APC®

www.apc.com

APC 16-port IP KVM Installation, Administration, and User’s Guide

Software Version 2.0

APC Corporation
132 Fairgrounds Road
W. Kingston , RI 02892
1.800-788-2208
http://www.apc.com
Release Date: July 2007
Part Number: 990-2881A

Contents

Chapter 2: Installation 53

Chapter 3: Advanced Installation Procedures 93

Chapter 4: Web Manager for Administrators 101

Before You Begin

This installation, administration, and user’s guide provides background information and procedures for installing, configuring, and administering the following products:

- APC 16-port IP KVM
- APC CAT5/IP KVM Console Extender
- APC KVM Server Modules

In addition, this guide offers information and procedures for accessing connected servers and other connected devices.

Audience

This manual is intended for installers and system administrators of the APC 16-port IP KVM and for users who may be authorized to connect to devices and to manage power through the APC 16-port IP KVM.

This document describes configuration, administration, and use of the APC 16-port IP KVM and APC CAT5/IP KVM Console Extender. It does not describe how to set up and administer other external services or servers that the APC 16-port IP KVM may access for authentication, system logging, SNMP notifications, data logging, file sharing, or other purposes. This document assumes that users who are authorized to connect to servers and other devices through the APC 16-port IP KVM already know how to use the connected devices.

Document Organization

This document contains the following chapters:

Chapter 1: Introduction	Defines and explains the overall product features and uses of the APC 16-port IP KVM.
Chapter 2: Installation	Explains the procedures for installing the APC 16-port IP KVM and setting up its basic configuration.
Chapter 3: Advanced Installation Procedures	Explains the procedures for installing APC CAT5/IP KVM Console Extender in addition to explaining how to install, an external modem, an APC rPDU and how to cascade KVM units to the APC 16-port IP KVM.
Chapter 4: Web Manager for Administrators	Explains how to use the Web Manager, highlighting such procedures as how to configure the APC 16-port IP KVM, add or delete users, define user access, add or delete server connections, and other topics pertaining to APC 16-port IP KVM administration.
Chapter 5: Web Manager for Regular Users	Presents the procedures for connecting to a port and other operations related to using the web user interface.
Chapter 6: Accessing Connected Devices	Explains how to connect to KVM ports and in-band servers and how to use the Remote Viewer and control KVM connection sessions.
Chapter 7: On Screen Display	Describes how to use the On Screen display for local connections to the User 1 port.
Glossary	Glossary of terms and acronyms used in the manual.

Typographic and Other Conventions

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

Table iii-1: Typographic Conventions

Typeface	Meaning	Example
Links	Hypertext links or URLs	Go to: http://www.apc.com
Emphasis	Titles or emphasized or new words or terms	A *Generic User* account has a default set of permissions that apply to all regular users and groups.
`Filename or Command`	Names of commands, files, and directories; onscreen computer output.	Edit the `pslave.conf` file.
`User type`	What you type in an example, compared to what the computer displays	[kvm #] **`ifconfig eth0`**

The following table describes other terms and conventions.

Table iii-2: Other Terms and Conventions

Term or Convention	Meaning	Examples
Hot keys	When hot keys are shown, a plus (+) appears between two keys that must be pressed at the same time, and a space appears between two keys that must be pressed sequentially.	`Ctrl+k p` entered while the user is connected to a KVM port brings up an rPDU power management screen. `Ctrl` and `k` must be pressed at the same time followed by `p`.

Table iii-2: Other Terms and Conventions

Term or Convention	Meaning	Examples
Navigation shortcuts	Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager forms or OSD screens.	Go to Configuration>KVM> General >User 1 in Expert mode.

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - www.apc.com (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - www.apc.com/support/

    Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to www.apc.com/support/contact for contact information.
- Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Chapter 1
Introduction

This chapter gives an overview of the features of the APC 16-port IP KVM. This chapter describes how administrators and operators can use the 16-port IP KVM features to securely manage connected computer systems and a large variety of devices from anywhere on the local area network or on the Internet. This chapter also provides important prerequisite information for understanding the information and procedures in the rest of this manual.

Description

The 16-port IP KVM is a 1U rack-mountble device that serves as a single access point for administering and using servers and other devices through in-band and out-of-band access methods.

You use the KVM ports on the 16-port IP KVM to connect servers. You can use the AUX port on the right back to connect APC rPDUs or an optional external modem. You use the management ports on the right back to connect to the 16-port IP KVM and to its connected devices.

16-port IP KVM administrators and users who are authorized to access connected devices can connect locally or remotely from LANs, WANs, or other dial-in connections through the Ethernet port or through an optional external modem.

Secondary KVM units such as another 16-port IP KVM can be cascaded for extended KVM server connections. A maximum of 16 secondary KVM devices can be cascaded from the primary 16-port IP KVM extending the number of KVM ports to a maximum of 128 for two-user configuration (i.e. two connections to each cascaded device), or 256 for a one-user configuration.

Access to the 16-port IP KVM for administration is separate from access to connected devices. Only the 16-port IP KVM administrator can configure access to the 16-port IP KVM and to the connected devices.

Both 16-port IP KVM administrators and users authorized to access connected devices can use the Web Manager from a browser. Authorized users can log on to devices, manage power, and change their own passwords, but they do not have access to the 16-port IP KVM screens for configuring users or ports.

All logins to the 16-port IP KVM are subject to authentication. The 16-port IP KVM administrator can restrict access to each of the connected devices by choosing among authentication methods for logins to the 16-port IP KVM and to its ports. Authentication can be local to the 16-port IP KVM or through an authentication server.

The 16-port IP KVM administrator can further control access by controlling which ports are assigned to each user name.

The 16-port IP KVM administrator can configure event logging, alarms, and notifications, set up encryption, and data buffering.

After initial network configuration is performed on the 16-port IP KVM, the APC Web Manager provides a real-time view of all the connected equipment and makes it possible for administration to be done from a browser on any computer on site or on the Internet.

Guidelines for Using the 16-port IP KVM

Configuration of user accounts and access to the ports and all other management of the connected devices is done through the Web Manager.

Troubleshooting in the event of network failure can be done using one of the two direct-connect methods, or by using the Web Manager through a dial-up connection to an external modem connected to the AUX port.

See “Accessing Connected Devices” on page 253 for instructions on how users without 16-port IP KVM administration privileges can access computers and APC rPDUs that are connected to the 16-port IP KVM.

Connectors on the 16-port IP KVM

The following sections describe the connectors on the back of the 16-port IP KVM, including ports and plugs.

Types of Ports

The 16-port IP KVM's ports include KVM ports, which support server connections, an AUX port, and management ports including the User 1, User 2, Console, and Ethernet ports, as described in the following table.

Table 1-1: Port Types

Port Type	Connection Information	Where Documented
KVM	Connect an RJ-45 CAT5 cable to a Server Module, which is connected to a PC with a USB or a PS/2 connector or a Sun server with a USB connector.	• "KVM Ports" on page 7 • "To Connect Computers to KVM Ports" on page 60
AUX	Connect an RJ-45 to RJ-12 cable to an APC rPDU, or connect an RJ-45 to RJ-45 cable to external modem.	• "AUX Port" on page 10 • "To Connect an APC rPDU to the AUX Port" on page 95 • "To Connect an External Modem to the AUX Port" on page 94
Console	Connect a CAT-5 RJ-45 to DB-9 cable to a COM port on a computer.	• "Management Ports (Console, Ethernet, User 1, User 2)" on page 8 • "To Connect to the Console Port" on page 63
Ethernet	Connect an Ethernet cable to the local area network (LAN).	• "Management Ports (Console, Ethernet, User 1, User 2)" on page 8 • "To Make an Ethernet Connection" on page 57
User 1 [PS/2 and VGA]	Connect a keyboard, video, mouse cable to a local station's keyboard, monitor, and mouse.	• "Management Ports (Console, Ethernet, User 1, User 2)" on page 8 • "To Connect to the User 1 Management Port" on page 64

Table 1-1: Port Types (Continued)

Port Type	Connection Information	Where Documented
User 2	Connect an RJ-45 cable of up to 500 feet to an APC CAT5/IP KVM Console Extender (AP5410) can be purchased separately. **Note:** The 500-foot limit includes the distance of the User 2 from the 16-port IP KVM and the distance of the most remote system connected to a KVM port.	• “Management Ports (Console, Ethernet, User 1, User 2)” on page 8 • “Installing the APC CAT5/IP KVM Console Extender” on page 97 • “To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM” on page 98

Connectors on the Back

The back of the 16-port IP KVM has KVM and management ports, a power cord connector, a power switch, and an AUX ports as illustrated in the following figure.

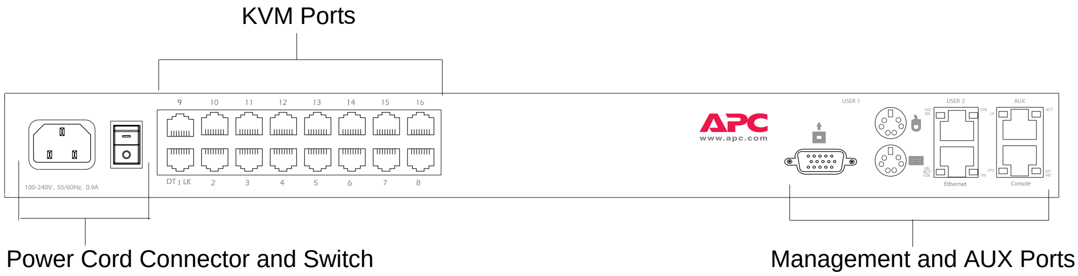


Figure 1-1:16-port IP KVM Back Panel

- On the left are the power connector, power switch, and 16 ports, which are used for connecting computing systems with KVM connections.

  See “Power Connector and Power Switch” on page 7 and “KVM Ports” on page 7.
- On the right is the AUX port, which is used to connect to rPDUs or an external modem, and the management ports, which are used for local management of the 16-port IP KVM.

  See “Management Ports (Console, Ethernet, User 1, User 2)” on page 8 and “AUX Port” on page 10.

Power Connector and Power Switch

The following figure shows the power connector and power switch on the left rear of a 16-port IP KVM.

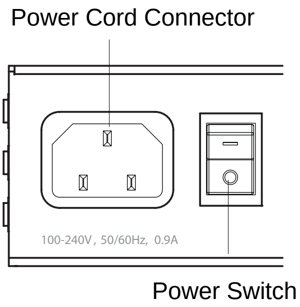


Figure 1-2: Power Connector and KVM Server Ports on the Left Rear

The 16-port IP KVM is furnished with a power cord used to connect the power connector to a power supply.

See “To Power On the 16-port IP KVM” on page 64 for instructions on supplying power to the 16-port IP KVM.

KVM Ports

The following figure shows KVM (keyboard, video, mouse) ports on the rear of the 16-port IP KVM.

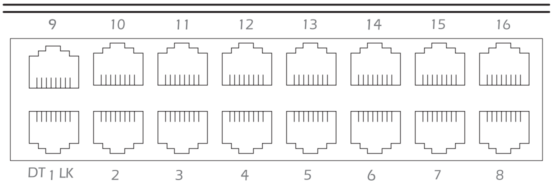


Figure 1-3:KVM Ports on the Rear

KVM ports provide remote access to the keyboard, monitor, and mouse of PCs with USB or PS/2 connectors or Sun servers with USB connectors. Connecting a computer to a KVM port allows use of a keyboard, video, and mouse of a remote station as if it were the keyboard video and mouse on the connected computer. KVM port connections, also called out-of-band connections give access to information that is otherwise inaccessible through in-band network interfaces.

For example, BIOS access, POST, and boot messages are inaccessible through in-band connections. In some cases, the in-band network interfaces are not available after the system boot is completed (for example, after a Windows Safe Mode boot) without the kind of access these KVM connections provide.

Each connected computing system is identified in the management software by the port number to which it is connected. The administrator can assign a descriptive alias to each port to identify the connected computer. For example, if a Sun E10K server is connected to port 3, the administrator might define the port's alias to be "Sun E10K."

Customers order one of three Server Module types for connecting each KVM port to a computer. See "KVM Server Module Usage and Types" on page 50 for more details.

See "To Connect Computers to KVM Ports" on page 60 for instructions on connecting servers to KVM ports.

Management Ports (Console, Ethernet, User 1, User 2)

The following figure shows the management ports on the right back of the 16-port IP KVM.

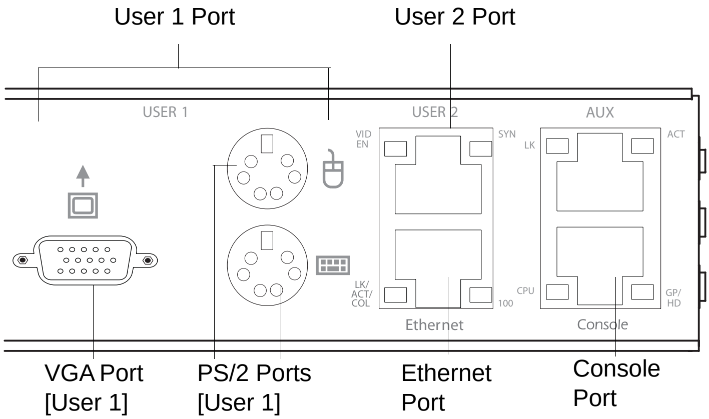


Figure 1-4: Management Ports

The following list describes the management ports on the right back of the 16-port IP KVM.

- **Console** – Its RJ-45 connection can be connected by a CAT5 to DB-9 cable to a COM port on a computer. Administrators can use a terminal emulation program to locally manage and troubleshoot the 16-port IP KVM. See “To Connect to the Console Port” on page 63 and “Configuring Basic Networking Using the wiz Command” on page 66 for more details.
- **Ethernet** – Use the Ethernet management port for connecting an Ethernet cable for Intranet and Internet access. See “Making an Ethernet Connection” on page 57 for instructions if needed.
- **User 1** – The User 1 port includes two PS/2 ports and a VGA port, which can be connected to a mouse, keyboard, and monitor. Once a local system is connected to the User 1 port, administrators can use the OSD (On Screen Display) interface to locally manage and use the 16-port IP KVM. See “To Connect to the User 1 Management Port” on page 64 and Chapter 7: On Screen Display for more details.
- **User 2** – This port is used for extending the local administration by connecting an RJ-45 cable of up to 500 feet to an APC CAT5/IP KVM Console Extender. The Console Extender can be ordered separately. Administrators can use the OSD (On Screen Display) to locally manage and use the 16-port IP KVM without being in the same room as the 16-port IP KVM. See “Installing the APC CAT5/IP KVM Console Extender” on

page 97 and “Controlling the OSD Through the APC CAT5/IP KVM Console Extender” on page 366 for more details.

AUX Port

The following figure shows the AUX ports on the right back of the 16-port IP KVM.

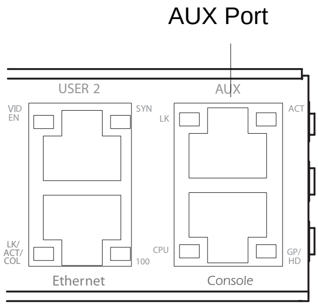


Figure 1-5: Management Ports

AUX – Its RJ45 connector can be used for the following:

- Connecting to an optional APC rPDU

  See “Connecting APC rPDUs to the 16-port IP KVM” on page 95 for installation instructions.

- Connecting to an optional external modem

  See “Connecting an External Modem” on page 94

Activity LEDs on the Back of the 16-port IP KVM

The 16-port IP KVM comes with paired LEDs positioned on each side of the following ports:

- User 2
- AUX
- Ethernet
- Console

The following figure shows the position of the LEDs as they appear on the back of the 16-port IP KVM. The LEDs are designed to monitor the interface connections as described in Table 1-2, “LED Descriptions,” on page 12.

The diagram below shows a close up view of the LEDs on the back of the 16-port IP KVM. The LEDS monitor the AUX ports, ETHERNET, and CONSOLE ports as described in Table 1-2.

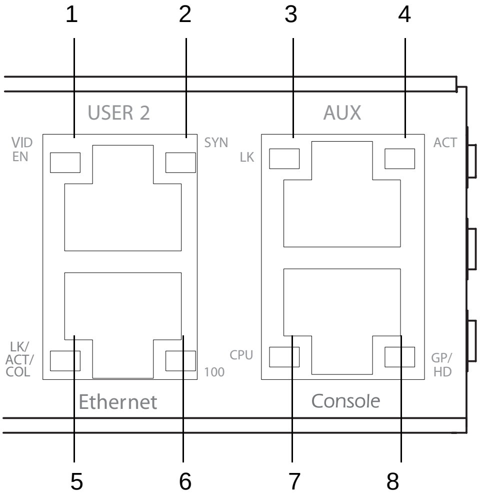


Figure 1-6:LEDs on the 16-port IP KVM Management Ports

The LED numbers in the tables below correspond to the numbers in the previous figure.

Table 1-2: LED Descriptions

Number	Label	Function	Color/Status
1	VID EN	Monitor KVM CAT5 video interface	Orange – Lights when video is enabled
2	SYN	Monitor KVM CAT5 video interface	Yellow – Lights when KVM input is being transmitted through one or more KVM ports.
5, 3	LK	Monitor RS-232 async port status	• OFF – Indicates the port is not open. • Orange – Lights when DTR (data terminal ready) signal is on (when the port is open).
4, 5	ACT	Monitor RS-232 async activity	• OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).
5	LK/ ACT/ COL	Monitor Ethernet line status	• OFF – Indicates either link is not up or cable is not connected. • Green – Lights solid when the link is up and blinks when data activity occurs, with frequency proportional to traffic. • Orange – Blinks when collisions occur
6	100	Monitor Ethernet speed	• Off – Indicates the link is 10baseT or no link is active. • Green – Steady when 100baseT link is active.

Table 1-2: LED Descriptions (Continued)

Number	Label	Function	Color/Status
7	CPU	Monitor CPU (software operation)	• Off or solid green – During boot and if software crashes. • Green – Blinks when software is operating normally. If software crashes, light stops blinking, and if the Watchdog timer is active, the 16-port CAT5 KVM reboots.
8	GP/ HD	Monitor compact flash (HD) or other (GP)	Not implemented.

Ordering Options

The following table list the part numbers of the KVM units and the related products.

Table 1-3: Ordering Options

Part Number	Description
AP5401	APC 16-Port CAT5 Analog KVM
AP5405	APC 16-Port IP KVM
AP5410	APC CAT5/IP KVM Console Extender
AP5460	APC CAT5/IP KVM PS/2 Server Module (SM)
AP5461	APC CAT5/IP KVM PC/Sun USB Server Module (SM)
AP5462	APC CAT5/IP KVM Sun Server Module (SM)
AP9317	APC KVM to APC Switched Rack PDU RJ45 to RJ12 Cable

Types of Users

The 16-port IP KVM support three types of users:

- Predefined administrators who can administer the 16-port IP KVM and its connected devices
- Optionally added users who can act as administrators of the 16-port IP KVM and its connected devices
- Optionally added users who can act as administrators of connected devices or regular users.

As summarized in the following table, two accounts, root and admin, are configured by default and cannot be deleted. The default “apc” account can add regular user accounts to allow other users to act as administrators of connected devices. An administrator can also choose to add regular users to the “admin” group, which enables the regular users to perform 16-port IP KVM administrative functions. The following table lists the responsibilities of each type of user and provides the default password for each.

