
Ports Statistics

Selecting Ports > Port Statistics in Expert mode, brings up the following read-only form.

![Figure 10-38: Expert > Ports > Port Statistics (Read-Only)](image)

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 10-13:** Expert > Ports>Port Status Read-Only Form

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The serial port number.</td>
</tr>
<tr>
<td>Alias</td>
<td>Displays the name (alias) for the serial port if one is assigned by the administrator.</td>
</tr>
<tr>
<td>Baud Rate</td>
<td>The measure of how fast data is moving between devices.</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>Data transmitted.</td>
</tr>
</tbody>
</table>
## Ports Statistics

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rx Bytes</strong></td>
<td>Data received.</td>
</tr>
<tr>
<td><strong>Frame</strong></td>
<td>A formatted packet of data usually associated with the Data-Link layer.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Error checking bit appended to a data packet. A method of checking the accuracy of transmitted characters. Parity is usually not used, but can be odd or even. A None parity means that data has not exchanged.</td>
</tr>
<tr>
<td><strong>Break</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Overrun</strong></td>
<td>The amount of time it takes for the new data to overwrite the older unread data.</td>
</tr>
</tbody>
</table>
Chapter 11: Administration Menu and 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

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>View information on the system hardware, version, file system and PCMCIA cards loaded.</td>
<td>Page 255</td>
</tr>
<tr>
<td>Notifications</td>
<td>Configure the alarm strings and the destination of the notification. CPS can send notification by email, pager or SNMP trap in the occurrence of any system warnings and alarms.</td>
<td>Page 257</td>
</tr>
<tr>
<td>Time/Date</td>
<td>Set the time zone and configure the system’s date and time manually, or use Network Time Protocol (NTP).</td>
<td>Page 266</td>
</tr>
<tr>
<td>Boot Configuration</td>
<td>Configure CPS to boot from its internal firmware or from the network.</td>
<td>Page 268</td>
</tr>
</tbody>
</table>

This section defines the settings for loading the operating system in the event that the CPS fails to boot successfully. CPS can boot from its internal firmware or from the network.
<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Config</td>
<td>Configure an FTP server to save and retrieve your CPS configuration, or choose a storage device to store your configuration.</td>
<td>Page 271</td>
</tr>
<tr>
<td>Upgrade Firmware</td>
<td>Upload or upgrade to a new firmware.</td>
<td>Page 274</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboot the CPS.</td>
<td>Page 277</td>
</tr>
<tr>
<td>Online Help</td>
<td>Configure a path to a local server for storing the online help files.</td>
<td>Page 278</td>
</tr>
</tbody>
</table>
System Information

Selecting Administration > System information in Expert mode brings up the following information form.

![System Information Form]

**Figure 11-1:** Expert > Administration > System Information
You can use the form to view the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| **System**    | • Kernel Version  
                • Current Date   
                • Up Time        
                • Power Supply State |
| **CPU**       | • CPU Type    
                • Clock Speed  
                • Revision     
                • Bogomips     |
| **Memory**    | • MemTotal   
                • MemFree      
                • Buffers      
                • Cached       
                • SwapCached   
                • Active       
                • Inactive     
                • HighTotal    
                • HighFree     
                • LowTotal     
                • LowFree      
                • SwapTotal    
                • SwapFree     
                • Dirty        
                • Writeback    
                •Mapped        
                • Slab         
                • CommitLimit  
                • Committed_AS 
                • PageTables   
                • VmallocTotal 
                • VmallocUsed 
                • VmallocChunk |
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.

![Notifications Form](image)

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 11-2: Expert > Notifications Form Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Alarm for Data Buffering</td>
<td>Enable by placing a check mark in this field.</td>
</tr>
<tr>
<td>[unlabeled view table]</td>
<td>List of alarm types and triggers.</td>
</tr>
<tr>
<td>[unlabeled dropdown list]</td>
<td>Email, Pager, or SNMP Notification methods.</td>
</tr>
</tbody>
</table>

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, see one of the following sections of this chapter:
   - 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.