Table 1-4: User Types, Responsibilities, and Default Password

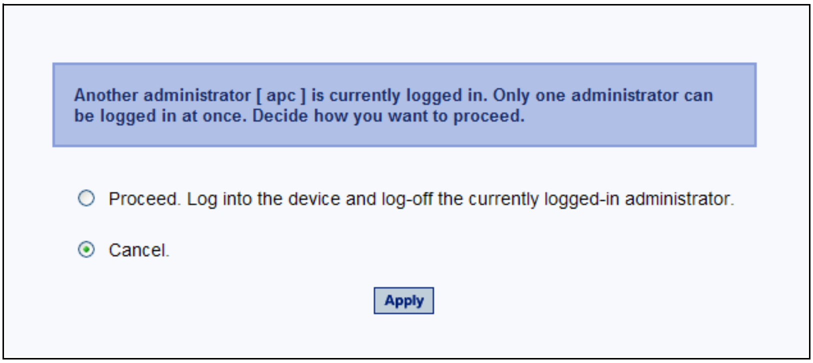
User Name	Responsibilities	Default Password
root	Cannot be deleted. Only console logins allowed. Runs the `wiz` command to do initial network configuration, as described in “Configuring Basic Networking Using the wiz Command” on page 66. Access Privileges: Full Read/Write/Delete.	apc
apc	Cannot be deleted. Has all access: through the Web Manager in Wizard and Expert mode, and through the OSD. Has full access to every function of the Web Manager. Access Privileges: Full Read/Write/Delete.	apc

Table 1-4: User Types, Responsibilities, and Default Password (Continued)

User Name	Responsibilities	Default Password
administratively assigned	User account configured by the administrator to be able to access devices connected to the ports of the 16-port IP KVM. Has access to the port through the Web Manager and through the OSD. Regular users can access and administer only devices that are connected to ports to which they are assigned. Default Access Privileges for generic users: Read/Write only for all ports. Administrators can restrict access for individual users to Read only to specific ports. If an administrator assigns a regular user to the “admin” group, that user can also perform the same administrative functions on the Web Manager as the “apc” user, as described above.	administratively assigned

Simultaneous 16-port IP KVM Logins

Only one 16-port IP KVM administrator can be logged in at a time. If a second administrative user attempts to log on to the Web Manager, the following prompt appears offering a choice of cancelling the attempt to log on or terminating the other administrator's login session.



Another administrator [apc] is currently logged in. Only one administrator can be logged in at once. Decide how you want to proceed.

○ Proceed. Log into the device and log-off the currently logged-in administrator.

● Cancel.

Figure 1-7: Simultaneous Administrator Login Prompt

Simultaneous Server Connections

The 16-port IP KVM supports a maximum of 6 concurrent server connections. Up to two connections are supported either locally or remotely over Ethernet. Up to 4 connections can be inband depending on whether a KVM-over-IP connection is being made. The types of user connections that can be made are explained below :

- Local users include:
  - One local user at the 16-port IP KVM (User 1).
  - One extended user at the APC CAT5/IP KVM Console Extender location (User 2)
- IP users include:
  - KVM – The 16-port IP KVM supports two KVM-over-IP connections.
  - Inband – The 16-port IP KVM supports up to four concurrent in-band connections depending on the number of KVM-over-IP connections being made. Since the maximum total IP connections is four, if one KVM-over-IP connection is being made, only three in-band connections can be made at that time.

- The following table lists the number and types of server connections that can be made locally and over IP.

Table 1-5: Number of Simultaneous Server Connections

Local Users	0	1	2
KVM-over-IP	2	1	-
Inband	2	3	4
Total	4	5	6

Administration Options

The following sections summarize the 16-port IP KVM administration options:

- “APC Web Manager” on page 17
- “On-Screen Display” on page 18
- “Linux Commands and 16-port IP KVM-specific Commands” on page 18

The administrator options require different types of log on credentials. For more information on which types of users can perform administrative tasks and access administrative options, see “Types of Users” on page 14.

Table 1-6: Administration Options

APC Web Manager	The Web Manager is the primary means of configuring the 16-port IP KVM and administering its connected devices. • See “Prerequisites for Using the Web Manager” on page 19 for an introduction that includes prerequisites for using the Web Manager and explanations about how the different types of user accounts use the Web Manager. • See “Web Manager for Administrators” on page 101 for more details about how 16-port IP KVM administrators use the Web Manager.

Table 1-6: Administration Options (Continued)

On-Screen Display	The On Screen Display (OSD) can be used locally from a keyboard, monitor and mouse that is directly connected to the 16-port IP KVM. When the monitor and the 16-port IP KVM are on, the OSD login screen appears on the monitor. • See “To Connect to the User 1 Management Port” on page 64 for instructions on how to make the hardware connection. • See “On Screen Display” on page 295 for how 16-port IP KVM administrators and regular users can use the OSD.
Linux Commands and 16-port IP KVM-specific Commands	The 16-port IP KVM offers the following types of access allowing administrators to log on and enter Linux commands and 16-port IP KVM-specific commands in a shell running on the 16-port IP KVM: • A local administrator who has a direct connection to the console port on the 16-port IP KVM, who is running a terminal or terminal emulation program, and who knows the root password. The direct login requires authentication using the root password. The default shell defined for the root user is bash. • A remote administrator who uses telnet or ssh to connect to the 16-port IP KVM and log on as root. See “To Connect to the Console Port” on page 63 and “Configuring Basic Networking Using the wiz Command” on page 66.

APC Web Manager

Administrators perform most tasks through the 16-port IP KVM's version of the APC Web Manager. The Web Manager runs in a browser and provides a real-time view of all the equipment that is connected to the 16-port IP KVM. The administrator or the regular user who has administrative access can use the Web Manager to configure users and ports, troubleshoot, maintain, cycle power, and reboot the connected devices, either while on site or from a remote location. 16-port IP KVM also allows regular users and administrators to use the Web Manager to access devices that are connected to KVM ports.

Web Manager uses forms and dialog boxes (which are pop-up windows) to receive data input. See also, "Prerequisites for Using the Web Manager" on page 19.

Administrators, see "Web Manager for Administrators" on page 101. Regular users, see "Web Manager for Regular Users" on page 245.

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 site's system or network administrator.

- An administrator needs to define basic network parameters on the 16-port IP KVM so the Web Manager can be launched over the network.

  See "Configuring Basic Networking Using the wiz Command" on page 66 for instructions on how to define network parameters on the 16-port IP KVM.

The administrator also needs the following to be able to connect to the 16-port IP KVM through the Web Manager:

- A networked Windows computer that has access to the network where the 16-port IP KVM is installed.
- A supported browser. Internet Explorer 5 and above, Netscape 8, Mozilla, and Firefox browsers are supported for configuration and management of 16-port IP KVM.

Note: Internet Explorer and Netscape 8 are recommended browsers for accessing servers through a KVM-over-IP session. If you are using Netscape 8 make surer to select Internet Explorer rendering engine and enable the ActiveX option.

- The IP address of the 16-port IP KVM.

  Entering the IP address of the 16-port IP KVM in the address field of the browser is the first step required to access the Web Manager.

  When DHCP is enabled, a device's IP address may change each time the 16-port IP KVM is booted up. Anyone wanting to access the 16-port IP KVM must find out the currently assigned IP address. If DHCP is enabled and you do not know how to find out the current IP address of the 16-port IP KVM, contact your system administrator for help. For more information, see "Considerations When Choosing Whether to Enable DHCP" on page 49.
- A user account defined on the Web Manager

  By default, the admin has an account on the Web Manager. An administrator can add regular user accounts to administer connected devices using the Web Manager.

TCP Ports

The TCP port numbers for KVM ports are used by the Remote Viewer when a user connects to a KVM port through the Web Manager. When a user connects to a KVM port through the Web Manager, the Remote Viewer uses port 5900. If a second IP module exists, port 5901 is used for the second Remote Viewer launched over IP. You can assign a different port number or numbers through the OSD or the Web Manager. Do not assign reserved TCP port numbers 1 through 1024.

Special circumstances may require 16-port IP KVM administrators to specify alternative TCP port numbers other than the defaults. For example, the firewall may block TCP port 5900 or 5901.

The following table provides links to procedures for changing default TCP port numbers.

Table 1-7: Configuring TCP Port Numbers

Task	Where Described
Change the TCP port number(s) assigned to the Remote Viewer(s)	“To Configure IP User (KVM Over IP) Sessions” on page 141
Change the TCP port number(s) assigned to in-band connections	“To Add or Modify an In-band (RDP) Server” on page 176

Cascaded Devices

The 16-port IP KVM supports cascading, which allows administrators to connect secondary KVM units to a primary 16-port IP KVM. Cascading allows administrators to increase the number of managed devices to up to 256 servers with a centralized configuration and access interface.

A maximum of 16 secondary KVM devices can be cascaded from the primary 16-port IP KVM extending the number of KVM ports to a maximum of 128 for two-user configuration (i.e. two connections to each cascaded device), or 256 for a one-user configuration.

The following diagram depicts a basic cascaded configuration of a primary 16-port IP KVM.

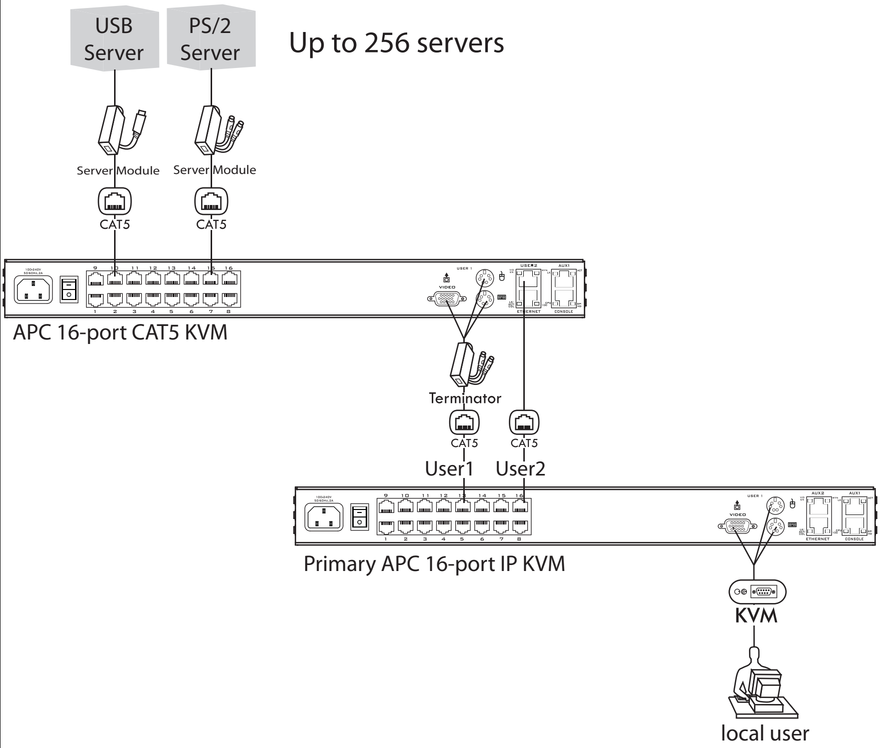


Figure 1-8: Cascaded KVM Devices from a 16-port IP KVM

As depicted in the previous figure, the 16-port IP KVM supports one level of cascading: The primary 16-port IP KVM controls the secondary level of KVM units connected to it. A secondary KVM units can be another 16-port IP KVM or a 16-port CAT5 KVM.

Administrators can connect up to 16 KVM units to the master 16-port IP KVM. Each cascaded KVM device has two management ports that can be connected to the primary 16-port IP KVM. You can connect any one of the master 16-port IP KVM's KVM ports to either the User 1 or User 2 management ports on the cascaded KVM.

Note: In addition to a CAT5 cable, you need a KVM Server Module to connect to the User 1 port of a cascaded KVM unit.

16-port IP KVM users can use the master 16-port IP KVM to access all devices connected to KVM ports on the master and primary KVM units.

Port Permissions

In the default configuration, only the "apc" and "root" users can access any ports. The administrator configures access for regular users as desired.

The following table summarizes the default port access permissions and default authentication types (Auth Type) and provides links to where the port permissions are described in more detail.

Table 1-8: Default Port Access Permissions

Default Access	Default Auth Type	Access Types	Where Documented
None	Local	No access Read only Read/Write Full access (Read/ Write/Power management)	"Understanding KVM Port Permissions" on page 24 "To Assign KVM Port Access to a User or Group" on page 156

The administrator must take the actions described under “Where Documented” to allow any other types of access than the defaults defined in the previous table. See “Authentication” on page 42 for the tasks related to setting up authentication.

Understanding KVM Port Permissions

KVM port permissions are defined in the Web Manager by assigning *Default Permissions* that apply to all KVM ports and by optionally assigning specific permissions to individual ports or groups of ports. The options for “Default Permissions” are shown in the following list.

- No access [Default]
- Read only
- Read/Write
- Full access (Read/Write/Power management)

For individual users and groups, if desired, the 16-port IP KVM administrator can construct lists of KVM ports with the following types of permissions:

- Ports with no permission
- Ports with read only permission
- Ports with read/write permission
- Ports with full permission

A *Generic User* account has a default set of permissions that apply to all regular users and groups. The Generic User’s Default Permission is “No access.”

To allow users to access KVM ports, the 16-port IP KVM administrator must do one or both of the following:

- Change the permissions assigned to the Generic User
- Change the permissions assigned to individual users or to groups of users

Editing the Generic User allows you to change the KVM port permissions for all regular users and groups at once.

The 16-port IP KVM administrator can specify different Default Permissions or KVM port permissions for any user or group. “KVM Port Permissions Hierarchy” on page 25 provides information that the 16-port IP KVM administrator needs to understand in order to perform advanced configuration of KVM permissions.

The following table shows the tools that the 16-port IP KVM administrator can use to set KVM port permissions and where in this manual to go for further details.

Table 1-9: Tools for Setting KVM Port Permissions

Tools	Where Documented
Web Manager	"To Assign KVM Port Access to a User or Group" on page 156
OSD	"KVM Ports Screens" on page 337

KVM Port Permissions Hierarchy

If you specify individual KVM port permissions or default permissions for users and groups, you need to understand the following information about how the system handles requests from a user who is trying to access a KVM port. The following series of decisions is made.

Decision 1: Check User's KVM Port Permissions

1. Does the user have specific KVM port permissions that allow or deny access to the port?
   - If yes, access is allowed or denied.
   - If no, go to Decision 2.

Example for Decision 1

- If user john is trying to access KVM port 4 and his account has port 4 in a list of ports with full permission, then john is given read/write and power management access.
- If user jane is trying to access port 4 and her account has port 4 in a list of ports with no permission, then jane is denied access.
- If users jim, joan, jerry, jill, joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and do not have port 4 listed for any types of access, then their access requests are passed to decision 2.

Decision 2: Check Group’s KVM Port Permissions

2. Is the user included in a group with KVM port permissions that allow or deny access to the port?
   - If yes, access is allowed or denied.
   - If no, skip to Decision 3.

Note: When a user is in more than one group, the most restrictive permission is used.

Example for Decision 2

- If user jim is trying to access port 4 and he is a member of a group called linux_ca2 that has port 4 in a list of ports with read/write permissions, then jim is given read/write access.
- If user joan is trying to access port 4 and she is in a group called linux_ca3 that has port 4 in a list of ports with no permission, then joan is denied access.
- If jerry and jill are trying to access port 4 and are in a group called linux_ca4 that has no specific port permissions defined, then their access requests are passed to decision 3.
- If joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and are not in any group, then their access requests are passed to decision 3.

Decision 3: Check Generic User’s KVM Port Permissions

3. Does the Generic User have specific KVM port permissions that allow or deny access the port?
   - If yes, access is allowed or denied.
   - If no, go to decision 4.

Example for Decision 3

- If user jerry is trying to access port 4 and the Generic User has port 4 in a list of ports with full access permissions, then jerry is given read writer and power management access.

- If user jill is trying to access port 4 and the Generic User has port 4 in a list of ports with no access permissions, then jill is denied access.
- If users joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and the Generic User does not have port 4 listed for any type of access, then their access request are passed to decision 4.

Decision 4: Check User's Default Permissions

4. Does the user have a Default Permission that allows or denies access to the port?

   - If yes, access is allowed or denied.
   - If the user has no Default Permission, the user is under the Generic User's default permission, and the request for access goes to decision 5.

Example for Decision 4

- If user joe is trying to access port 4 and he has a Default Permission that allows read only access to ports, then joe is given read only access.
- If user jennifer is trying to access port 4 and she has a Default Permission that allows no access to ports, then jennifer is denied access.
- If users jordan, jolanda, and jezebel are trying to access port 4 and their Default Permissions are under the Generic User's Default Permission, then their access requests are passed to decision 5.

Decision 5: Check Group's Default Permissions

5. Does the user belong to a group that has a Default Permission that allows or denies access to the port?

   - If yes, permission is granted or denied.
   - If no, go to decision 6.

Example for Decision 4

- If user jordan trying to access port 4 is in a group called windows_ca1 that has a Default Permission of full, then jordan is given read/write and power management access.
- If user jolanda trying to access port 4 is in a group called windows_ca2 that has a Default Permission of no access, then jolanda is denied access.

- If user jennifer is not a member of any group with a Default Permission specified, then her access request is passed to decision 6.

Decision 6: Check Generic User's Default Permissions

Note: If an access request gets this far, the Default Permission of the Generic User is the only permission that could apply.

6. Does the Default Permission for the Generic User allow access to the port?

- If yes, access is granted.
- If no, access is denied.

Server Access: In-band and Out of Band

16-port IP KVM users can access servers over the Ethernet using the following methods:

- In-band access – An IP address is used to connect to and control Windows (Win2000, 2003, XP, and NT) Terminal Servers.
- Out-of-band access – KVM ports are used to connect to PCs with USB or PS/2 connectors or Sun servers with USB connectors.

The differences between the in-band and out-of-band connection methods are briefly described in the following table. For a more detailed description of the requirements and functionality of each connection method, see the following section, "Determining the Connection Type and its Supported Functionality" on page 30.

Table 1-10: In-band and Out of Band Connections

	In-band	**Out-of-Band**
Connection Type	Remote Desktop Protocol (RDP) over the Ethernet or PPP	Keyboard, video, mouse (KVM) CAT5 connection to a 16-port IP KVM and Ethernet or PPP access to the 16-port IP KVM Web Manager

Table 1-10: In-band and Out of Band Connections

	In-band	Out-of-Band
Supported Source Computers	Client machine running a Windows operating system with a valid IP address	All Windows clients
Supported Target Servers	Windows (Win2000, 2003, XP, and NT) Terminal Servers	PCs with a USB or PS/2 connectors or Sun servers with USB connectors
Supported Browsers	Internet Explorer 5, 6	Internet Explorer 6, Netscape 7, Mozilla, Firefox
Direct Log In	Not available	Available if configured by the 16-port IP KVM administrator See “To Enable Direct Access to KVM Ports” on page 134.
Power Management While Connected	Not available	Available if configured by the 16-port IP KVM administrator and if the server is plugged into an APC rPDU that is connected to the 16-port IP KVM. See “Power Management” on page 38.
Viewer	ActiveX viewer See “Viewing In-band Connections” on page 257	Remote Viewer See “Viewing KVM Connections” on page 256.

Determining the Connection Type and its Supported Functionality

When a user wants to connect to a server displayed on the Web Manager Connect to Server form, the drop-down list indicates whether the server can be accessed by a KVM connection, an in-band connection, or both. In the connect list, all servers connected to KVM ports appear first followed by all servers that are accessed through in-band connections and are not connected to KVM ports; those servers that can be connected by both methods appear at the bottom of the list.

The types of connections that can be made to each server is displayed in parenthesis at the end of each server entry in the list. The following table describes the functionality of each connection type.

Table 1-11: Available Functionality During KVM and In-band Connections

Server Connection Labels	Description
(KVM)	Indicates that the server can be accessed only through an out-of-band, KVM connection. This server is connected to a KVM port on the 16-port IP KVM or on a cascaded KVM unit. Users can control all applications on the server, have BIOS access, and can view POST, and boot messages. Users can access this server even when the network is down or after a system boot is completed. Users can also control the power flow on this server if the server is plugged into an APC rPDU and the port is properly configured for power management.

Table 1-11: Available Functionality During KVM and In-band Connections (Continued)

Server Connection Labels	Description
(Inband)	Indicates that the Microsoft Terminal Server running RDP can be accessed only through an in-band connection and is not connected to a KVM port. Users can access this server only to run applications once the server is already running. The performance on in-band connections is slightly better than that of KVM connections, and no synchronization of keyboard and mouse is necessary.
(KVM + Inband)	Indicates that the server can be accessed through in-band and out-of-band (KVM) connections. The first time users select this server from the Connect drop-down list, an in-band connection is attempted. The connection automatically switches to KVM only if the in-band connection fails or if an in-band connection to this server already exists. Users who want to access this server with a KVM connection, must do one of the following: • Make two connection attempts to the same server from the Web Manager “Connect to Server” form. The first connection is an in-band connection viewed through an RDP ActiveX viewer. The second connection is a KVM connection viewed through the KVM ActiveX Viewer. See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 266. • Make a direct login to the KVM port. See “Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 263 and “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 264 for more information.

Administering Users of Connected Servers

This section reviews the tasks that 16-port IP KVM administrators must do to enable access to connected servers.

The “apc” account can add new regular user accounts to allow others to connect to ports and administer or use connected devices.

Types of Access to Ports

The 16-port IP KVM administrator can restrict regular user accounts to allow them only to manage specific servers and devices. Each account can have one of the following types of access after login:

- Read only
- Read write
- Read write power

Note: The 16-port IP KVM offers access privileges to KVM ports only. In-band connections are authenticated, and the access privileges are granted on the in-band server itself.

Tasks Related to Access to Connected Devices

Planning should include the following steps:

- Create a list of servers to connect to the 16-port IP KVM.
- Decide whether the servers need to be connected to ports for KVM access, need to have RDP enabled for in-band access, or both.
- Create a list of user accounts with the type of access each user needs to which ports.
- Obtain user names and passwords with the proper permissions for connected servers to give to the 16-port IP KVM users who will connect to these servers.
- Create meaningful aliases to assign to port numbers and to in-band Windows Terminal Servers.
- List all the devices that need to be connected to rPDUs and the users who can access them.

During setup of the 16-port IP KVM, the installer connects the desired servers to the ports as planned.

During configuration, the 16-port IP KVM administrator does the following, if desired:

- Assigns aliases to ports to identify the connected servers.
- Assigns aliases to rPDUs to identify the location or types of devices being managed.
- Creates accounts for users of connected devices.
- Specifies which ports each user can access and which type of access each can have.
- Specifies an authentication method for access to the 16-port IP KVM and to all KVM ports.
- Redefines keyboard shortcuts (hot keys) if desired.
- Redefines TCP port numbers used for accessing KVM ports, if desired.

See the following table for a list of related tasks and where they are documented.

Task	Where documented
Specify an alias for a KVM port.	• “To Specify or Change the Alias for a KVM Port” on page 146
Specify an alias for an rPDU.	• “To Specify or Change the Alias of an rPDU” on page 130
Assign permissions to access ports.	• “To Assign KVM Port Access to a User or Group” on page 156
Assign permissions to rPDUs and outlets.	• “To Configure Users to Manage Specific Power Outlets” on page 128

Redefining Keyboard Shortcuts (Hot Keys)

Predefined keyboard shortcuts (also called hot keys) allow users to do the following:

- Perform common actions while connected through a KVM port
- Emulate Sun keyboard keys while connected through a KVM port to a Sun server.

If desired, the 16-port IP KVM administrator can redefine the default hot keys either through the Web Manager or the OSD.

Redefining KVM Connection Hot Keys

The hot key sequences used while connected to KVM ports have two parts, which are called the *common escape sequence* and the *command key*. The default common escape sequence is `Ctrl+k`, and the command key is different for each command. For example, the `q` command key is entered after `Ctrl+k` to quit the login session as shown here: `Ctrl+k q`. See “Hot Keys for KVM Connections” on page 273 for the defaults. Under Configure>KVM in the Web Manager, the common escape sequence is defined separately from the command keys. The 16-port IP KVM administrator can redefine two different sets of command keys for users accessing KVM ports through the OSD (User 1 or User 2) and another set for connections made through the Web Manager.

Redefining Sun Keyboard Equivalent Hot Keys

The 16-port IP KVM provides a default set of hot keys for use while connected to Sun servers through KVM ports to emulate keys that are present on Sun keyboards but are not present on Windows keyboards. The hot keys are made up of an escape key followed by a function key. See “Hot Keys for Emulating Sun Keyboard Keys” on page 274 for more details. The default escape key is the Windows key, which is labeled with the Windows logo. 16-port IP KVM administrators can redefine the Sun emulation escape key to be one of the following: Ctrl, Shift, or Alt.

Summary of Tasks for Redefining Hot Keys

See the following table for a summary of tasks for redefining keyboard shortcuts with references to where they are documented.

Table 1-12: Tasks for Redefining Hot Keys

Part	Web Manager Form	Where Documented	OSD Form	Where Documented
KVM Common escape sequence	Configuration> KVM>General > General	“To Redefine KVM Session Keyboard Shortcuts” on page 135	Configure> General	“General Configuration Screens [OSD]” on page 305
KVM Command keys for the local user session	Configuration> KVM>General >User 1 Configuration> KVM>General >User 2	“To Redefine KVM Session Keyboard Shortcuts” on page 135	Configure> User Station	“User Station Screens” on page 333
KVM Command keys for IP user sessions	Configuration> KVM>General >IP Users		N/A	
Sun keyboard emulation escape key	Configuration> KVM>General	“To Redefine KVM Session Keyboard Shortcuts” on page 135	Configure> General	“KVM Ports Screens” on page 337

Packet Filtering on the 16-port IP KVM

IP filtering refers to the selective blocking of the IP packets based on certain characteristics. The 16-port IP KVM can be configured to filter packets as does a firewall.

The IP Filtering form is structured in two levels:

- Chain – The IP Filtering form which contains a list of chains
- Rule – The chains which contain the rules that control filtering

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 (that is, 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 crack the network system or generate unnecessary traffic in the network.

The following table describes the different levels of IP filtering

Table 1-13: Levels of IP Filtering

Chain	The filter table contains a number of built-in chains and may include user-defined chains. The built-in chains are called according to the type of packet. User-defined chains are called when a rule which is matched by the packet points to the chain. Each table has a set of built-in chains classified as follows: • INPUT - For packets coming into the box itself. • FORWARD - For packets being routed through the box. • OUTPUT - For locally generated packets.

Table 1-13: Levels of IP Filtering (Continued)

Rule	Each chain contains a sequence of rules that control filtering. The rules address the following issues: • How the packet should appear in order to match the rule Some information about the packet is checked according to the rule, for example, the IP header, the input and output interfaces, the TCP flags and the protocol. • What to do when the packet matches the rule The packet can be accepted, blocked, logged, or jumped to a user-defined chain. When a chain is analyzed, the rules of this chain are reviewed one-by-one until the packet matches one rule. If no rule is found, the default action for that chain will be taken.

Power Management

The 16-port IP KVM enables users who have power management permissions to power off, power on, and reboot remote devices connected to an APC rPDU.

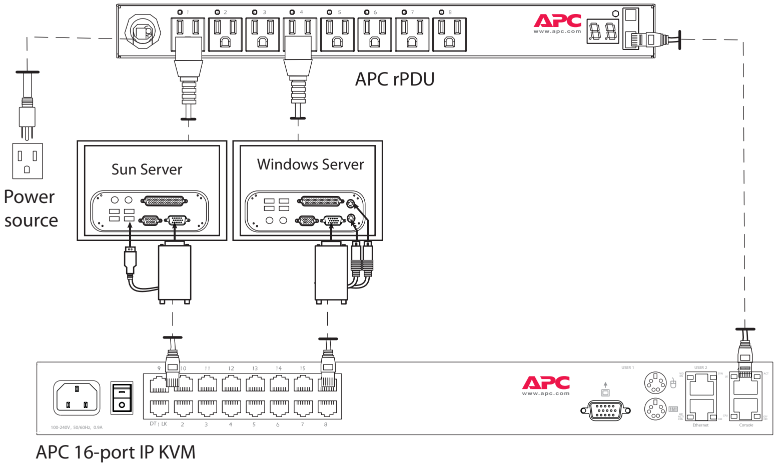


Figure 1-9: Connecting an APC rPDU to the 16-port IP KVM

See “Setting Up and Configuring Power Management” on page 40 for information about the procedures the 16-port IP KVM administrator must perform before anyone can use the tools to manage power.

16-port IP KVM users most commonly perform power management through the Web Manager. See “Options for Managing Power” on page 39 for more information.

Options for Managing Power

The sections listed below describe the different ways that users with power management permissions (called authorized users) can perform power management through the 16-port IP KVM and provide links to related information and procedures.

Controlling Power Through the Web Manager rPDU Power Management Forms

Through the Web Manager's rPDU Power Management form, users with power management permissions can perform power management on any device plugged into an rPDU connected to the AUX port. See "Power Management for Regular Users" on page 250.

Administrators must configure users for rPDU power management. See "To Configure Users to Manage Specific Power Outlets" on page 128. Or see "Setting Up and Configuring Power Management" on page 40 for a list of all of the administration tasks involved in setting up power management.

Controlling Power While Connected to KVM Ports

Users who have power management permissions can do power management while connected to servers through KVM ports by using a keyboard shortcut that brings up a power management screen. The default keyboard shortcut is Ctrl+k p.

Administrators must perform multiple configuration tasks in order to set up and grant users permission for power management. See "Setting Up and Configuring Power Management" on page 40 for a list of all of the administration tasks involved in setting up power management.

Setting Up and Configuring Power Management

Administrators most commonly assign power management permissions to users and configure ports for power management using the Web Manager. However, the OSD also offers menus for configuring power management on local devices.

Two types of power management can be set up and configured on the 16-port IP KVM:

- Power management of any device plugged into an rPDU connected to the AUX port.

  See “Controlling Power Through the Web Manager rPDU Power Management Forms” on page 39.
- Power management while accessing a server connected to a KVM port and plugged into an rPDU connected to the AUX port.

  See “Controlling Power While Connected to KVM Ports” on page 39.

The following set up and configuration tasks must be performed for both types of power management:

Table 1-14: Tasks: General Power Management Set Up

	Task	Where Documented/Notes
1	Install rPDU units.	• “To Connect an APC rPDU to the AUX Port” on page 95
2	Configure the AUX port for use with power management.	“To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219
3	Plug devices into outlets on the rPDU connected to the AUX port.	Devices plugged into connected rPDUs can be managed from the 16-port IP KVM Web Manager Access Page.
4	Configure users to manage power.	“To Configure Users to Manage Specific Power Outlets” on page 128

The following additional configuration tasks must be performed for power management while accessing a server connected to a KVM port and plugged into an APC rPDU connected to the AUX port:

Table 1-15: Tasks: KVM-connected Power Management

	Task	Where Documented/Notes
5	Plug servers connected to KVM ports into outlets on the rPDU connected to the AUX port.	This is the first step in allowing users to control power not only from the Web Manager Access page, but while connected to KVM ports as well. Refer to the documentation of your rPDU model for more information if needed.
5	Associate the ports to which the servers are connected with the power outlets to which the servers are plugged in.	"To Configure a KVM Port for Power Management" on page 143
6	Give users full access (read, write, power) permission on the KVM port(s).	"To Assign KVM Port Access to a User or Group" on page 156

Security

The 16-port IP KVM comes with the following configurable security features:

- Encryption

  See Encryption.
- Authentication

  See Authentication.

Encryption

Administrators can specify that communications are encrypted between the 16-port IP KVM and any computer attached to a KVM port. In the Web Manager, the administrator chooses Expert>Configuration>KVM>Security to bring up the IP security form.

See “Security” on page 159 for instructions.

Authentication

Anyone accessing the 16-port IP KVM must log on by entering a user name and password. Controlling access by requiring users to enter names and passwords is called authentication. User Names and passwords entered during login attempts are checked against a database that lists all the valid user names along with the encrypted passwords. Access is denied if the user name or password is not valid. The password database that is used for checking can reside either locally (on the 16-port IP KVM) or on an authentication server on the network. The selected authentication server must be already installed and configured in order for authentication to work. Using one or more of the many types of popular authentication methods supported on the 16-port IP KVM can reduce administrator workload when a user account needs to be added, modified, or deleted.

Choosing Among Authentication Methods

The administrator can select among authentication methods to control logins to the following components:

- For logins to the 16-port IP KVM

  The authentication method chosen for the 16-port IP KVM is used for subsequent access through `telnet`, `ssh`, or the Web Manager.
- For logins to all KVM ports

The following table describes the supported authentication methods and indicates which methods are available for the 16-port IP KVM and which are available for KVM ports. All authentication methods except “Local” require an authentication server, which the administrator specifies while selecting the authentication method. The 16-port IP KVM uses local authentication if any of the authentication servers fails.

Table 1-16: Supported Authentication Types for 16-port IP KVM and Port Types

Authentication Type	Description	16-port IP KVM	All KVM Ports
None	No login required	N/A	X

Table 1-16: Supported Authentication Types for 16-port IP KVM and Port Types

Authentication Type	Description	16-port IP KVM	All KVM Ports
Local	Uses user/password file for local authentication on the 16-port IP KVM	X [Default]	X [Default]
Kerberos	Uses Kerberos network authentication protocol	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails	X	X
KerberosDownlocal	Uses local authentication if Kerberos server is down	X	X
LDAP	Uses LDAP (Light-weight directory access protocol)	X	X
LDAP/Local	Uses local authentication if LDAP authentication fails	X	X
LDAPDownlocal	Uses local authentication if LDAP server is down	X	X
NIS	Uses NIS authentication	X	X
NIS/Local	Uses local authentication if NIS authentication fails	X	X
NISDownlocal	Uses local authentication if NIS server is down	X	X

Table 1-16: Supported Authentication Types for 16-port IP KVM and Port Types

Authentication Type	Description	16-port IP KVM	All KVM Ports
NTLM	Uses SMB authentication for Microsoft Windows NT/2000/2003	N/A	X
RADIUS	Uses RADIUS authentication	X	X
RADIUSDownlocal	Uses local authentication if RADIUS server is down	X	X
RADIUS/local	Uses local authentication if RADIUS authentication fails	X	X
TACACS+	Uses Terminal Access Controller Access Control System (TACACS+) authentication.	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails	X	X
TACACS+Downlocal	Uses local authentication if TACACS+ server is down	X	X

Tools for Specifying Authentication Methods

The administrator generally uses the Web Manager for specifying an authentication method for the 16-port IP KVM and for all KVM ports, as described in “Configuring an Authentication Method” on page 161. Optionally, the administrator can use the OSD (on screen display) for selecting an authentication method and specifying an authentication server (when needed).

The following table lists the tasks necessary for specifying authentication methods using the Web Manager and the OSD:

Table 1-17: Tasks: Specifying Authentication Methods

Task	**Where Documented/Notes**
Choosing an authentication method for the 16-port IP KVM	• Web Manager – “To Configure an Authentication Method for 16-port IP KVM Logins” on page 162 • OSD – “Authentication Screens” on page 352
Choosing an authentication method for the for all KVM ports	• Web Manager – “To Configure an Authentication Method for 16-port IP KVM Logins” on page 162 • OSD – “General Configuration Screens [OSD]” on page 305
Configuring a remote authentication server	If configuring any authentication method other than Local, an authentication server must be set up for that method. • Web Manager – “Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices” on page 164 • OSD – “Authentication Screens” on page 352

Notifications, Alarms, and Data Buffering

The 16-port IP KVM administrator can set up logging, notifications, and alarms to alert remote administrators about problems. System-generated messages about the 16-port IP KVM, any connected rPDUs, computers, or other devices can be sent to syslog servers for handling.

The 16-port IP KVM administrator can also set up data buffering, so that data from communications with KVM-connected computers can be stored in files at the following locations:

- Local–stored in the 16-port IP KVM’s flash memory
- Remote files–stored in either of the two following types of servers:
  - NFS servers
  - Syslog servers

For more details about syslog servers see, “Syslog Servers” on page 46.

For more background about setting up logging, notifications, alarms, and for links to all related procedures in this manual, see “Configuring Logging and Alarms” on page 47.

Syslog Servers

Messages about the 16-port IP KVM, its connected rPDUs, and other connected devices can be sent to central logging servers, called syslog servers. Data from KVM-connected computers can optionally be stored in files on syslog servers.

Syslog servers run operating systems that support system logging services, usually UNIX-based servers with the syslogd configured.

Prerequisites for Logging to Syslog Servers

An already-configured syslog server must have a public IP address that is accessible from the 16-port IP KVM. The 16-port IP KVM administrator must be able to obtain the following information from the syslog server's administrator.

- The IP address of the syslog server
- The facility number for messages coming from the 16-port IP KVM.

  Facility numbers are used on the syslog server for handling messages generated by multiple devices. See "Facility Numbers for Syslog Messages" on page 47 for more background on how facility numbers are used.

Facility Numbers for Syslog Messages

Each syslog server has seven local facility numbers available for its system administrator to assign to different devices or groups of devices at different locations. The available facility numbers are: Local 0 through Local 7.

Example of Using Facility Numbers

The syslog system administrator sets up a server called "syslogger" to handle log messages from two 16-port IP KVM units. One 16-port IP KVM is located in Brazil, and the other 16-port IP KVM is in New York. The syslog server's administrator wants to aggregate messages from the Brazil 16-port IP KVM into the `local1` facility, and to aggregate messages from New York 16-port IP KVM into the `local2` facility.

On "syslogger" the system administrator has configured the system logging utility to write messages from the `local1` facility to the `/var/log/saopaulo-config` file and the messages from the `local2` facility to the `/var/log/newyork-config` file. While identifying the syslog server using the Web Manager, according to this example, you would select the facility number Local 2 from the Facility Number drop-down list on the SysLog form.

Configuring Logging and Alarms

The following procedures can be used configure logging, alarms, and data buffering.

- "To Add a Syslog Server [Wizard]" on page 119
- "To Delete a Syslog Server [Wizard]" on page 119

- “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 186
- “To Configure Creation of Alarms and Syslog Files for rPDUs” on page 130

VPN and the 16-port IP KVM

The 16-port IP KVM administrator can set up VPN (Virtual Private Network) connections to establish encrypted communications between the 16-port IP KVM and an individual host or all the hosts on a remote subnetwork. The encryption creates a security tunnel for communications through an intermediate network which is untrustworthy.

A security gateway with the IPsec service enabled must exist on the remote network. The IPsec gateway encrypts packets on their way to the 16-port IP KVM and decrypts packets received from the 16-port IP KVM. A single host running IPsec can serve as its own security gateway. The 16-port IP KVM takes care of encryption and decryption on its end.

Connections between a machine like the 16-port IP KVM to a host or to a whole network are usually referred to as host-to-network and host-to-host tunnel. 16-port IP KVM host-to-network and host-to-host tunnels are not quite the same as a VPN in the usual sense, because one or both sides have a degenerated subnet consisting of only one machine.

The 16-port IP KVM is referred to as the Local or “Left” host, and the remote gateway is referred to as the Remote or “Right” host.

In summary, you can use the VPN features on the 16-port IP KVM to create the two following types of connections:

- Create a secure tunnel between the 16-port IP KVM and a gateway at a remote location so every machine on the subnet at the remote location has a secure connection with the 16-port IP KVM.
- Create a secure tunnel between the 16-port IP KVM and a single remote host

The gateway in the former example and the individual host in the second example both need a fixed IP address.

To set up a security gateway, you can install IPsec on any machine that does networking over IP, including routers, firewall machines, various application servers, and end-user desktop or laptop machines.

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

Considerations When Choosing Whether to Enable DHCP

DHCP is enabled by default. It relies on a DHCP server known to the 16-port IP KVM. Because a DHCP server may assign a different IP address every time the 16-port IP KVM reboots, when DHCP is enabled, a user needs to take an additional step to find out the dynamically assigned IP address before being able to bring up the Web Manager. Following are three ways to find out the dynamically assigned IP address:

- Make an inquiry to the DHCP server on the network where the 16-port IP KVM resides, using the MAC address (a 12-digit hexadecimal number, which is on a label at the bottom of the 16-port IP KVM).
- Connect to the 16-port IP KVM remotely using `telnet` or `ssh`.
- Connect directly to the 16-port IP KVM to find out the DHCP address using the `ifconfig` command.