![Figure 11-3: Expert > Administration > Notifications > Email > Add/Edit Dialog box](image)

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

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 11-3: Expert > Email Notifications Dialog Box Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alarm Trigger</strong></td>
<td>The trigger expression used to generate an alarm.</td>
</tr>
<tr>
<td>[untitled dropdown field]</td>
<td>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.</td>
</tr>
<tr>
<td><strong>To/From/Subject/Body</strong></td>
<td>The email for the designated recipient of the alarm notification.</td>
</tr>
<tr>
<td><strong>SMTP Server IP</strong></td>
<td>The IP address of the SMTP server.</td>
</tr>
<tr>
<td><strong>SMTP Port</strong></td>
<td>The port used by the SMTP server.</td>
</tr>
</tbody>
</table>

**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.

**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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Trigger</td>
<td>The trigger expression used to generate an alarm.</td>
</tr>
</tbody>
</table>
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.

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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Trigger</td>
<td>The trigger expression used to generate an SNMP trap.</td>
</tr>
<tr>
<td>[untitled dropdown field]</td>
<td>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.</td>
</tr>
<tr>
<td>OID Type Value</td>
<td>The value that uniquely identifies an object to the SNMP agent.</td>
</tr>
<tr>
<td>Trap Number</td>
<td>The trap type defined in the Management Information Base (MIB). The choices are:</td>
</tr>
<tr>
<td></td>
<td>• Cold Start</td>
</tr>
<tr>
<td></td>
<td>• Warm Start</td>
</tr>
<tr>
<td></td>
<td>• Link Down</td>
</tr>
<tr>
<td></td>
<td>• Link Up</td>
</tr>
<tr>
<td></td>
<td>• Authentication Failure</td>
</tr>
<tr>
<td></td>
<td>• EGP Neighbor Loss</td>
</tr>
<tr>
<td></td>
<td>• Enterprise Specific</td>
</tr>
<tr>
<td>Community</td>
<td>The password used to authenticate the traps.</td>
</tr>
<tr>
<td>Server</td>
<td>The IP address of the server running the SNMP.</td>
</tr>
<tr>
<td>Body</td>
<td>The content of the notification.</td>
</tr>
</tbody>
</table>

**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 257.
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.

Figure 11-6: Expert > Administration > Time/Date

You can use the Time/Date form in Expert mode to set the CPS’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 CPS’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.

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 time zone from the “Timezone” pull-down list.
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 time zone from the “Timezone” pull-down list.
   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.

Figure 11-8: Expert > Administration > Boot Configuration

Boot configuration defines the location from where CPS loads the operating system. The CPS can boot from its internal firmware or from the network. By default, CPS 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 CPS boot image file must be downloaded from APC and available on the TFTP or BOOTP server.
- CPS 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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address assigned to Ethernet</td>
<td>A fixed IP address or a DHCP assigned IP address to the CPS unit.</td>
</tr>
</tbody>
</table>
### Field Name | Definition
---|---
**Watchdog Timer** | Whether the watchdog timer is active or Inactive. If the watchdog timer is active, the CPS reboots if the software crashes.
**Unit boot from** | Specify whether to boot CPS 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)
- 100BaseT Half-Duplex
- 100BaseT Full-Duplex
- 10BaseT Half-Duplex
- 10BaseT Full-Duplex
**Fast Ethernet Max. Interrupt Events** | The maximum number of packets that the CPU handles before an interrupt (0 is the default).

### To Configure CPS Boot

1. Go to Administration > Boot Configuration in Expert mode.
   
The Boot Configuration form appears.
2. Enter the IP address of the CPS 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 CPS.
   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.

![Backup Config Form](image)

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 CPS configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from CPS 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>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP</td>
<td>IP address of an FTP server on the same subnet as the CPS. (Verify accessibility by pinging the FTP server.)</td>
</tr>
</tbody>
</table>
When “Storage Device” is selected from the “Type” pull-down menu, the following form appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path and Filename</td>
<td>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 <em>VCPS_v2.6.0.bin</em> in a directory called “/upload” on the FTP server, you would enter the following in the “Path and Filename” field: <code>/upload/VCPS_v2.6.0.bin</code></td>
</tr>
<tr>
<td>Username and Password</td>
<td>Obtain the username and password to use from the FTP server’s administrator.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the configuration</td>
</tr>
<tr>
<td>Load</td>
<td>Downloads a previously saved copy of the configuration file from the selected device.</td>
</tr>
</tbody>
</table>

When “Storage Device” is selected from the “Type” pull-down menu, the following form appears.