KVM Server Module Usage and Types

A KVM Server Module is used when connecting a computer or a cascaded KVM device to a KVM port on the APC 16-port IP KVM.

Administrators or operators at remote stations who have access through the 16-port IP KVM's management software to a KVM port have the same kind of access as if they were using the actual keyboard, mouse, and monitor of the computer that is connected to the port.

The Server Module comes in three models shown in the following table:

Table 1-18: KVM Server Modules

Server Type	Connection	KVM Server Module Model	Part Number
PC	VGA and PS/2 ports	PS/2	AP5460
Sun USB	VGA and SUN Mini-DIN ports	Sun USB	AP5462
PC/Sun	VGA and USB ports (This Server Module does not work with all Sun computers. The Sun computer must have a VGA and USB port.)	PC/Sun USB	AP5461

See "To Connect Computers to KVM Ports" on page 60 for instruction on using the KVM Server Modules.

When a 16-port IP KVM is ordered, the customer selects a KVM Server Module for each type of computer to be connected to the 16-port IP KVM's KVM ports. For example, when ordering a 16-port IP KVM with four KVM ports to be connected to two Windows servers with DIN connectors and two Sun servers with VGA ports and USB connectors, the customer would order two PS/2 Server Modules and two Sun USB Server Modules.

Activity LEDs on the Server Module

There are two activity LEDs located on the Server Module.

1. The “Link” LED displays a solid amber light when the Server Module connects to the server. A quick blinking “Link” LED indicates the Server Module microcode failed to boot.
2. The “On” LED displays a blinking green light when the Server Module is on.

Chapter 2
Installation

This chapter outlines and described tasks for installing the 16-port IP KVM and provides other important installation-related information.

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

1	Review the contents of the shipping box	Page 54
2	Set up the 16-port IP KVM	Page 55
3	Make an Ethernet connection	Page 57
4	Connect servers to be managed through the 16-port IP KVM	Page 58
5	Make a direct connection (terminal or local monitor, keyboard, and mouse) to the 16-port IP KVM to prepare for basic network configuration	Page 63
6	Power on the 16-port IP KVM and connected devices	Page 64
7	Perform basic network configuration (using the wiz command or OSD network screen)	Page 65
8	Finish configuration and manage the connected devices using the Web Manager	Page 78

Also see the following instructions for setting up the 16-port IP KVM:

Changing Default Passwords	Page 79
Enabling Access to the Web Manager without Making a Direct Connection	Page 81
Preconfiguring the 16-port IP KVM for Remote Installation	Page 84
Additional Configuration Tasks	Page 85

Perform the optional procedures in “Advanced Installation Procedures” on page 93 if you are installing an APC rPDU, an external modem, a APC CAT5/ IP KVM Console Extender, or another cascaded KVM devices.

Shipping Box Contents 16-port IP KVM

The shipping box for the 16-port IP KVM contains the following items:

- 16-port IP KVM
- One NEMA 5-15 power cable
- One IEC320 power cable
- One Console (CAT5) cable
- One set rack-mounting brackets
- Documentation CD
- Product Registration Form
- Declaration of Conformity

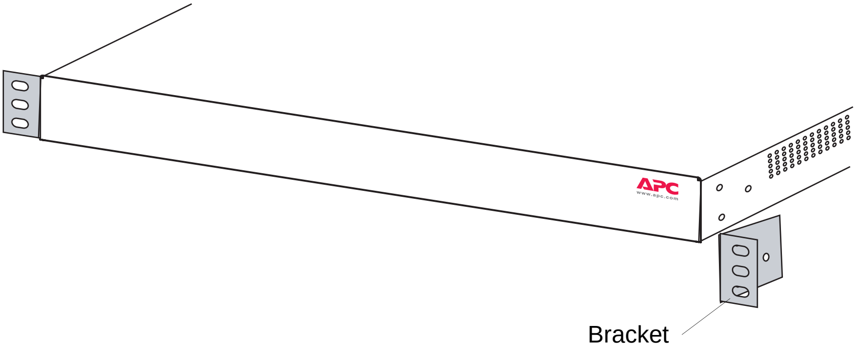
When ordering the 16-port IP KVM, customers also order one KVM Server Module for each server to be connected to one of the KVM ports. The number and types of KVM Server Modules in each order are based on the number of KVM ports on the 16-port IP KVM model that is being shipped and on the types of servers that are to be connected to the KVM ports. For details, see “KVM Server Module Usage and Types” on page 50.

Setting Up the 16-port IP KVM

You can mount the 16-port IP KVM on a rack or place it on a desktop or other flat surface. Two brackets are supplied with six Phillips screws for attaching the brackets to the 16-port IP KVM for mounting.

- If you are not mounting the 16-port IP KVM, place the 16-port IP KVMon a desk or table.
- If you are mounting the 16-port IP KVM, obtain a Phillips screwdriver and appropriate nuts and bolts before starting the following procedure.

The following graphics depict the orientation of the brackets for front mounting the 16-port IP KVM.



▼ *To Mount the 16-port IP KVM*

1. Decide whether you need to mount the 16-port IP KVM by the front or back and locate the appropriate sets of holes on the 16-port IP KVM.

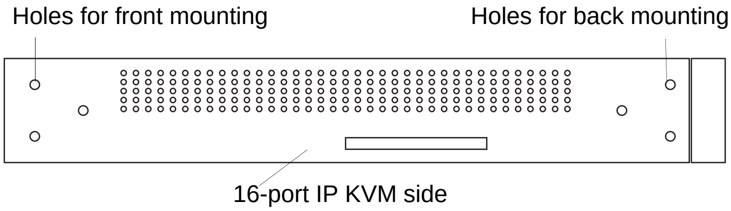
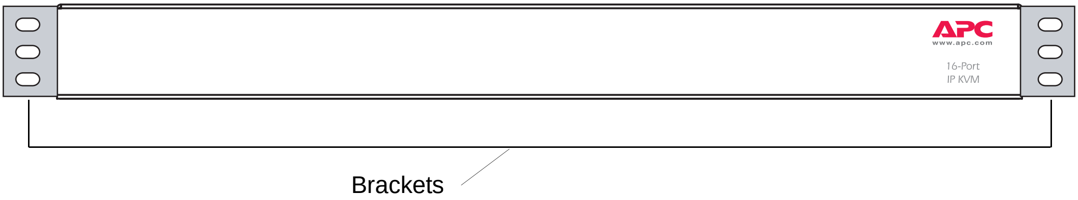


Figure 2-1: Rack Mounting Holes on the 16-port IP KVM

2. Connect the two supplied brackets to the 16-port IP KVM, connecting one bracket to each side of the box.

3. For each bracket, insert a screw through each of the three holes on the bracket into the appropriate holes at either the front or back of the 16-port IP KVM.

   The following figure shows the bracket flanges on the front of the 16-port IP KVM after the brackets are installed.



4. Use a Phillips screwdriver to tighten the screws.

5. Use the mounting hardware recommended for your rack to mount the 16-port IP KVM on a rack.

Making an Ethernet Connection

Make an Ethernet connection to the 16-port IP KVM in order to have Ethernet access to the Web Manager and remote access to devices connected to the 16-port IP KVM.

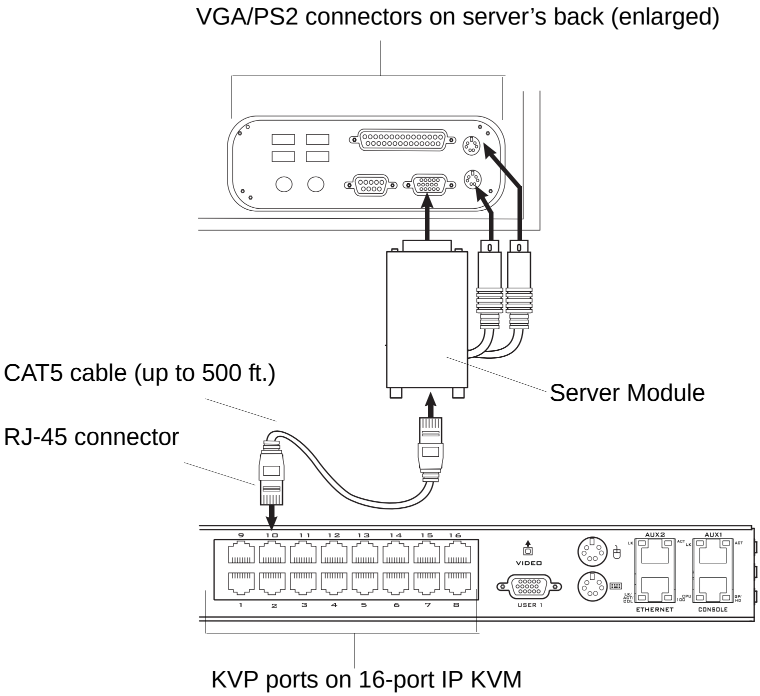
▼ *To Make an Ethernet Connection*

1. Connect one end of an Ethernet cable to your local area network (LAN).
2. Connect the other end to the Ethernet port on the 16-port IP KVM.

Remote connections can also be made through an external modem connected to the AUX port. See “Modem Connections” on page 290 for background information and instructions.

xConnecting Servers to the KVM Ports

You need to connect a KVM Server Module to every server before connecting it to a KVM port. There are three Server Module types, PC PS/2 for servers with VGA and PS/2 connectors, PC USB for servers with VGA and USB connectors, and Sun USB Server Modules for Sun servers with USB connectors. See "KVM Server Module Usage and Types" on page 50 for more details about the KVM Server Modules, which are ordered and shipped separately.


VGA/PS2 connectors on server's back (enlarged)
CAT5 cable (up to 500 ft.)
Server Module
RJ-45 connector
9 10 11 12 13 14 15 16
1 2 3 4 5 6 7 8
VIDEO
USER 1
AUX2
AUX1
ETHERNET
CONSOLE
KVP ports on 16-port IP KVM

Note: The 16-port IP KVM components are hot pluggable, but components of connected devices, such as the PS/2 keyboard and mouse ports on a computer, may not be hot pluggable. Turn off power to all devices before connecting them. Power on connected devices again only after the 16-port IP KVM is powered on.

Follow the procedures below when connecting computers to KVM ports on the 16-port IP KVM. For connecting APC rPDUs or cascaded KVM units, see Chapter 3, “Advanced Installation Procedures.”

Note: KVM port connections rely on the CAT5 cable having all four pairs wired. If you are connecting a KVM port to a server through a patch panel, make sure that all cables in the path are CAT5 or better and that the patch panel has all four pairs wired.

▼ *To Prepare to Connect Servers to the 16-port IP KVM*

1. Ensure that all configuration is complete on servers to be connected.

Work with the administrator of the devices to ensure all the following prerequisites are complete:

- All servers are installed and fully configured.
- User accounts with the appropriate permissions level exist on each server and you have the computer’s root password for users who need root access to manage the server through the 16-port IP KVM.
- On all computers to be connected to KVM server ports, the mouse settings have been modified, as described in “Avoiding Conflicting Mouse Settings” on page 86.

2. If a server is to use remote authentication, do the following steps:

a. Make sure that the following prerequisite configuration is complete:

- Authentication servers are installed and fully configured.
- You have the root password for all users who need root access to manage the server through the 16-port IP KVM.

Note: You may want to assign different passwords for a server’s administrator on the 16-port IP KVM and on the server’s remote authentication server. If the administrator logs into the server using the password for the authentication server and log on fails, the failure can indicate that the authentication server is down and that the server’s administrator should be notified to take action.

b. Obtain the information you need to identify the authentication server on the 16-port IP KVM from the server's administrator.

c. After the 16-port IP KVM is installed, make sure to specify the desired authentication method for the ports that are connected to each server.

   See "Authentication" on page 42 for background information and see "Configuring an Authentication Method" on page 161 for the procedure.

3. Because some components of connected equipment may not be hot pluggable, make sure all servers are powered off.

▼ *To Connect Computers to KVM Ports*

Do these steps after completing "To Prepare to Connect Servers to the 16-port IP KVM" on page 59.

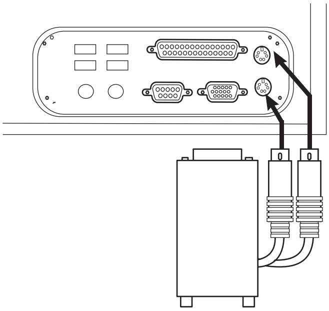
1. Select the appropriate Server Module.

Three Server Module types are available: PS/2 for PCs, USB for PCs, and USB for Sun systems. See "KVM Server Module Usage and Types" on page 50 for more details about the Server Modules, which are ordered and shipped with the 16-port IP KVM.

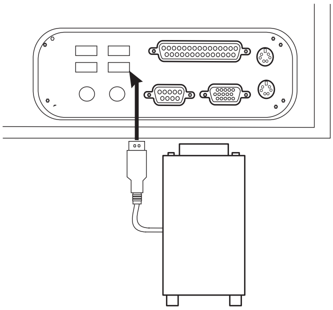
Important: To avoid system conflicts connect the Server Module to the server in the following order.

2. Connect the appropriate keyboard and mouse connectors.

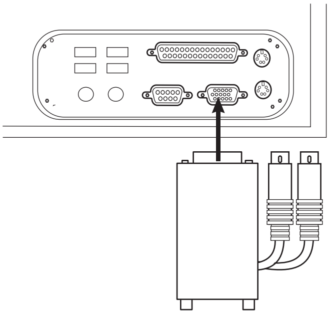
- On a PS/2 Server Module for a PC server, first connect the Server Module's green connector to the server's mouse port, and then connect the Server Module's purple keyboard connector to the server's keyboard port.



- On a USB Server Module for a PC or a Sun server, connect the Server Module’s USB connector to the USB port on the server.



3. Connect the Server Module’s VGA (HD-15 male) connector to the computer’s VGA (monitor) port. Tighten both screws firmly but do not over-tight them.



4. If the PC’s VGA port is recessed too far for easy access, insert a VGA mini extender before attempting to connect the VGA connector.

Note: Two activity LEDs are located on the Server Module. The “Link” LED displays a solid amber light when the Server Module connects to the server. The “On” LED displays a blinking green light when the Server Module is on.

5. To extend the connection from the computer to the 16-port IP KVM, connect an RJ-45 to RJ-45 CAT5 cable up to 500 feet long to the Server Module.
6. Connect the RJ-45 connector on other end of the cable to a KVM port on the 16-port IP KVM.

7. Repeat Step 1. through Step 7. for all computers to be connected to the KVM ports.

8. If any user is using a PC with Windows XP server pack 2 installed and Internet Explorer 5 or 6 to remotely administer a connected server, make sure the procedure under “Avoiding Internet Explorer Conflicts” on page 89 has been done on the PC.

9. If this is a first-time installation, go to “Making a Direct Connection for Network Configuration” on page 63.

Making a Direct Connection for Network Configuration

The system administrator must specify basic network settings on the 16-port IP KVM before administrators can connect to and manage the unit and the connected devices through a browser. To prepare to perform necessary basic network configuration, make a direct connection to the 16-port IP KVM by doing one of the following:

- Connect a terminal or computer to the CONSOLE port.

  See "To Connect to the Console Port" on page 63.
- Connect a keyboard, monitor, and mouse to the keyboard, monitor, and mouse connectors on the 16-port IP KVM.

  See "To Connect to the User 1 Management Port" on page 64.

See "Enabling Access to the Web Manager without Making a Direct Connection" on page 81, if desired, for other procedures that require advanced system administration expertise.

▼ *To Connect to the Console Port*

Perform the following steps to connect a computer to the console port of the 16-port IP KVM. This procedure assumes that you know how to use a terminal emulation program.

On a PC, ensure that HyperTerminal or another terminal emulation program is installed on the Windows operating system. On a computer running a UNIX-based operating system, such as Solaris or Linux, make sure that a compatible terminal emulator such as Kermit or Minicom, is installed.

1. Connect an RJ-45 serial cable to the console port on the 16-port IP KVM.
2. Connect the other end to a USB serial adapter or DB-9 connection on the computer.
3. Using a terminal emulation program installed on a computer, start a session with the following console port settings:

Serial Speed: **9600** bps	Stop Bits: **1**
Data Length: **8** bits	Flow Control: **None**

Parity: **None**	ANSI emulation

4. Go to Chapter 2. “Powering On the 16-port IP KVM and Connected Devices” on page 64.

▼ *To Connect to the User 1 Management Port*

1. Plug the station's monitor, keyboard, and mouse cables to the Keyboard, Video, and Mouse connectors, labelled User 1, on the 16-port IP KVM.
2. Go to “Powering On the 16-port IP KVM and Connected Devices” on page 64.

Powering On the 16-port IP KVM and Connected Devices

The 16-port IP KVM components are hot pluggable, but components of connected devices, such as the PS/2 keyboard and mouse ports on a computer, may not be hot pluggable. Turn off power to all devices before connecting them. Power on connected devices again only after the 16-port IP KVM is powered on.

▼ *To Power On the 16-port IP KVM*

1. Make sure the 16-port IP KVM’s power switch is off.

   The power is off when the side of the power switch with the circle is pressed down.
2. Plug in the power cable.
3. Turn the 16-port IP KVM’s power switch on.

   The 16-port IP KVM beeps once.

▼ *To Power On Connected Devices*

Do this after “xConnecting Servers to the KVM Ports” on page 58.

- Turn on the power switches of the connected computers and devices.

Performing Basic Network Configuration

The administrator must specify basic network settings before regular users can connect to and manage the 16-port IP KVM and the connected devices through a browser. Do one of the following to assign a fixed IP address to the 16-port IP KVM, and to specify the netmask and other networking parameters:

- Through a console connection, log on and use the wiz command.

  See “Configuring Basic Networking Using the wiz Command” on page 66.
- Through a local KVM connection, log on to the OSD and configure networking through the network screen.

  See “Configuring Basic Networking Using the OSD” on page 69.

Before you start, collect the following network information from the administrator of the network where the 16-port IP KVM is to reside.

□ Hostname:	
□ 16-port IP KVM’s public IP address:	
□ Domain name:	
□ DNS server’s IP address:	
□ DefaultGateway address:	
□ Network mask:	
□ 16-port IP KVM’s MAC address (from the label on the bottom):	
□ NTP server’s IP address (if you are using a time/date server):	

Note: The following procedures tell you to disable DHCP. Enabling DHCP requires a DHCP server at your site. See “Considerations When Choosing Whether to Enable DHCP” on page 49 for more details and see “To Use a Dynamic IP

Address to Access the Web Manager” on page 82 for the tasks that must be performed.

Configuring Basic Networking Using the wiz Command

The following procedures require a hardware connection already made between the 16-port IP KVM’s console port and the COM or USB port of a computer, as described under “To Connect to the Console Port” on page 63.

▼ To Logged On to the 16-port IP KVM Through the Console

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

```
 16-port IP KVM login: root
Password: apc
```

As shown in the previous screen, the default password is “apc.” If the password has been changed from the default, use the new password.

▼ To Change the Password Through the Console

If the default password “apc” is still in use, change the root password.

Note: Changing the default password closes a security hole that could be easily exploited.

1. Enter the **passwd** command.

```
[root@16-port IP KVM /]# passwd
```

2. Enter a new password when prompted.

```
New password: new_password

Re-enter new password: new_password

Password changed
```

3. Enter the “saveconf” command to save the configuration to flash.

```
[root@ 16-port IP KVM /]# saveconf
```

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

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

```
[root@ 16-port IP KVM /]# wiz
```

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

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

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

```
Hostname [ 16-port IP KVM]:
boston_branch_kvm
```

4. Press Enter to disable DHCP.

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

5. Enter a public IP address to assign to the 16-port IP KVM.

```
System IP[192.168.160.10]: public_IP_address
```

6. Enter the domain name.

```
Domain name[apc.com]: domainname
```

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

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

8. Enter the IP address for the gateway.

```
Default Gateway[eth0] : gateway_IP_address
```

9. Enter the netmask for the subnetwork.

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

10. To apply and confirm these parameters, see “To Apply and Confirm the Network Parameters Defined Using the wiz Command” on page 68.

▼ *To Apply and Confirm the Network Parameters Defined Using the wiz Command*

This procedure must be completed immediately after defining network parameters using the wiz command as described in “To Use the wiz Command to Configure Network Parameters” on page 67

1. Review the values of all the network configuration parameters, as shown in the following screen example. The values shown are for example only.

```
Current configuration:

Hostname : kvm
DHCP : disabled
System IP : 192.168.45.32
Domain name : apc.com
drwxr-xr-x    1 root
Primary DNS Server :
192.168.44.21
Default Gateway : 198.168.44.1
Network Mask : 255.255.252.0
Are all these parameters
correct? (y/n) [n] :
```

2. Enter **y** if the values shown are correct, or press Enter.

3. The following prompt appears when “y” is entered.

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

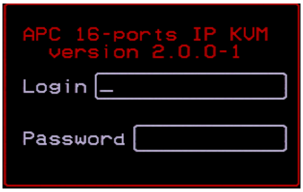
4. Enter **y** to save the changes.

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

5. To confirm the configuration, enter the `ifconfig` command.
6. The new network parameters display.
7. Log out from the terminal session.
8. In a HyperTerminal application on a Windows PC, go to “File > Exit”.
9. If performing a first-time installation, go to “Completing Configuration Using the Web Manager” on page 78.

Configuring Basic Networking Using the OSD

This procedure requires a hardware connection already made between the 16-port IP KVM’s KVM management port and a local monitor, keyboard, and mouse, as described under “To Connect to the User 1 Management Port” on page 64. After the 16-port IP KVM and monitor are powered on, the OSD login screen appears.



APC 16-ports IP KVM
version 2.0.0-1

Login _

Password

The following table shows how to perform common actions described in the following procedures when working with the OSD.

Table 2-1: OSD Equivalents for Common Actions

Action	OSD Equivalent
Press OK.	Tab to the OK button and press the Enter key on your keyboard.
Enter <any value>.	Type the value in the appropriate field and press the Enter key.

Table 2-1: OSD Equivalents for Common Actions (Continued)

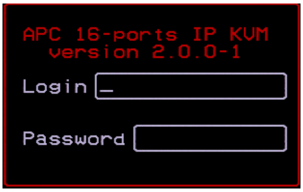
Action	OSD Equivalent
Save changes.	Tab to the Save button and press the Enter key.
Select <an option>.	Press an arrow key to navigate. Select the menu option and then press the Enter key.
Go to a specific screen, as in: "Go to 'Configure > Users and Groups > Local Users > Change Password'."	From the Main menu, select the first option shown in the menu path; "Configure" in the example. On the next menu, select the next option shown after the > (right angle bracket); "Users and Groups" in the example. Repeat until you select the last option in the menu path.
Exit the OSD.	Click the X box on the upper right of the viewer. If you are on the Main Menu, you can select Exit.

Note: If your keyboard has a Return key instead of an Enter key, press the "Return" key when you see "Enter."

▼ *To Logged On to the OSD*

1. On the OSD login screen, enter "apc" as the Login name.
2. Enter the password.

   The default password is "apc." If the password has been changed from the default, use the current password.



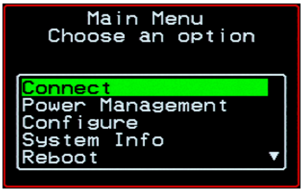
APC 16-ports IP KVM
version 2.0.0-1

Login _

Password

3. Press Enter.

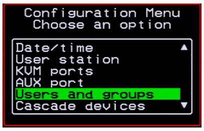
   The OSD Main Menu appears.

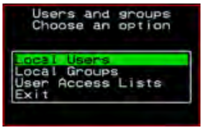


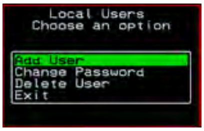
4. If you are performing an initial configuration of basic networking parameters, go to “To Change a Password Using the OSD” on page 71; otherwise, go to “To Configure Network Parameters Using the OSD” on page 73.

▼ To Change a Password Using the OSD

1. From the OSD Main Menu, go to Configure > Users and Groups > Local Users > Change Password.

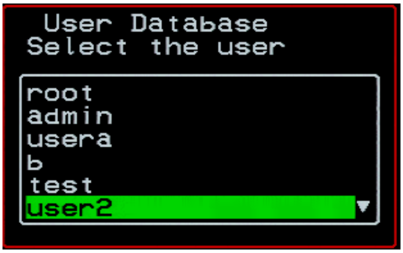






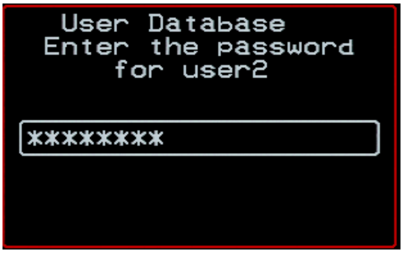
Warning! If the “apc” password has not been changed, change it now. Changing the default password closes a security hole that could be easily exploited.

2. Select the user name from the list of users on the User Database screen.



User Database
Select the user

3. Enter a new password.



User Database
Enter the password
for user2

****

4. Re-enter the new password.

   The password confirmation dialog box appears.

5. Press Enter.

   The Local Users menu appears.

6. Select Exit or press the Esc key to exit the Local Users menu.

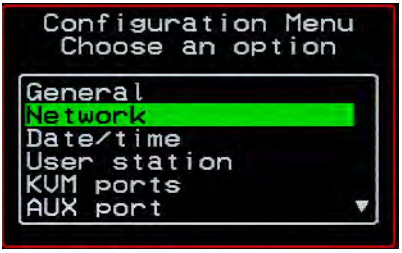
   You can use the Exit or Cancel option or the Esc key to exit any window on the OSD.

7. If you are performing an initial configuration of basic networking parameters, see “To Configure Network Parameters Using the OSD” on page 73.

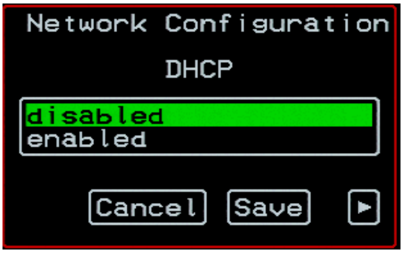
8. Otherwise, go to the appropriate menu option for your next task.

▼ *To Configure Network Parameters Using the OSD*

1. From the OSD Main Menu, go to Configure > Network.

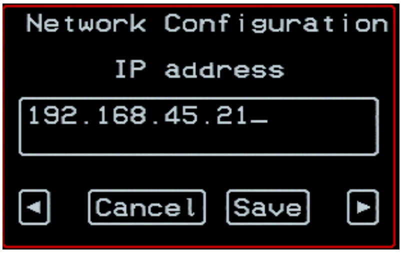


The DHCP form appears.



2. Select the “disabled” option and press Enter.

The IP address form appears.



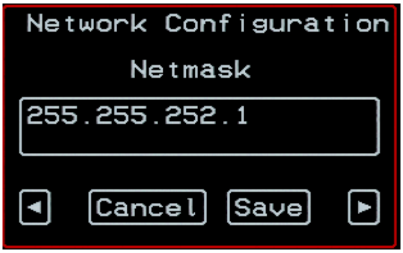
Network Configuration

IP address

192.168.45.21_

3. Enter the IP address for the 16-port IP KVM and press Enter.

The Netmask form appears.



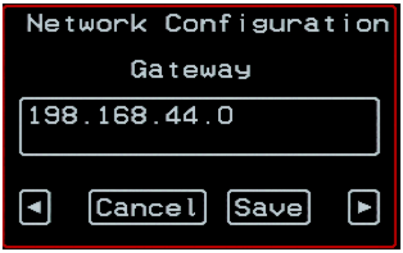
Network Configuration

Netmask

255.255.252.1

4. Enter the netmask (in the form 255.255.255.0) and press Enter.

   The Gateway form appears.



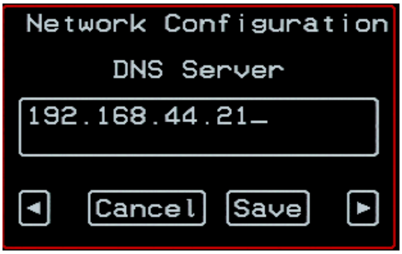
Network Configuration

Gateway

198.168.44.0

5. Enter the IP address for the gateway and press Enter.

   The DNS Server form appears.



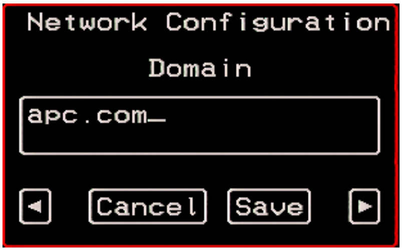
Network Configuration

DNS Server

192.168.44.21_

6. Enter the IP address for the DNS server and press Enter.

   The Domain form appears.



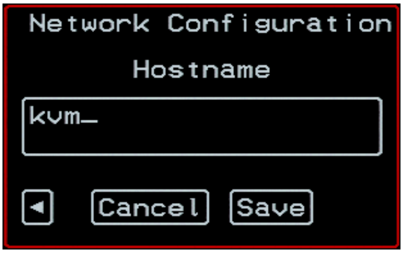
Network Configuration

Domain

apc.com_

7. Enter the domain name and press Enter.

   The Hostname form appears.



Network Configuration

Hostname

kvm_

8. Enter the hostname for the 16-port IP KVM and save the changes to complete the basic network configuration.

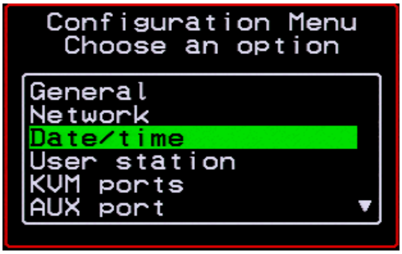
   The Configuration menu appears.

   - To configure an NTP (network time protocol) server or to enter the date and time manually, go to “To Set the Time and Date Using the OSD” on page 76.
   - If you do not wish to configure the time and date at this time, and if you are performing an initial configuration of basic networking parameters, go to: “Completing Configuration Using the Web Manager” on page 78.
   - Otherwise, go to the appropriate menu option for your next task or exit from the OSD.

▼ *To Set the Time and Date Using the OSD*

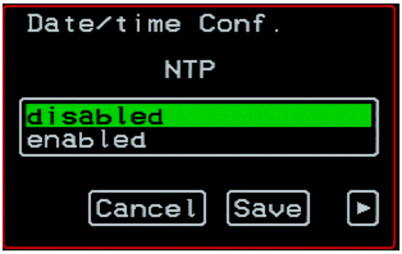
1. From the Main menu of the OSD, go to Configure.

The Configuration menu appears.



2. Select Date/time.

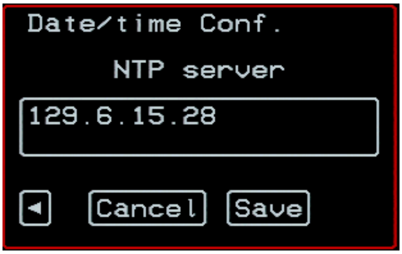
The Date/time conf. form appears.



3. To enable the NTP time and date server, do the following.

a. On the Date/time conf. form, select the “enabled” option.

The NTP server screen appears



NTP server
129.6.15.28

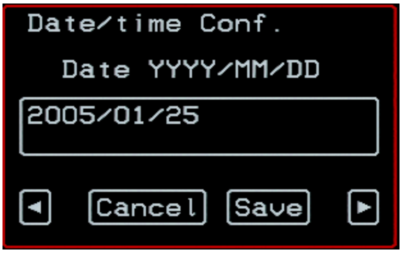
b. Enter the IP address of the NTP server.

c. Save the changes.

4. To enter the date and time manually, do the following.

a. On the Date/time conf. form, select disabled.

The Date entry screen appears.



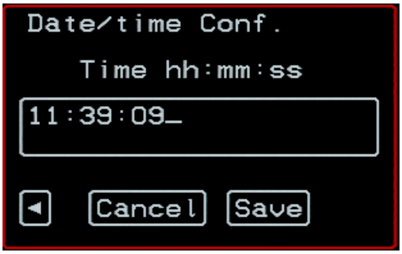
Date/time Conf.

Date YYYY/MM/DD

2005/01/25

b. Enter the date in the format shown and press Enter.

The Time entry screen appears.



Date/time Conf.

Time hh:mm:ss

11:39:09_

c. Enter the time in the format shown and save the changes.

If you are performing an initial configuration of basic networking parameters, go to: “Completing Configuration Using the Web Manager” on page 78.

Otherwise, go to the appropriate menu option for your next task.

Completing Configuration Using the Web Manager

The “apc” user can administer the 16-port IP KVM and its connected devices through the Web Manager without doing any additional configuration.

The following list shows other common configuration tasks:

- Enable direct login to ports from the Web Manager login screen
- Set up local or remote data buffering (to save console input to a log file) and specify alarms
- Set up logging of system messages to a syslog server
- Configure power management for the AUX port if the port is connected to an optional APC rPDU
- Choose among authentication methods and specify authentication servers
- Specify optional encryption levels
- Configure rules for a firewall
- Configure a time and date (NTP) server or set the time and date manually

See “Web Manager for Administrators” on page 101 for procedures for performing the common 16-port IP KVM administration tasks listed in this section.

Following is a brief list of ways the admin can assign tasks to other users:

- Let other users manage servers or rPDUs without being able to make changes to the 16-port IP KVM configuration
- Assign users or groups to specific ports, restricting users to a limited set of devices
- Let other users share all administration of the 16-port IP KVM

Changing Default Passwords

For security purposes, the root and admin users must change their default passwords as soon as possible. Not changing the default passwords leaves a big security hole that can be exploited.

▼ *Changing admin’s Default Password [Web Manager]*

1. Bring up the Web Manager.
2. Log in as apc using the default password, “apc”.
3. In Wizard Mode, go to **Step2: Access**.
4. Select “apc” from the Users List.
5. Click the “Change Password” button.
6. Enter the password into the New Password field.
7. Enter the password again into the Repeat New Password field.
8. Click OK when done.

▼ *Changing the Root Password [Command Line]*

1. Verify that a terminal or a computer with a terminal emulator is connected to the console port on the 16-port IP KVM.
2. From the terminal or terminal emulator, log on to the console port as **root**, using the existing password. [The default password is “apc”.]

```
KVM login: root
```

Password: apc

a. Enter the **passwd** command.

```
[root@KVM /]# passwd
```

b. Enter a new password when prompted.

```
New password: new_password

Re-enter new password:
new_password

Password changed
```

3. Save the new password by entering the **saveconf command.**

```
[root@KVM /]# saveconf
```

4. Log out.

```
[root@KVM /]# logout
```

5. Close the terminal session.
6. In a HyperTerminal application on a Windows PC, choose File > Exit or F4.

▼ *Changing Default Passwords [OSD]*

This procedure requires a hardware connection already made between the 16-port IP KVM's KVM management port and a local monitor, keyboard, and mouse, as described in “To Connect to the User 1 Management Port” on page 64. Do the following to change the passwords for the root and admin users.

1. Log into the OSD.
2. From the Main Menu, select the Configure option.
3. From the Configure Menu, select the Users and Groups option.
4. From the list of users on the User Database screen, select the user name.
5. On the “Enter the Password” screen, enter the new password.
6. On the password confirmation window, re-enter the password.
7. Select OK.
8. Select ESC on your keyboard to go back to the Configure menu.

9. Select Save/Load Config.
10. Select Save Configuration to save the configuration to flash.

Enabling Access to the Web Manager without Making a Direct Connection

This section describes additional alternatives for enabling access to the Web Manager that do not require making a direct connection. Both of the two following approaches require an experienced administrator to configure:

- The 16-port IP KVM ships with a default IP address: 192.168.160.10. You can use the default address to bring up the Web Manager, assign a fixed IP address to the 16-port IP KVM and specify other network parameters without making a direct connection. To do so, you must temporarily change the IP address of a computer on the same subnet. See “To Use the Default IP Address to Access the Web Manager” on page 81.”
- DHCP is enabled on the 16-port IP KVM by default. If you have network access to the DHCP server for the 16-port IP KVM, and if you are able to discover the 16-port IP KVM’s dynamically assigned IP address, you do not need to make a direct connection. See “To Use a Dynamic IP Address to Access the Web Manager” on page 82.”

▼ *To Use the Default IP Address to Access the Web Manager*

The default IP address for the 16-port IP KVM 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 16-port IP KVM.

1. Set up the APC 16-port IP KVM.

   See “Setting Up the 16-port IP KVM” on page 55.

2. Connect computers and other devices to be managed through the 16-port IP KVM.

   See “xConnecting Servers to the KVM Ports” on page 58.

3. Power on the 16-port IP KVM and connected devices.

See “Powering On the 16-port IP KVM and Connected Devices” on page 64.

4. On a computer that resides on the same subnet with the 16-port IP KVM, change the network portion of the IP address of that computer to `192.168.160.`*`NN`*, where NN is not 10, and change the Netmask to `255.255.255.0`.

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

5. Bring up a browser on the computer whose address you changed, enter the 16-port IP KVM’s default IP address (`http://192.168.160.10`)to bring up the Web Manager, and log on.

6. To allow subsequent use of the Web Manager from any computer, go to the Wizard: “Step 1: Network Settings” to change the default IP address to a fixed public IP address and to configure the other basic network parameters and save them to Flash.

7. Restore the computer’s IP address to its previous IP address.

8. Finish configuring 16-port IP KVM users and ports using the Web Manager.

▼ *To Use a Dynamic IP Address to Access the Web Manager*

This procedure assumes that DHCP is enabled on the 16-port IP KVM.

1. Set up the APC 16-port IP KVM.

   See “Setting Up the 16-port IP KVM” on page 55.

2. Connect computers and other devices to be managed through the 16-port IP KVM.

   See “xConnecting Servers to the KVM Ports” on page 58.

3. Power on the 16-port IP KVM and connected devices.

   See “Powering On the 16-port IP KVM and Connected Devices” on page 64.

4. To obtain the 16-port IP KVM’s current IP address from the console port do the following:

a. Using the console port, log on as “root.”

See “To Connect to the Console Port” on page 63 for instructions if needed.

b. Execute the command

```
ifconfig eth0
```

Output similar to the following will appear. The line in bold type face labelled “inet address” lists the IP address of the 16-port IP KVM:

```
eth0  Link encap:Ethernet  HWaddr
       00:60:2E:01:4F:FC
      inet addr:192.168.50.72
       Bcast:192.168.51.255
       Mask:255.255.252.0
      UP BROADCAST RUNNING MULTICAST
       MTU:1500  Metric:1
      RX packets:7282803 errors:43
       dropped:0 overruns:0 frame:43
      TX packets:167335 errors:3
       dropped:0 overruns:0 carrier:3
      collisions:0 txqueuelen:100
      RX bytes:539070845 (514.0 MiB)  TX
       bytes:18911603 (18.0 MiB
      Base address:0xe00
```

5. Finish configuring 16-port IP KVM users and ports using the Web Manager.

Preconfiguring the 16-port IP KVM for Remote Installation

This section provides procedures that list the tasks for preconfiguring the 16-port IP KVM and setting it up in a separate location. You might preconfigure a 16-port IP KVM, for example, if you need to ship the 16-port IP KVM to a remote location that does not have a system administrator.

If you would prefer to have APC preconfigure the 16-port IP KVM with basic network parameters at APC before it is shipped, ask your APC contact to put you in touch with APC professional services. For a fee, they can preconfigure the 16-port IP KVM with parameters you supply.