![Figure 11-10: Expert > Administration > Backup Config > Storage Device](image)

The following table describes the available fields when “Storage Device” is selected from the “Type” drop-down menu.
Table 11-4: Expert > Backup Config Type Storage Device Form

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Configuration</td>
<td>The system saves the configuration in the storage device but does not override the internal flash configuration after reboot.</td>
</tr>
<tr>
<td>Replace Configuration</td>
<td>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.</td>
</tr>
</tbody>
</table>

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/<filename>.
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.
2. Select “Storage Device” from the “Type” pull-down menu.
3. To backup a copy of the current configuration files, select “Default Configuration” and press the “Save” button.
4. To restore a copy of the configuration files saved on the storage device without replacing the internal flash configuration, select “Default Configuration” and press the “Load” button.
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.

![Upgrade Firmware Form](image)

**Figure 11-11:** Expert > Administration > Upgrade Firmware

You can use this form to configure an automated upgrade of the CPS’s firmware which includes the Kernel, applications, and configuration files. To upgrade firmware, see the APC Software/Firmware downloads Web page, www.apc.com/tools/download/. Use the product selection menu to find the Console Port Server firmware.

**Note:** Check the file name for the upgrade version and read the upgrade instructions carefully. Distinct procedures are required depending on the version from which you are upgrading.
The following table describes the fields in the “Upgrade Firmware” form.

**Table 11-5: Expert > Upgrade Firmware Form Fields**

<table>
<thead>
<tr>
<th>Field/Menu Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>FTP is the only supported type.</td>
</tr>
<tr>
<td><strong>Firmware Download Site</strong></td>
<td>New firmware for the APC Console Port Server can be located on the APC firmware download page, <a href="http://www.apc.com/tools/download/">www.apc.com/tools/download/</a></td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Username recognized by the FTP server. The APC FTP username for download is “anonymous”</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password associated with the username. You can use any password for “anonymous” login in the password field.</td>
</tr>
<tr>
<td><strong>Pathname and File Name</strong></td>
<td>Firmware downloads are accessible from the APC Web site, <a href="http://www.apc.com/tools/download/">www.apc.com/tools/download/</a>. An example of the firmware filename might be: APC-AP9301-Linux V_2.6.0a</td>
</tr>
<tr>
<td><strong>Run Checksum</strong></td>
<td>Runs the checksum program to verify the accuracy of the uploaded data.</td>
</tr>
</tbody>
</table>

**To Upgrade the Firmware of the CPS**

This procedure is for upgrading the latest release of the CPS’s firmware. The upgrade installs the software on the flash memory.

2. Using the Filter by Software/Firmware pulldown, select **Firmware Upgrades - APC Console Port Server**, then click the Submit button. The following figure shows the APC downloads main page and the pulldown menu.
3. Select the firmware revision to download and press Continue.

4. Choose one of the file types you wish to download (typically .bin or .MD5) and press Continue for that type.

**Note:** If you are registered to download software, click on Login to go to the Download page. If you are not registered, click on the Register to Download button, fill out and Submit the online form, then login for the Download page.

5. From the Download page, click the Download Now button and choose the FTP server where you would like the file to reside locally.

6. From the CPS screen Administration > Upgrade Firmware, choose FTP from the Type menu. (FTP is the only supported type).

7. Enter the URL of the server in the “FTP Site” field.
   The APC address is: Enter the username recognized by the FTP server in the “Username” field.
   The APC username for firmware downloads is “anonymous.”
8. Enter the password associated with the username on the FTP server in the “Password” field.

   The APC interface accepts any password for “anonymous” login.

9. Search for and select the desired firmware revision you downloaded.

10. Click the “Upgrade Now” button.

11. Click “cancel changes” if you need to restore the backed-up configuration files.

**Reboot**

Selecting Administration > Reboot in Expert mode opens the following form.

![Diagram of Expert > Administration > Reboot form]

**Figure 11-13:** Expert > Administration > Reboot

Clicking the “Reboot” button reboots the CPS.

**To Reboot the CPS**

1. Go to Administration > Reboot in Expert mode.

2. Click the “Reboot” button. A confirmation dialog box appears.

3. Click OK.
Online Help

Selecting Administration > Online Help in Expert mode opens the following form.

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 CPS administrator can download the online help, and reconfigure the path to a local server where the online help can be stored. The CPS 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. In the CPS Web Manager, navigate to Administration > Online Help in Expert mode. See the preceding figure.

2. In the “Online Help Path” field, configure the path to: http://www.apc.com/search/
## Appendix A: Technical Specifications

The following table lists the Console Port Server hardware specifications:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>MPC855T (PowerPC Dual-CPU)</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>128MB DIMM SDRAM / 16MB CompactFlash</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>1 Ethernet 10/100BT on RJ45</td>
</tr>
<tr>
<td></td>
<td>1 RS232 Console on RJ45</td>
</tr>
<tr>
<td></td>
<td>RS232 Serial Ports on RJ45</td>
</tr>
<tr>
<td></td>
<td>PCMCIA slots (Model AP9303 only) supporting: Secondary Ethernet, Wireless networking, CDMA, GPRS, GSM, V.90 modems, ISDN.</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>Internal 100-240VAC, 50/60 Hz</td>
</tr>
<tr>
<td></td>
<td>Optional Dual entry, redundant power supplies†</td>
</tr>
<tr>
<td><strong>Operating Temperature</strong></td>
<td>50°F to 112°F (10°C to 44°C)</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>-40°F to 185°F (-40°C to 85°C)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>5% to 90% non-condensating</td>
</tr>
<tr>
<td><strong>Dimensions CPS 8-32</strong></td>
<td>17 x 8.5 x 1.75 in (43.18 x 21.59 x 4.45 cm)</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td>FCC Part 15, A</td>
</tr>
<tr>
<td></td>
<td>EN55022, A (CE)</td>
</tr>
<tr>
<td></td>
<td>EN55024</td>
</tr>
<tr>
<td></td>
<td>UL 1950</td>
</tr>
<tr>
<td></td>
<td>Solaris Ready™</td>
</tr>
</tbody>
</table>
Appendix B: Safety, Regulatory, and Compliance Information

The following Safety Information for Console Port Server is described in this appendix.

| Safety Guidelines for Rack-Mounting the CPS | page 280 |
| Safety Precautions for Operating the CPS     | page 281 |
| Working inside the CPS                       | page 282 |
| Replacing the Battery                       | page 283 |
| FCC Warning Statement                        | page 283 |
| Notice About FCC Compliance for all Console Port Server Models | page 284 |
| Canadian DOC Notice                          | page 284 |
| Aviso de Precaución S-Mark Argentina         | page 284 |
| Trabajar dentro del Console Port Server      | page 285 |
| Batería                                      | page 285 |

Safety Guidelines for Rack-Mounting the CPS

The following considerations should be taken into account when rack-mounting the Console Port Server.

**Temperature**

The manufacturer's maximum recommended ambient temperature for the Console Port Server is 122°F (50°C).

**Elevated Operating Ambient Temperature**

If the CPS 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 Console Port Server**

Please read all the following safety guidelines to protect yourself and your Console Port Server.

---

**Caution:** Do not operate your Console Port Server with the cover removed.

---

**Caution:** To avoid shorting out your Console Port 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 Console Port 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 Console Port 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 CPS and that they are not located where they can be stepped on or tripped over. Do not spill food or liquids on CPS.

**Caution:** Do not push any objects through the openings of the Console Port Server. Doing so can cause fire or electric shock by shorting out interior components.

**Caution:** Keep your Console Port Server away from heat sources and do not block host’s cooling vents.

**Working Inside the Console Port Server**

Do not attempt to service the CPS yourself, except when following instructions from APC Customer Support personnel. In the latter case, first take the following precautions:

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

**Electrostatic Discharge (ESD) Precautions**

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

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

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

**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.

**Attention!:** All y a risque d’explosion si la batterie est remplacée par une batterie de type incorrect. Mettre au rebut les batteries usagées conformément aux instructions.

**FCC Warning Statement**

The Console Port 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 Console Port Server Models

To comply with FCC standards, the Console Port 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 Console Port 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’Console Port Server n’émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectrique edicté par le Ministère des Communications du Canada.