▼ *To Preconfigure the 16-port IP KVM*

1. Perform the tasks listed in the following table to preconfigure the 16-port IP KVM for installation at another location.

Task	Where Documented
Make a direct connection to prepare for basic network configuration.	“Making a Direct Connection for Network Configuration” on page 63
Power on the 16-port IP KVM and connected devices.	“Powering On the 16-port IP KVM and Connected Devices” on page 64
Perform basic network configuration.	“Performing Basic Network Configuration” on page 65

2. If you ship the 16-port IP KVM to a remote location for installation, also send the following:
    - A record of the 16-port IP KVM’s fixed IP address and other network parameters.
    - A copy of the instructions under “To Set Up a Preconfigured 16-port IP KVM” on page 85.

▼ *To Set Up a Preconfigured 16-port IP KVM*

Perform the tasks shown in the following table with a 16-port IP KVM that has been preconfigured as described in“To Preconfigure the 16-port IP KVM” on page 84. After the tasks are completed in the order shown, a remote administrator can bring up the Web Manager by entering the 16-port IP KVM’s fixed IP address in a browser.

	Task	Where Documented
1	Set up the APC 16-port IP KVM.	“Setting Up the 16-port IP KVM” on page 55
2	Make an Ethernet connection.	“Making an Ethernet Connection” on page 57
3	Connect computers and other devices.	“xConnecting Servers to the KVM Ports” on page 58
4	Power on the 16-port IP KVM and connected devices.	“Powering On the 16-port IP KVM and Connected Devices” on page 64

Additional Configuration Tasks

See the following sections for other procedures.

Task	Where Documented/Notes
Avoiding Conflicting Mouse Settings	“Avoiding Conflicting Mouse Settings” on page 86
Avoiding Internet Explorer Conflicts	“Avoiding Internet Explorer Conflicts” on page 89
Assigning Your Own TCP Viewer Port Address	“TCP Ports” on page 21

Avoiding Conflicting Mouse Settings

The administrator of each computer connected to one of the 16-port IP KVM's KVM server ports must perform one of the procedures in this section. Performing the procedure prevents conflicts between the mouse settings on the connected computers and the mouse settings on computers used to do administration through the 16-port IP KVM.

Work with the administrators of computers to be connected to the 16-port IP KVM to ensure that one of the following procedures is performed, depending on the type of computer:

- "To Prevent Mouse Conflicts [Windows XP/Windows 2003]" on page 86
- "To Prevent Mouse Conflicts [Windows 2000 / ME]" on page 87
- "To Prevent Mouse Conflicts [Windows 95/98/NT]" on page 87
- "To Prevent Mouse Conflicts [Linux]" on page 88

▼ *To Prevent Mouse Conflicts [Windows XP/ Windows 2003]*

1. As administrator, on the Start Menu, go to: Control Panel > Mouse > Pointer Options.
2. To disable "Enhance pointer precision," click the check box to clear it.
3. To set the motion speed to medium, move the slider to the middle of the "Select a pointer speed" scale.
4. Go to: Control Panel > Display > Appearance > Effects
5. To disable transition effects, click both transition effects check boxes to clear them.
6. Click OK.

▼ *To Prevent Mouse Conflicts [Windows 2000 / ME]*

1. As administrator, on the Start menu, go to: Settings > Control Panel > Mouse > Pointer Options.
2. To set the mouse pointer acceleration to none, do the following:
   a. Click the **Advanced** button.

      The Advanced Setting Pointer Speed dialog box appears.

   b. On Windows ME, clear the **Pointer acceleration** check box.

   c. On Windows 2000, clear the **Enable pointer acceleration** check box.

   d. Click **OK**.
3. Set the motion speed to medium by moving the slider to the middle of the **Adjust how fast the pointer moves** scale.
4. Click **OK**.
5. To disable transition effects do the following:
   a. Go to: Control Panel > Display > Effects.

   b. Clear **Use transition effects for menus and tooltips**.

   c. Click **OK**.

▼ *To Prevent Mouse Conflicts [Windows 95/98/NT]*

1. As administrator, on the Start menu, go to: Settings > Control Panel > Mouse > Motion.
2. Set the motion speed by moving the slider to the lowest setting on the “Pointer Speed” scale.
3. Go to: Settings > Control Panel > Display > Effects > Advanced Settings for Pointer Speed.
4. Disable window, menu, and list animation by clearing “Animate windows, menus, and lists.”

▼ *To Prevent Mouse Conflicts [Linux]*

This procedure assumes that you have the login name and password for an account configured with the following types of access:

- Access on the 16-port IP KVM to the port where the computer is connected
- Access as root on the connected computer

1. Log into the APC Web Manager with the user name and password of an account that has been configured to access the port where the computer is connected.
2. Go to Expert > Access > Connect to Server.
3. From the drop-down list select the port number or alias for the computer, and click the Connect button.
4. If port authentication is configured, log on to the server as root.

   The root prompt appears.

```
#
```

5. Disable the mouse pointer acceleration and threshold settings by entering the **XSET m 0** command:

```
# xset m 0
```

6. Exit the Remote Viewer.

Note: Repeat this procedure to synch mouse settings after every reboot of the connected computer.

Avoiding Internet Explorer Conflicts

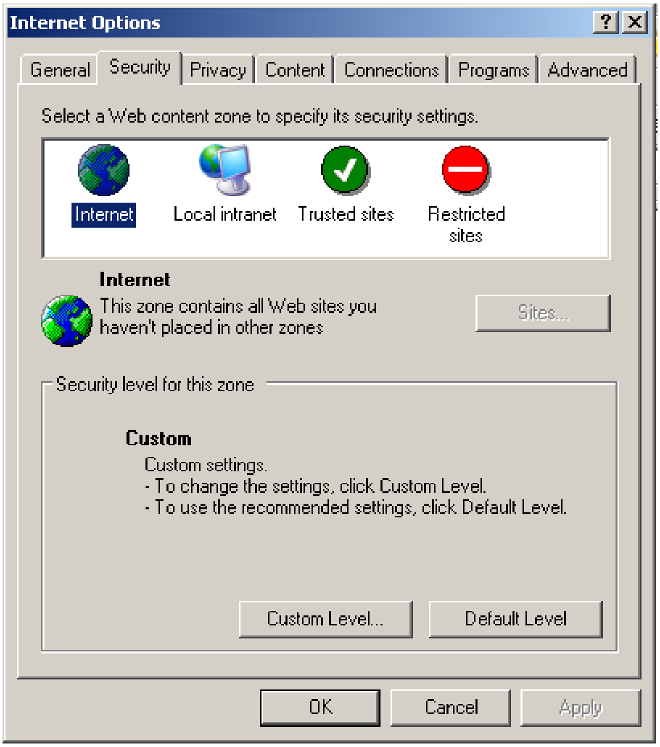
The procedure described in this section must be performed on an PC if all the following are true:

- A PC running Windows XP with Service Pack 2 is being used to remotely administer a computer connected to a KVM server port
- Internet Explorer (IE) is used to bring up the APC Web Manager and the Remote Viewer

▼ *To Modify IE Security Settings*

1. From the Internet Explorer menu bar, select **Tools** > **Internet Options** > **Security** Tab.

   The **Security** form appears.



Internet Options

Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

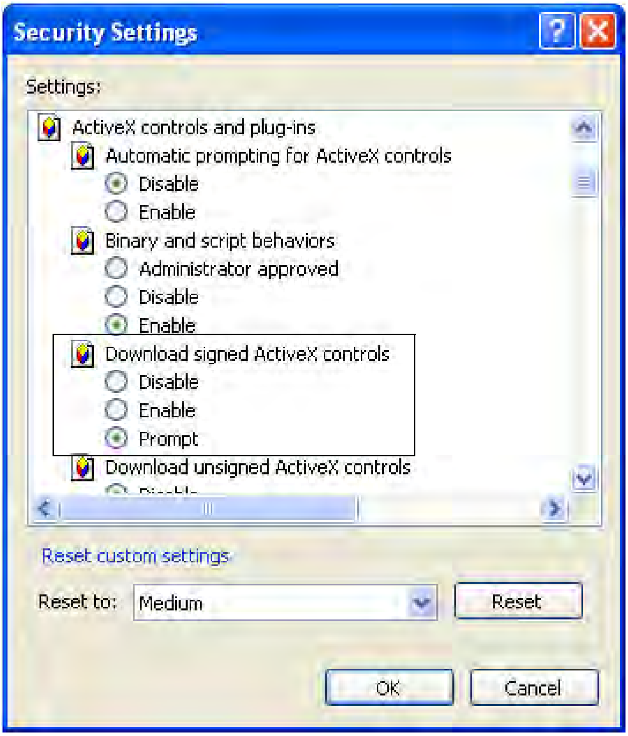
Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

2. Click the **Custom Level** button.

   The Security Settings form appears.

3. On the Security Settings form, go to **ActiveX controls and plug-ins** > **Download signed ActiveX controls.**



Security Settings

Settings:

ActiveX controls and plug-ins
- Automatic prompting for ActiveX controls
  - ● Disable
  - ○ Enable
- Binary and script behaviors
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
- Download signed ActiveX controls
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Download unsigned ActiveX controls

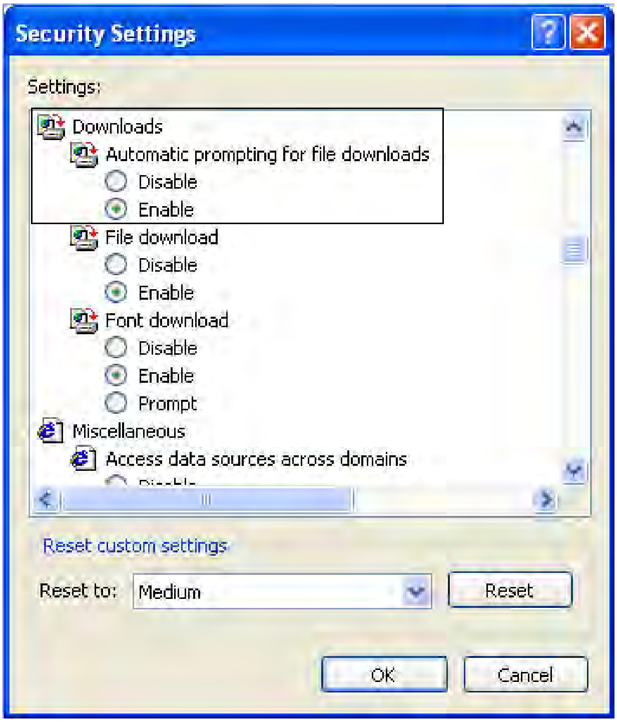
Reset custom settings

Reset to: Medium

4. Select either **Enable** or **Prompt**.

5. If you selected **Enable**, press the **OK** button.

6. If you selected **Prompt**, go to **Downloads** > **Automatic prompting for file downloads**, and select **Enable**.



Security Settings

Settings:

Downloads

Automatic prompting for file downloads

○ Disable

● Enable

File download

○ Disable

● Enable

Font download

○ Disable

● Enable

○ Prompt

Miscellaneous

Access data sources across domains

Reset custom settings

Reset to: Medium

7. Select the **OK** button.

Chapter 3
Advanced Installation Procedures

16-port IP KVM supports the installation of related components, which are used to extend the access to and control of the 16-port IP KVM and its connected devices.

The following table lists the components that can be installed with the 16-port IP KVM and shows the page numbers where the tasks are described in more detail.

External modems	Page 94
APC rPDU	Page 95
Cascaded KVM units	Page 95
APC CAT5/IP KVM Console Extender	Page 97

Connecting an External Modem

You can connect a modem to the AUX port on the 16-port IP KVM. After the modem is connected and properly configured, you can use it to dial in to the 16-port IP KVM when the production network or management network is down, or when Ethernet access is unavailable.

▼ *To Connect an External Modem to the AUX Port*

This procedure requires the following cables and connectors:

- A straight through cable with an RJ-45 connector on one end and the appropriate connector or adapter (USB, DB-9, or DB-25) on the other end for connecting the AUX port to the appropriate port on the external modem.
- A phone cord with RJ-11 connectors on both ends for connecting the modem to the phone line.

1. Connect the RJ-45 end of the cable to the AUX port on the 16-port IP KVM.
2. Connect the other end of the cable to the modem.
3. Use a phone cable to connect the jack on the modem to a live telephone jack at your site.
4. Configure the AUX port for PPP.

   See “AUX Port” on page 218 and “To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219.

Connecting APC rPDUs to the 16-port IP KVM

You can control an APC rPDU by connecting it to the AUX port on the 16-port IP KVM.

▼ *To Connect an APC rPDU to the AUX Port*

1. Use an APC KVM to APC Switched Rack PDU RJ-45 to RJ-12 cable to connect the AUX port on the 16-port IP KVM to the RJ-12 serial port of your APC Switched rPDU.
2. Configure the AUX port for power management. See “To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219.

After the rPDU is connected, you may want to perform one or more of the following tasks:

Task	Where Documented
Manage the power of devices connected to configured rPDU units.	• Web Manager – “To Power On, Power Off, or Cycle Devices Plugged into rPDU Outlets” on page 288 • OSD – “Power Management Menu” on page 300
Control the power of a device while connected to it through a KVM port.	• Web Manager – “To Power On, Power Off, or Reboot the Connected Server” on page 280 • OSD – “To Power On, Power Off, or Cycle Devices Plugged into rPDU Outlets” on page 288

Connecting Cascaded KVM Units to the Primary 16-port IP KVM

The 16-port IP KVM supports the cascading of two types of secondary KVM devices: the 16-port IP KVM and the 16-port CAT5 KVM. See “To Connect a

Secondary KVM Unit to the Primary 16-port IP KVM” on page 96 for instructions on cascading KVM devices to the 16-port IP KVM.

For background information on cascading, see “Cascaded Devices” on page 22.

▼ *To Connect a Secondary KVM Unit to the Primary 16-port IP KVM*

1. Power off all KVM hardware and connected devices.
2. To connect to the User 2 port of a secondary KVM unit, do the following:
   a. Connect one end of a CAT5 cable to a KVM port on the primary 16-port IP KVM.

   b. Connect the other end of the CAT5 cable to the User 2 port on the secondary KVM unit.
3. To connect to the User 1 port of a secondary KVM unit, do the following:
   a. Connect one end of a CAT5 cable to a KVM port on the primary 16-port IP KVM.

   b. Connect the other end of the CAT5 cable to a KVM Server Module.

   c. Connect the Server Module’s VGA and PS/2 connectors to the User 1 port on the secondary KVM unit.

   See “xConnecting Servers to the KVM Ports” on page 58 for detailed instructions on how to connect devices to KVM ports using KVM Server Modules.
4. Repeat steps 1 through 3 for each secondary KVM unit to be connected to the primary 16-port IP KVM.

Installing the APC CAT5/IP KVM Console Extender

With a CAT5 cable up to 500 feet long, the Console Extender can be connected to the User 2 port of the 16-port IP KVM unit, enabling the extended user to perform local administration tasks or to select the local keyboard, video, and mouse console between a local station and a server connected to the 16-port IP KVM.

	Tasks	Where Documented/Notes
1	Place the Console Extender on a desk or table up to 500 feet away from the 16-port IP KVM.	You can use a CAT5 cable of up to 500 feet long to extend the local administration of the 16-port IP KVM.
2	Connect the Console Extender to the 16-port IP KVM.	"To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM" on page 98.
3	Connect a keyboard, monitor, and mouse to the Console Extender.	"Options for Accessing the APC CAT5/IP KVM Console Extender" on page 98
4	Supply power to and turn on the Console Extender.	"Supplying Power to the APC CAT5/IP KVM Console Extender" on page 99
5	Use the Console Extender to control the 16-port IP KVM.	"Controlling the OSD Through the APC CAT5/IP KVM Console Extender" on page 366

Shipping Box Contents APC CAT5/IP KVM Console Extender

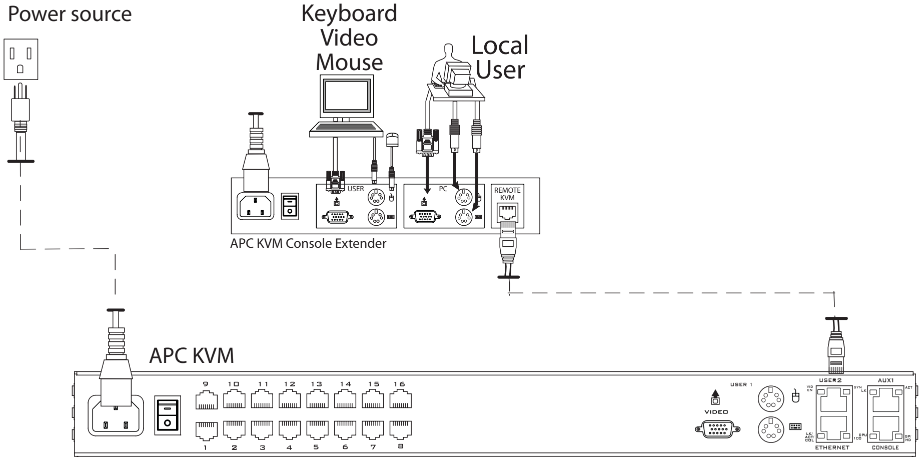
The shipping box for the Console Extender contains the following items:

- APC CAT5/IP KVM Console Extender
- One NEMA 5-15 power cable
- One IEC320 power cable
- One Console (CAT5) cable
- One KVM cable

- Documentation CD
- Product Registration Form
- Declaration of Conformity

▼ To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM

1. Insert one end of a CAT5 cable into the Remote KVM port on the Console Extender.
2. Insert the other end of the CAT5 cable into the User 2 port on the 16-port IP KVM.



Options for Accessing the APC CAT5/IP KVM Console Extender

The Console Extender offers two options for monitor, keyboard, and mouse control. Administrators can connect a dedicated keyboard, monitor, and mouse directly to the Console Extender. Or administrators can connect the Console Extender to their local work station in order to toggle the keyboard, monitor, and mouse control between the 16-port IP KVM and the local computer.

▼ To Connect the APC CAT5/IP KVM Console Extender to a Dedicated Keyboard, Monitor, and Mouse

1. Connect your monitor's VGA cable to the USER VGA port on the Console Extender.
2. Connect your keyboard's PS/2 cord to the USER keyboard PS/2 port on the Console Extender.
3. Connect your mouse's PS/2 cord to the USER mouse PS/2 port on the Console Extender.

▼ To Connect the APC CAT5/IP KVM Console Extender to the Local Work Station

1. Connect your monitor's VGA cable to the PC VGA port on the Console Extender.
2. Connect your keyboard's PS/2 cord to the PC keyboard PS/2 port on the Console Extender.
3. Connect your mouse's PS/2 cord to the PC mouse PS/2 port on the Console Extender.
4. Use a KVM cable to connect the VGA port, PS/2 keyboard port, and PS/2 mouse port on the back of your PC to the PC VGA port, PS/2 keyboard port, and PS/2 mouse port on the Console Extender.

Note: When the Console Extender is connected to the local PC, as described in the previous procedure, the Console Extender receives power from the PC and does not need to be plugged into a power supply.

Supplying Power to the APC CAT5/IP KVM Console Extender

The Console Extender can be powered by a power cord connected to its power supply port, or it can be powered by the local work station. Power can be transmitted from the PC through a KVM cable to the Console Extender.

▼ *To Power On the APC CAT5/IP KVM Console Extender*

1. If the Console Extender has its own dedicates keyboard, monitor, and mouse connected to its USER port, do the following:

   a. Make sure the 16-port IP KVM’s power switch is off.

   b. Plug in the power cable.

   c. Turn the 16-port IP KVM’s power switch on.

2. If the Console Extender is connected to the local PC, turn the 16-port IP KVM’s power switch on.

   The power is supplied by the PC. See “To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM” on page 98 for instructions on connecting the Console Extender to the local PC.