Aviso de Precaución S-Mark Argentina

Por favor de leer todos los avisos de precaución como medida preventiva para el operador y el Console Port Server.

**Caution:** No hacer funcionar el Console Port Server con la tapa abierta.

**Caution:** Para prevenir un corto circuito en el Console Port 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 Console Port Server de fluctuaciones en corriente eléctrica, utilice una fuente eléctrica de respaldo. Asegurarse de que nada descanso sobre los cables del Console Port Server, y que los cables no obstruyan el paso. Asegurarse de no dejar caer alimentos o bebidas en el APC.
No intente dar servicio al Console Port Server, solo que este bajo la dirección de Soporte Técnico de APC. Si este es el caso, tome las siguientes precauciones:

Apague el Console Port Server. Asegúrese 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.
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**
Chips on the motherboard of a computer containing read-only data.

**BIOS**
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. APC products run the Linux operating system, and most APC products provide CLI access. Administrators type “CLI” on the command line of the Linux shell. The APC 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 two or more parts separated by dots; on the left is the most specific, and 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.
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

When the management data in a computer network 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. For IPV4 (Internet Protocol Version 4), it belongs to one of five classes (A-E) and is expressed as four 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 trustworthiness 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, electromagnetic 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 is 1500 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 ACS 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 1980s. 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 that 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

A

access 224
  allow SSH root 7, 65, 195
  root 296
  SSH root 99
access requirements, port 44
access server
  (CAS) profile, console 209
  (CAS), console 208, 288
access to connected devices
  configuring 18
  planning 17
accessing CPS 4
accessing the web manager, other methods of 36
action, boot 152
active ports sessions 182
add rule 12
adding
  a group 180
  a user 179
  users 35
admin 178
administering users 17
administrative modes, overview of 61
administrator forms, common features of 56
administrators, common tasks for CPS 54
administrators, web manager for 53
alarm
  notification 265
  notification, serial ports 265
  threshold 50, 106
  trigger 260
alarms 16
alias 251
alias, port IP 241
allow
  multiple sessions 233
  SSH root access 7, 65, 195
APC CPS, working inside the 282
applications menu & forms 97
assigning users 35
audience vii
authentication 8, 184, 286
  biometric 242
  for CPS logins, configuring 185
  methods 151, 226
  protocols 151
  serial port 7, 65, 195
  servers, configuring 185
authorization
  raccess 188
  user 189
authorized users/groups 224
authtype 185

B

backup configuration 271
banner, console 126
banner, login 242
basic installation procedures 27
battery, replacing 283
baud rate 75, 251, 286
bidirectional 211
bidirectional Telnet 208
bidirectionlogin timeout 225
bidirectionshell command 225
biometric authentication 242
BIOS 286
BogoMips 286
bonding 127, 286
boot action 152
boot configuration 268
boot, to configure CPS 269
bootp 268
box contents, shipping 23
brackets, mounting 24
break 252
break interval 242
break sequence 242
break signal 287
buffer size, syslog 230
buffering
  data 16, 228
  off-line data 294
buzzer 49, 106
bytes, RX 252
bytes, TX 251
channel 145
checksum 287
CLI 287
CLI, configuring ports for power management using 20
cluster 288
command line, power management 21
command, wiz 31
common features of administrator forms 56
common tasks for CPS administrators 54
community 155, 264, 288
compact flash 132
compact flash PCMCIA cards, configuring 143
configuration 109
  backup 271
  boot 268
  firewall 158
configuring
  access to connected devices 18
  authentication for CPS logins 185
  authentication servers 185
  CDMA PCMCIA cards 146
  compact flash PCMCIA cards 143
  CPS in Expert mode 89
  CPS in Wizard mode 64
  Ethernet PCMCIA cards 142
  GSM PCMCIA cards 139
  ISDN PCMCIA cards 137
  modem PCMCIA cards 135
  network parameters 31
  ports 35
  ports for power management 20
  ports for power management using CLI 20
C
cable, straight-thru 24
call back 135
Canadian doc notice 284
CAS
  console access server 208, 288
    profile, console access server 209
  CD, documentation 24
CDMA 4
CDMA PCMCIA cards, configuring 146
certification, NEBS 282
chain 10
power management 20
wireless LAN PCMCIA cards 144
connect 42, 98
connect to CPS 42
connect to serial ports 44
connect, host to 242
connecting CPS PM rPDUs 38
connecting servers to CPS 29
connection
  protocol 44, 75
  protocol modem 212
  protocol power management 212
  protocols terminal server (TS) profile 209
connection name 151
connection profiles 208
connections, vpn 149
connectors on the APC Console Port Server 4
console 288
  access server CAS 208, 288
  access server CAS profile 209
  banner 126
  raw 209
  SSH 209
  Telnet 209
  TelnetSSH 209
contents, shipping box 23
CPS
  accessing 4
  administrators, common tasks for 54
  boot, to configure 269
  command line, power management from 21
  connect to 42
  connecting servers to 29
  connectors on the 4
  firmware, to upgrade 275
  in Expert mode, configuring 89
  in Wizard mode, configuring 64
  logins, configuring authentication for 185
  mounting 28
  packet filtering 10
  to reboot 277
  working inside the APC 282
CPS PM rPDUs, connecting 38
CPS, connectors on the 4
CPU usage 182
CSLIP 212
current 50, 106
custom, security profile 34, 64, 195