Chapter 4
Web Manager for Administrators

This chapter is for administrators who use the Web Manager for managing and configuring the 16-port IP KVM. Two types of administrators can access all the Web Manager functions described in this chapter:

- An administrator who knows the password for the “apc” account, which is configured by default
- An optionally configured regular user whose account is in the “admin” group (See “Users & Groups” on page 151 for how the “apc” user adds a regular user account and adds the account to the admin group.)

Administrators whose accounts are configured without administrative access can log on to the Web Manager as regular users and then access connected devices, as described in Chapter 5. “Web Manager for Regular Users” on page 245. For more background about the differences between user types, see “Types of Users” on page 14.

Before following the procedures in this chapter, review “Prerequisites for Using the Web Manager” on page 19, if needed, to make sure that you can connect to the Web Manager.

The sections listed in the following table give background information related to 16-port IP KVM 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.

Common Tasks

The following table lists common tasks that 16-port IP KVM administrators perform with links to the procedures.

Task	**Where Documented/Notes**
Set up other users to access connected devices without being able to make changes to the 16-port IP KVM configuration	• “To Add a User [Wizard]” on page 114 • “To Add a User [Expert]” on page 152
Assign users or groups to specific ports, restricting access to a limited set of devices	• “To Assign KVM Port Access to a User or Group” on page 156
Set up other users to share all administration of the 16-port IP KVM	• “To Add a User [Wizard]” on page 114 • “To Add a User [Expert]” on page 152
Enable direct login to ports from the Web Manager login screen	• To Enable Direct Access to KVM Ports
Set up logging of system messages to a syslog server	• “To Add a Syslog Server [Wizard]” on page 119 • To Delete a Syslog Server [Wizard] • To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert] • To Configure Creation of Alarms and Syslog Files for rPDUs

Task	Where Documented/Notes
Configure power management for the AUX port (if the port is connected to an optional APC rPDU)	• “To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219 • “To Configure a KVM Port for Power Management” on page 143
Manage power on an optional APC rPDU)	• “To Turn On, Turn Off, or Power Cycle Outlets” on page 125 • “To Edit an Outlet’s PwrOn Delay, PwrOff Delay, or Cycle Duration” on page 126 • “To View rPDU Information” on page 127 • “To Configure Users to Manage Specific Power Outlets” on page 128 • “To Specify or Change the Alias of an rPDU” on page 130 • “To Configure Creation of Alarms and Syslog Files for rPDUs” on page 130
Choose among authentication methods and specify authentication servers for logins to the 16-port IP KVM and for logins to devices connected to the 16-port IP KVM’s ports	• “To Configure an Authentication Method for 16-port IP KVM Logins” on page 162 • “To Configure an Authentication Method for KVM Port Logins” on page 163
Specify encryption levels for KVM ports	“To Configure Encryption on Port Connections [Expert]” on page 160
Configure rules for the 16-port IP KVM to filter packets like a firewall	• “To Add a Chain for IP Filtering” on page 198 • “To Edit A Chain for IP Filtering” on page 199 • “To Add a Rule for IP Filtering” on page 200 • “To Edit a Rule for IP Filtering” on page 197

Common Features of Administrators' Windows

The features of all Web Manager windows for 16-port IP KVM administrators are described in the following sections:

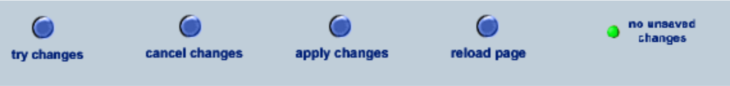
- Control and logout buttons and 16-port IP KVM Information

  See "Administrators' Control Buttons, Log Off Button, and 16-port IP KVM Information."
- Getting more information

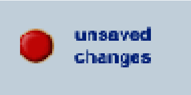
  See "Obtaining More Information" on page 105

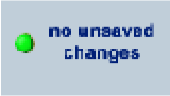
Administrators' Control Buttons, Log Off Button, and 16-port IP KVM Information

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

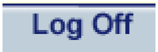
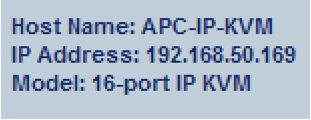


The following table describes the uses for each control button.

Button Name	Use
try changes	Tests the changes entered on the current form without saving them.
cancel changes	Cancels all unsaved changes.
apply changes	Applies all unsaved changes.
reload page	Reloads the page.
Help	Brings up the online help with information relating to the current form.
	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.

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

The following table describes the logout button and the other information that displays in the upper right corner of all Web Manager windows.

WIndow Area	Purpose
 	Click this button to log off.
 Host Name: APC-IP-KVM IP Address: 192.168.50.169 Model: 16-port IP KVM	Displays the hostname and IP address assigned during initial configuration (see “Performing Basic Network Configuration” on page 65). Also displays the model name of the 16-port IP KVM.

Obtaining More Information

Information about the purpose of each Web Manager form and the values to be specified on the form is available by clicking the Help button. For definitions of unfamiliar terms see the Glossary. For links to sections of the book where unfamiliar terms are discussed, see the Index.

Logging On to the Web Manager and Saving Changes

The following table lists procedures common to both Wizard and Expert mode.

To Log On to the Web Manager as Admin	Page 106
To Save Configuration Changes	Page 106

For procedures specific to each mode, see “Administrative Modes” on page 109.

▼ *To Log On to the Web Manager as Admin*

This procedure assumes that the prerequisites described under “Prerequisites for Using the Web Manager” on page 19 are done and that you can connect to the Web Manager.

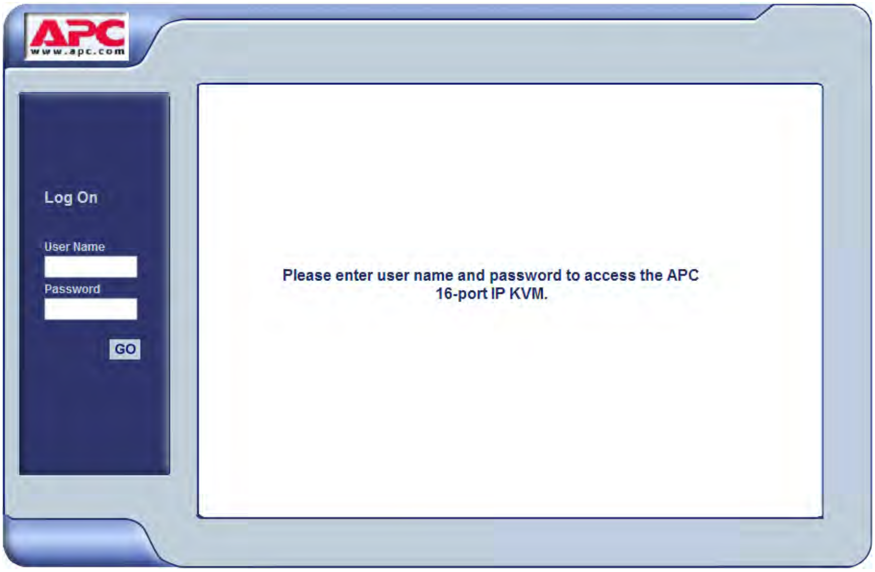
1. To bring up the Web Manager, enter the IP address of the 16-port IP KVM in the address (URL) field of a supported browser on a computer running a Windows operating system.

Note: Devices like the APC 16-port IP KVM that are installed in computer rooms are usually assigned fixed IP addresses. If DHCP is enabled, you must find out the dynamically assigned IP address each time before you bring up the Web Manager. Check with the administrator who configured the basic network parameters on the 16-port IP KVM, for help finding the IP address, if needed. Or see “Considerations When Choosing Whether to Enable DHCP” on page 49 for a list of ways to find out the 16-port IP KVM IP address assigned by the DHCP server.

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

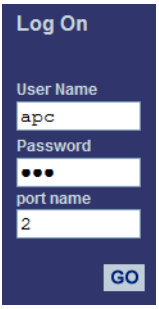
b. If DHCP is not enabled, use a fixed IP address assigned by the administrator to the 16-port IP KVM.

The Login page appears. If direct logins to ports is not enabled, a “user name” and a “password” field appear on the login area of the screen, as shown in the following screen example.



Please enter user name and password to access the APC 16-port IP KVM.

If direct logins to KVM ports is enabled, a “port” field also appears in the login area of the screen, as shown in the following screen example.



User Name: apc

Password: ●●●

port name: 2

2. If direct logins to ports is enabled, to bring up the Web Manager with the port number filled in, enter the IP address of the 16-port IP KVM followed by the port number in the form:

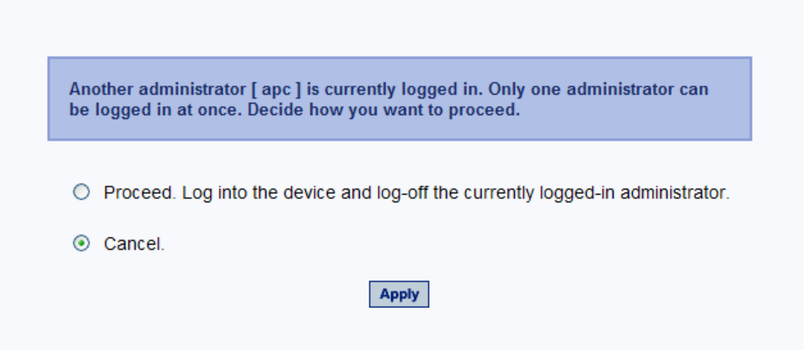
```
IP_address/login.asp?portname=portnumber
```

A login screen displays empty “username” and “password” fields and a port field filled with the name of the port from the URL you entered in the browser.

See “Web Manager Login Screen” on page 259 for background information on the multiple ways to login to the Web Manager.

3. Enter your account’s user name and password.

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



Another administrator [apc] is currently logged in. Only one administrator can be logged in at once. Decide how you want to proceed.

○ Proceed. Log into the device and log-off the currently logged-in administrator.

● Cancel.

Note: For more information about the numbers of simultaneous logins allowed, see “Simultaneous 16-port IP KVM Logins” on page 16.

If the previous dialog box appears, go to Step 4.

4. Click the appropriate radio button and then click Apply.

▼ *To Save Configuration Changes*

The red graphical LED in the lower right hand corner of the Web Manager blinks when any changes made in the forms have not been saved.

- Click the “apply changes” button to save configuration changes.

  The “no unsaved changes” graphical LED appears.

Administrative Modes

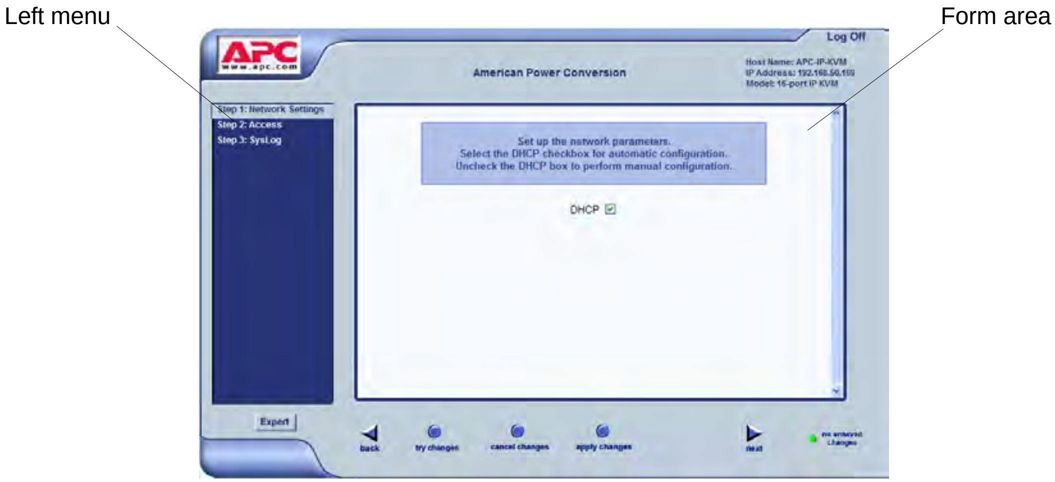
This section describes the two administrative modes of the web manager:

- “Wizard Mode” on page 110
- “Expert Mode” on page 120

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

Wizard Mode

The Wizard mode guides the administrator through three configuration steps. The following figure shows a typical window in Wizard mode. Selecting an item from the left menu brings up a corresponding form in the middle.



Host Name: APC-IP-KVM
IP Address: 192.168.50.159
Model: 16-port IP KVM

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

DHCP ☑

Figure 4-1: Example Window in Wizard Mode

After you log on as described in “To Log On to the Web Manager as Admin” on page 106, Expert mode is in effect by default. To change to Wizard mode, select the Wizard button, which displays only in Expert mode.

Procedures in Wizard Mode

The following table lists all procedures that are performed in Wizard mode.

To Change Network Settings [Wizard]	Page 112
To Add a User [Wizard]	Page 114
To Delete a User [Wizard]	Page 116
To Change a Password [Wizard]	Page 116
To Add a Syslog Server [Wizard]	Page 119

To Delete a Syslog Server [Wizard]	Page 119

Steps in Wizard Mode

Three configuration steps display in the left menu of the Web Manager in Wizard mode. The following table lists the sections where the steps are described.

Step 1: Network Settings [Wizard]	Page 111
Step 2: Access [Wizard]	Page 113
Step 3: SysLog [Wizard]	Page 118

Step 1: Network Settings [Wizard]

In Wizard Mode, selecting "Step 1: Network Settings” brings up a form for reconfiguring existing network settings. During initial setup of the 16-port IP KVM, the administrator configures the default basic network settings that were needed to enable logins through the Web Manager. (See “Performing Basic Network Configuration” on page 65, if desired, for more information about the initial network configuration.) You can skip this step if the current settings are correct. Check with your network administrator if you are not sure.

Before making any changes to existing network settings, you may want to review “Performing Basic Network Configuration” on page 65, which provides a form to record information you need to collect ahead of time.

In Expert mode, under Configuration>Network, you can specify additional networking-related information: a Console Banner, a secondary IP address and secondary network mask, and an MTU. See “To Configure Host Settings [Expert]” on page 182. In Expert mode under Configuration>Network, you can configure syslog servers for ports; specify rules for filtering syslog messages, Virtual Private Network (VPN), and SNMP settings; specify IP filtering rules (for the 16-port IP KVM to act as a firewall), and perform other advanced configuration tasks.

▼ To Change Network Settings [Wizard]

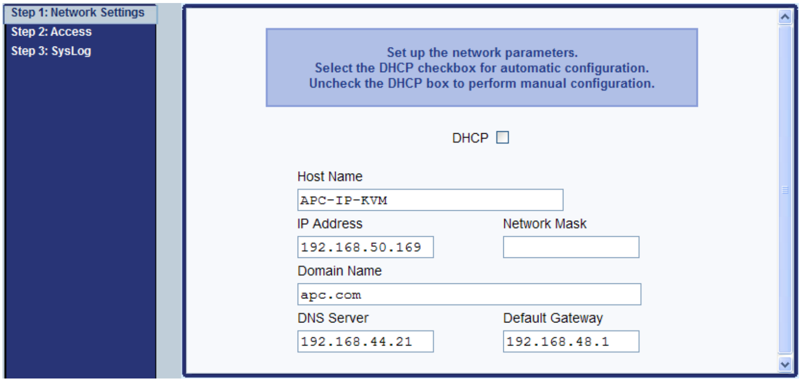
1. Collect any IP addresses or other network information to change.

   See the list of network information to collect under “Performing Basic Network Configuration” on page 65, if needed.

2. In Wizard mode, go to “Step 1: Network Settings.”

   If the “DHCP” check box is not checked, the DHCP selection page displays as shown below. If the “DHCP” check box is checked, only the check box appears below the instructions.

Note: If DHCP is enabled, a local DHCP server assigns the 16-port IP KVM a dynamic IP address, which can change. The administrator chooses whether or not to use DHCP during initial setup. The initial setting may have been changed since initial configuration.



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

DHCP □

Host Name: APC-IP-KVM

IP Address: 192.168.50.169

Network Mask:

Domain Name: apc.com

DNS Server: 192.168.44.21

Default Gateway: 192.168.48.1

3. If the “DHCP” check box is not checked, enter the network information in the fields.

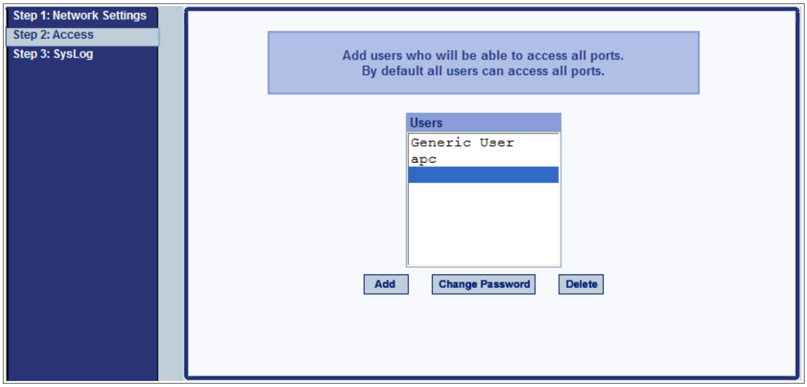
4. Click the “apply changes” button.

Warning! If you change the 16-port IP KVM’s IP address and apply the changes, you will need to reconnect to the Web Manager with the new IP address.

5. If appropriate, press the Next button or select “Step 2: Access” from the left menu**.**

Step 2: Access [Wizard]

In Wizard mode, selecting “Step 3: Access” brings up a form for adding or deleting users and for setting or changing passwords. Use this form if you want to add user accounts to allow other administrators to administer connected devices without being able to change the configuration of the 16-port IP KVM. The administrator can configure added users to administer the 16-port IP KVM by assigning them to the “admin” group.


Add users who will be able to access all ports.
By default all users can access all ports.

The Access form lists the currently defined Users and has three buttons: Add, Change Password, and Delete.

In the Users list, by default, are two user accounts that cannot be deleted:

- apc
- Generic User

The Admin (the “apc” account) has access to all functions of the Web Manager and has access to all ports on the 16-port IP KVM.

The Generic User defines the access permissions for all users except the admin and root users. Any new regular user account automatically inherits the access permissions configured for the Generic User.

The following lists has links to the procedures for adding and deleting regular users and changing the passwords for regular users or administrators.

To Add a User [Wizard]	Page 114
To Delete a User [Wizard]	Page 116

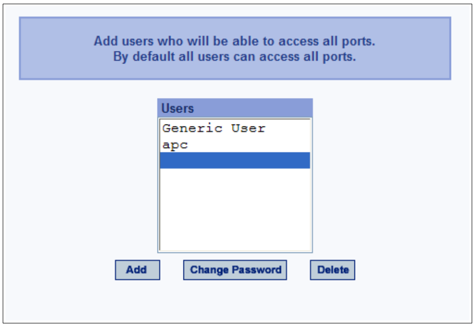
To Change a Password [Wizard]	Page 116

Note: To perform advanced configuration of users and groups, for example, to restrict user access to KVM ports, or to create a group, go to Expert>Configuration>Users and Groups.

▼ *To Add a User [Wizard]*

1. In Wizard mode, go to Step 3: Access.

   The Access form appears.

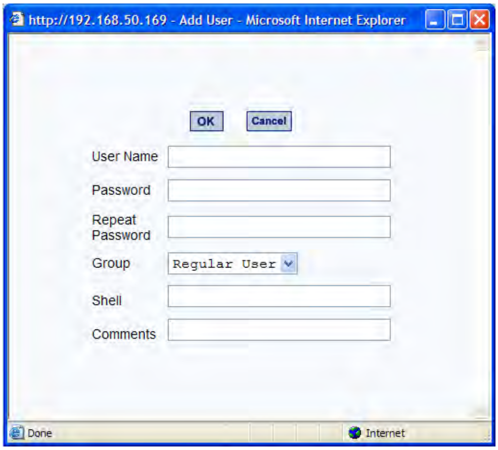


Add users who will be able to access all ports.
By default all users can access all ports.