D
data buffering 16, 228
  Destination 83
  File Size 84
  Local files 84
  Mode 83
  NFS File Path 84
  off-line 294
  Remote server 84
  time stamp 84, 230
data size 75
data buffering events 258
default IPaddress 36
default, security profile 34, 64, 195
destination
  local 230
  port 13
  remote 230
detected maximum 106
DHCP 36, 54, 288
DNS server 127, 288
documentation CD 24
documents, related ix
domain name 127, 289
dynamic mode support 7, 65, 196

E
ejecting PCMCIA cards 148
email notification 260
email notifications 259
emergency management service (EMS) 242
EMS 242
EMS, emergency management service 242
EMS, windows 242
enabling ports 35
encrypted 145
escape sequence 289
ESSID 145
Ethernet 269, 289
Ethernet PCMCIA cards, configuring 142
events, data buffering 258
Expert mode 62
configuring CPS in 89
menus and forms mapping 91

F
facility numbers 17, 230
fallback mechanism 226
FCC compliance 284
FCC warning statement 283
file path, NFS 230
filtering, IP packet 290
filtering, structure of IP 10
firewall configuration 158
firmware, to upgrade the CPS’s 275
flash 269, 289
flow control 75, 289
forms
administration 253
applications 97
common features of administrator 56
mapping, Expert mode 91
network 124
regular user 41
security 177
fragments 12, 167
frame 252
FTP 8, 66, 196, 271, 290
FTP server, using 273
FTP site 275

G
gateway IP 127
group, adding 180
groups, users 177
GSM 4
GSM PCMCIA cards, configuring 139

H
hard disk, IDE 132
host name 126
host settings 125
host table 172
host to connect 242
hotkey 233
hotkeys x
hot-swap 290
http 7, 65, 195
http redirection to https 7, 65, 195
https 7, 65, 195

I
ICMP 8, 66, 196, 290
ICMP protocol 14
icons, power management 112
IDE 271
IDE hard disk 132
IDE timeout 242
identifiers (OID), object 293
info, view rPDUs 49, 105
input interface 12, 167
installation and configuration 22
installation procedures, basic 27
installing PCMCIA cards 37
inverted checkbox 162
IP
gateway 127
local 135, 246
packet filtering 290
primary 127
remote 135, 246
IP alias, port 241
IP filtering, structure of 10
IPAddress, default 36
IPMI key 236
IPMI power management 114
IPMI server 236
IPsec 8, 66, 196, 291
ISDN 4, 291
ISDN PCMCIA cards, configuring 137

J
Java plug-in 25
JCPU 183

K
keep-alive interval, TCP 242, 298
Kerberos 8, 192, 226, 291
Kerberos/local 8, 186, 226
Kerberosdownlocal 8, 186, 226
key, IPMI 236
key, power management 237
key, RSA 151

L
LDAP 8, 186, 226, 291
LDAP/local 8, 186, 226
LDAPdownlocal 9, 186, 226
local destination 230
local IP 135, 246
local port number 246
local TCP port number 246
local terminal 210
local/NIS 9, 186, 226
local/radius 9, 186, 226
local/TACACS+ 9, 186, 226
log level 168
log prefix 168
logging into the web manager 58
logging to syslog servers, prerequisites for 17
login banner 242
logins, configuring authentication for CPS 185
M

MAC 291
management information base (MIB) 153, 263
management, rPDU power 46
mapping, Expert mode menus and forms 91
masquerading 291
master 245
maximum detected 106
menu & forms
  administration 253
  applications 97
  network 124
  security 177
menus and forms mapping, Expert mode 91
methods of accessing the web manager, other 36
MIB 153, 263
  management information base 153, 263
MIIMON 127
mode
  Expert 62
  wizard 61
modem
  connection protocol 212
  PCMCIA cards, configuring 135
  RAS 208
moderate, security profile 6, 34, 64, 195
modes, overview of administrative 61
mounting brackets 24
mounting the CPS 28
MTU 127, 292
multi-outlet control, prerequisites for 112
multi-outlet ctrl, rPDU 50, 110
multiple sessions, allow 233
multi-user 232

N

navigation shortcuts x
NEBS 292
NEBS certification 282
network mask 127, 292
network menu & forms 124
network parameters, configuring 31
nexthop 151
NFS 293
NFS file path 230
NIS 9, 186, 227
NIS/local 9, 186, 227
NISdownlocal 9, 186, 227
notification
  alarm 265
  email 260
  pager 262
  serial ports alarm 265
  SNMP trap 264
notifications 16, 257
NTP 192, 266, 293
server, using 267
setting time and date 267
setting time and date with 267
number
  local TCP port 246
  remote TCP port 246
  trap 264
object identifiers (OID) 293
off-line data buffering 294
OID 155, 294
OID, object identifiers 293
Online Help 278
OOBI 294
open, security profile 6, 34, 64, 195
options for managing power 21
options, stty 242
options, TCP 168
other methods of accessing the web manager 36
outlets manager 47, 102
output interface 12, 167
over current protection 49, 106
overrun 252
overview of administrative modes 61

packet 294
packet filtering on CPS 10
packet filtering, IP 290
pager notification 262
parity 75, 252, 294
PCMCIA 294
PCMCIA cards
  configuring CDMA 146
  configuring compact flash 143
  configuring Ethernet 142
  configuring GSM 139
  configuring ISDN 137
  configuring modem 135
  configuring wireless LAN 144
  ejecting 148
  installing 37
  PCMCIA management 132
  PCPU 183
  PCPU processing time 182
physical ports 205
planning access to connected devices 17
plug-in, Java 25
PM rPDUs, connecting CPS 38
port 295
  destination 13
  powermgmt 236
  source 13
  TCP 241
port access requirements 44
port IP alias 241
port number
  local 246
  local TCP 246
  remote TCP 246
  TCP 45
ports
  configuring 35
  enabling 35
  for power management, configuring 20
  physical 205
  statistics 251
  status 250
  virtual 244
power management 18, 212
  configuring 20
  configuring ports for 20
  connection protocol 212
  from CPS command line 21
icons 112
IPMI 114
key 237
rPDU 46
through the web manager 21
using CLI, configuring ports for 20
power, options for managing 21
powermgmt port 236
ppp 135, 212, 295
ppp-no auth 212
pre-installation requirements 25
prerequisites for
logging to syslog servers 17
multi-outlet control 112
using the web manager 5, 54
pre-shared secret 151
primary IP 127
privilege users 233
product models and configurations 3
profiles
   connection 208
   security 194
   serial port settings and security 66,
   197
protocol 246
   authentication 151
   connection 44, 75
   ICMP 14
   modem connection 212
   power management connection 212
   terminal server (TS) profile connection 209
   UDP 13
pu interval 52
Q
quickstart guide 24
R
raccess 188
raccess authorization 188
Radius 9, 186, 227, 295
Radius/downlocal 186
Radius/local 9, 186, 227
Radiusdownlocal 9, 227
RAM 269
RAS 208
RAS, modem 208
raw socket 211
raw, console 209
reboot 277
reboot the CPS 277
record time stamp 230
regular user 178
regular user forms 41
regular users, web manager 39
related documents ix
remote destination 230
remote IP 135, 246
remote TCP port number 246
replacing the battery 283
requirements, port access 44
requirements, pre-installation 25
RISC 296
root 4, 6, 31
   access 296
   access, allow SSH 7, 65, 195
   access, SSH 99
routes, static 173
rPDU
    multi-outlet ctrl 50, 110
    power mgmt. 46
rPDUs info, view 49, 105
rPDUs, connecting CPS PM 38
RS232 signal 250
RSA key 151
rule, add 12
run checksum 275
RX bytes 252

security
    profile custom 34, 64, 195
    profile default 34, 64, 195
    profile moderate 6, 34, 64, 195
    profile open 6, 34, 64, 195
    profile secured 6, 34, 64, 195
    profile, selecting 34
security advisory 59, 68
security menu & forms 177
security profiles 194
security profiles, and serial port settings 66, 197
selecting a security profile 34
serial port authentication 7, 65, 195
serial port settings and security profiles 66, 197
serial ports alarm notification 265
serial ports, connect to 44
servers, syslog 16
sessions, active ports 182
sessions, allow multiple 233
set the time and date 267
setting time and date with NTP 267
settings, host 125
shell 79
shipping box contents 23
shortcuts, navigation x
simple network management protocol (SNMP) 153
slave 245
SLIP 212
SMS 262
SMTP 260, 296
sniff mode 233
SNMP 7, 16, 65, 153, 196
SNMP trap notification 264
SNMP trap notifications 263
SNMP traps 297
SNMP, simple network management protocol 153
SNMPv1 263
SNMPv2 263
SSH (secure shell) 297
SSH root access 99
SSH root access, allow 7, 65, 195
SSH, console 209
SSH, secure shell 296
SSHv1 7, 64, 195, 210
SSHv2 7, 64, 195, 210
static routes 173
statistics, ports 251
status, ports 250
stop bit 297
stop bits 75
storage device 271
storage device, using 273
straight-thru cable 24
structure of IP filtering 10
stty 297
stty options 242
subnet 151
subnet mask 297
swapcached 256
syscontact 155
syslocation 155
syslog 49, 106, 130
  buffer size 230
  server 230
  servers 16
  servers, prerequisites for logging 17
system information 255
system information, to view 257

table, host 172
table, routing 296
TACACS 298
TACACS+ 186, 227, 298
TACACS+/downlocal 186
TACACS+/local 9, 186, 227
TACACS+downlocal 9, 227
TCP
  flags 13, 164
  keep-alive interval 242, 298
  options 168
  port 241
  port number, local 246
  port number, remote 246
  port numbers 45
  sequence 168
  Telnet 6, 64, 195, 210, 298
  Telnet, bidirectional 208, 211, 214
  Telnet, console 209
  TelnetSSH, console 209
  temperature 106
terminal profile menu 121
terminal server 299
terminal server (TS) 208
terminal server (TS) profile connection protocols 209
terminal type 242
terminial, local 210
TFTP 268
time/date 266
timer, watchdog 269, 299
to configure CPS boot 269
to reboot the CPS 277
to set the time and date 267
to upgrade the CPS’s firmware 275
to view system information 257
trap notification, SNMP 264
  trap number 264
  traps, SNMP 297
  trigger, alarm 260
TS profile connection protocols, terminal server 209
TS, terminal server 208
TTY 183, 299
TX bytes 251

U

UDP 299
UDP protocol 13
updelay 127
upgrade
   CPS’s firmware 275
   firmware 274
usage, CPU 182
user
   adding 179
   multi 232
   regular 178
user authorization 189
user forms, regular 41
users
   adding 35
   administering 17
   assigning 35
   privilege 233
   types of 6
users and groups 177
users manager 107
users/groups, authorized 224
using a storage device 273
using an FTP server 273
using an NTP server 267
using the web manager, prerequisites for 5, 54

W
watchdog timer 269, 299
web manager 5
   logging into 58
   other methods of accessing 36
   power management 21
   prerequisites for using 5, 54
web manager for administrators 53
web manager for regular users 39
windows EMS 242
wireless LAN PCMCIA cards, configuring 144
wiz command 31
wizard mode 61
Wizard mode, configuring CPS in 64
working inside the APC CPS 282

V
view rPDUs info 49, 105
view system information 257
virtual 203
virtual ports 244
vpn 10, 299
vpn connections 149