Users
Generic User
apc

2. Click Add.

   The “Add User” dialog box appears.


http://192.168.50.169 - Add User - Microsoft Internet Explorer
OK
Cancel
Done
Internet

User Name

Password

Repeat Password

Group: Regular User

Shell

Comments

3. Enter the required information in the fields as shown in the following table.

Field Name	**Definition**
User Name	The user name for the account being added.
Password	The password for the account.
Group	On the drop-down list, Select Regular User [Default] or Admin. **Note:** To configure a user to be able to perform all 16-port IP KVM administration functions, select the “Admin” group. See “Types of Users” on page 14, if needed, for more background.
Shell	Optional. The default shell when the user makes a `ssh` or `telnet` connection with the switch. Choices are: `sh` or `bash`. The default is `sh`.
Comments	Optional notes about the user’s role or configuration.

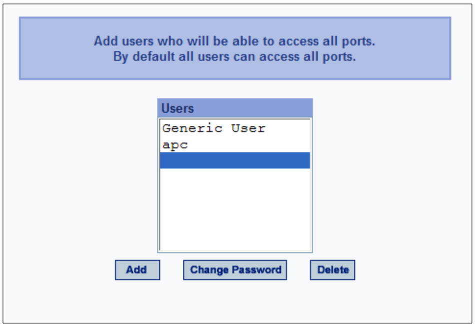
4. Click OK.

5. Click the “apply changes” button.

▼ To Delete a User [Wizard]

1. In Wizard mode, go to “Step 3: Access.”

   The “Access” form appears.



Add users who will be able to access all ports.
By default all users can access all ports.

1. Select the user name to delete.
2. Click “Delete.”

   The user name disappears from the Users list.

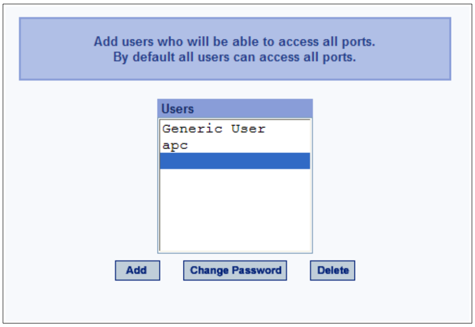
3. Click the “apply changes” button.

▼ To Change a Password [Wizard]

Note: Leaving the default admin or root passwords unchanged would leave the 16-port IP KVM and connected devices open to anyone who knows the default passwords and the 16-port IP KVM’s IP address. For security’s sake, make sure the admin and root passwords have been changed from the default “apc.” If either the admin or root passwords have not been changed, change them now.

1. In Wizard mode, go to “Step 3: Access.”

   The “Access” form appears.

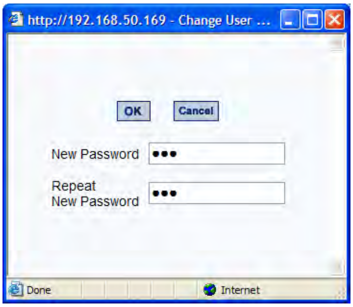


Add users who will be able to access all ports.
By default all users can access all ports.

Users
Generic User
apc

2. Select the name of the user whose password you want to change.
3. Click “Change Password.”

   The “Change User Password” dialog box appears.



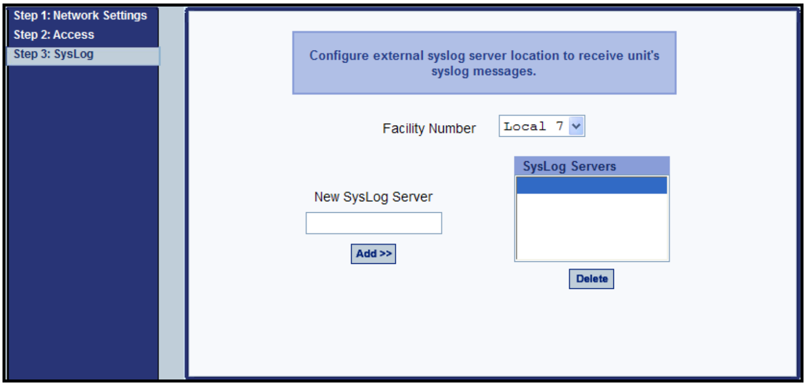
New Password ●●●

Repeat New Password ●●●

4. Enter the new password in both fields, and click OK.
5. Click the “apply changes” button.

Step 3: SysLog [Wizard]

In Wizard mode, selecting “Step 3: SysLog” brings up a form for identifying one or more syslog servers to receive syslog messages from the 16-port IP KVM.



Configure external syslog server location to receive unit's syslog messages.

Facility Number: Local 7

New SysLog Server

SysLog Servers

Before performing this procedure, make sure an already-configured syslog server is available to the 16-port IP KVM.

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 16-port IP KVM

Each syslog server has eight local facility numbers (Local 0 through Local 7) that the syslog server’s administrator can assign and use for handling log messages from different locations. See “Syslog Servers” on page 46, if needed, for more background on logging and on how facility numbers are used.

The following table has links to the procedures for adding and deleting a syslog server.

To Add a Syslog Server [Wizard]	Page 119
To Delete a Syslog Server [Wizard]	Page 119

Use this form to configure system logging for the 16-port IP KVM. More advanced configuration of syslog servers and event notification can be done in Expert mode. To configure system logging for messages relating to KVM ports, in Expert mode go to “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 186.

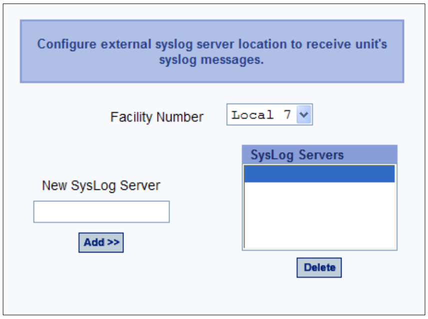
▼ *To Add a Syslog Server [Wizard]*

This procedure assumes you have the following information:

- The IP address of the syslog server
- The facility number for messages coming from the 16-port IP KVM

1. In Wizard mode, go to “Step 3: SysLog.”

   The SysLog form appears.



Configure external syslog server location to receive unit's syslog messages.

Facility Number: Local 7

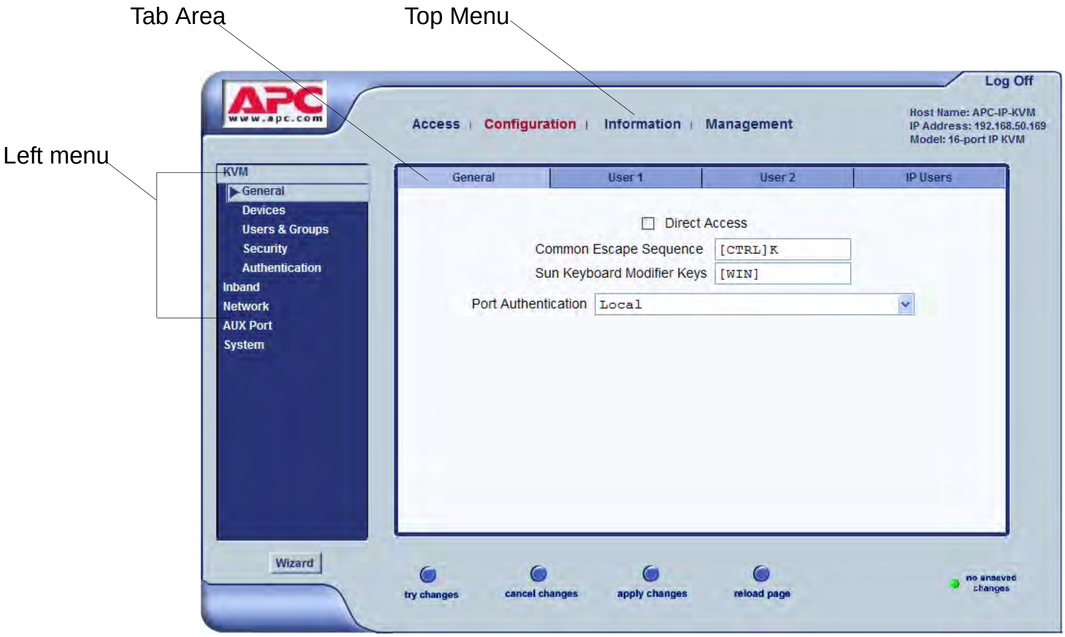
2. From the Facility Number drop-down list, select the facility number.
3. In the New Syslog Server field, enter the IP address of a syslog server, and select the Add button. (Repeat this step until all syslog servers are listed.)
4. The new server(s) appear in the Syslog Servers list.
5. Click “apply changes.”

▼ *To Delete a Syslog Server [Wizard]*

1. From the Syslog Server list, select the syslog server that you want to delete from the current facility location, and select Delete.
2. Repeat this step for as many servers you need to delete.
3. Click “apply changes.”

Expert Mode

To perform advanced configuration, click the Expert button at the bottom of the left menu to switch to Expert mode. The following figure shows a typical window in Expert mode.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

☐ Direct Access

Common Escape Sequence [CTRL]K

Sun Keyboard Modifier Keys [WIN]

Port Authentication Local

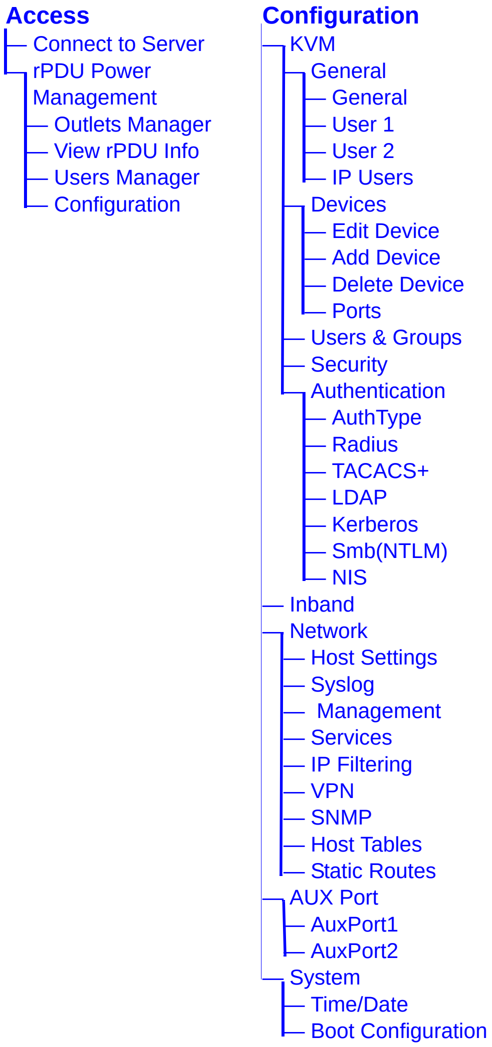
Making a selection from the top menu changes the list of menu options displayed in the left menu.

An option in the left menu (such as KVM in the preceding figure) often has several forms associated with it. Selecting a tab labeled with the name of the form or selecting the form's name in the left menu brings up the form.

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 "User 1" form in the right tab in the previous figure would use this convention, "In Expert mode, go to Configuration>KVM>General>User 1."

Overview of Menus and Forms in Expert Mode

The following figure shows all the menus and forms available in Expert mode. If you are viewing this document online, click any term to go to the section where the form is described.



Access
- Connect to Server
- rPDU Power Management
  - Outlets Manager
  - View rPDU Info
  - Users Manager
  - Configuration

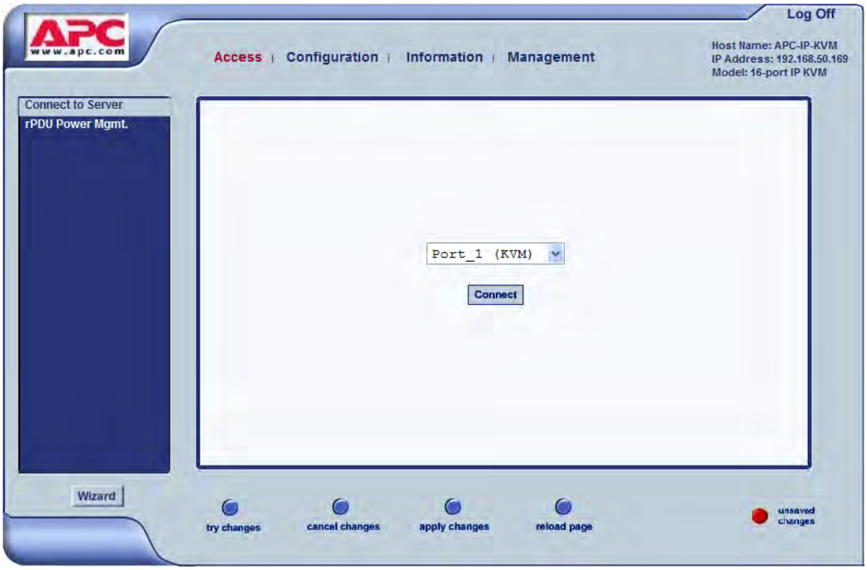
Configuration
- KVM
  - General
    - General
    - User 1
    - User 2
    - IP Users
  - Devices
    - Edit Device
    - Add Device
    - Delete Device
    - Ports
  - Users & Groups
  - Security
  - Authentication
    - AuthType
    - Radius
    - TACACS+
    - LDAP
    - Kerberos
    - Smb(NTLM)
    - NIS
- Inband
- Network
  - Host Settings
  - Syslog
  - Management
  - Services
  - IP Filtering
  - VPN
  - SNMP
  - Host Tables
  - Static Routes
- AUX Port
  - AuxPort1
  - AuxPort2
- System
  - Time/Date
  - Boot Configuration

Information
- General
- Port Status

Management
- Backup Configuration
- Firmware Upgrade
- Microcode Upgrade
- Microcode Reset
- Active Sessions
- Reboot

Access

Under “Access” in Expert mode, two options appear in the left menu bar, as shown in the following figure.



See the following sections for details about the tasks performed using the forms under Access in Expert mode. “rPDU Power Management” on page 123

See the following sections for details about the tasks performed using the forms under Access in Expert mode.

- “Connect to Server” on page 122
- “rPDU Power Management” on page 123

For instructions for forms that allow the regular user to connect to ports on the 16-port IP KVM to administer connected devices and perform power management, see Chapter 5: Web Manager for Regular Users.

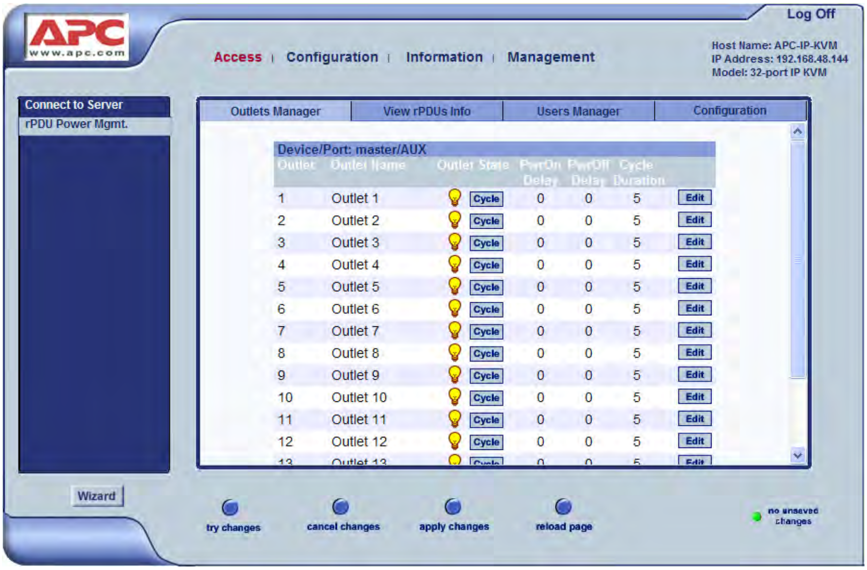
Connect to Server

On the “Connect to Server” form under Access, you can access servers that are connected to KVM ports or to in-band servers that use RDP (Remote

Desktop Protocol). Chapter 6: Accessing Connected Devices discusses connecting to servers in more detail.

rPDU Power Management

On the “rPDU Power Management” forms under “Access” in Expert mode, you can manage power of devices that are plugged into the APC rPDU outlets.



Device/Port: master/AUX

Outlet	Outlet Name	Outlet State		PwrOn Delay	PwrOff Delay	Cycle Duration	
1	Outlet 1	💡	Cycle	0	0	5	Edit
2	Outlet 2	💡	Cycle	0	0	5	Edit
3	Outlet 3	💡	Cycle	0	0	5	Edit
4	Outlet 4	💡	Cycle	0	0	5	Edit
5	Outlet 5	💡	Cycle	0	0	5	Edit
6	Outlet 6	💡	Cycle	0	0	5	Edit
7	Outlet 7	💡	Cycle	0	0	5	Edit
8	Outlet 8	💡	Cycle	0	0	5	Edit
9	Outlet 9	💡	Cycle	0	0	5	Edit
10	Outlet 10	💡	Cycle	0	0	5	Edit
11	Outlet 11	💡	Cycle	0	0	5	Edit
12	Outlet 12	💡	Cycle	0	0	5	Edit
13	Outlet 13	💡	Cycle	0	0	5	Edit

You can manage power when the following two prerequisites are completed:

- An rPDU is connected to an AUX port on the 16-port IP KVM.

  See “To Connect an APC rPDU to the AUX Port” on page 95 for installation procedures.
- The AUX port is configured for power management.

  See “To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219.

See the following sections for details about the tasks performed using the forms under rPDU Power Management.

- “Outlets Manager” on page 124
- “View rPDU Info” on page 127

- “Users Manager” on page 127
- “Configuration” on page 129

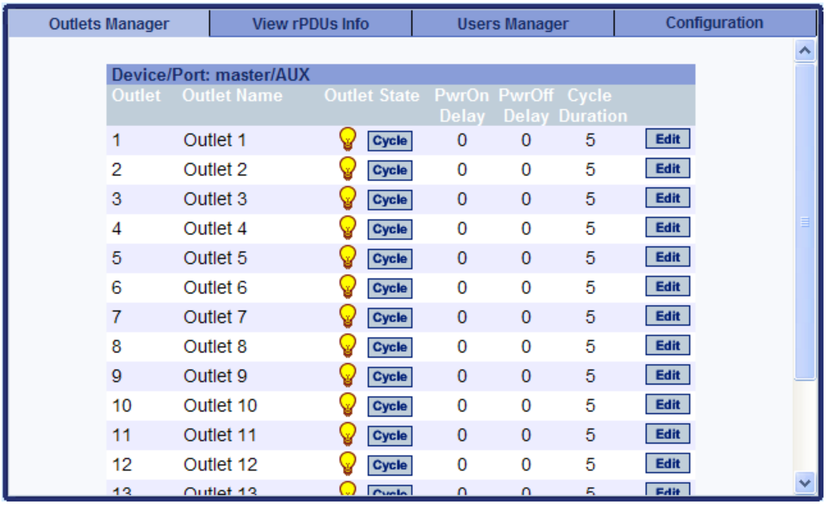
See the following sections for related procedures:

- “To Turn On, Turn Off, or Power Cycle Outlets” on page 125
- “To Edit an Outlet’s PwrOn Delay, PwrOff Delay, or Cycle Duration” on page 126
- “To View rPDU Information” on page 127
- “To Configure Users to Manage Specific Power Outlets” on page 128
- “To Specify or Change the Alias of an rPDU” on page 130
- “To Configure Creation of Alarms and Syslog Files for rPDUs” on page 130

Outlets Manager

On the “Outlets Manager” form under Access>rPDU Power Management in Expert mode, you can do the following for all outlets on all connected rPDUs:

- Check the status
- Power on
- Power off
- Cycle (by briefly switching the outlet off and on)
- Specify the PwrOn Delay, PwrOff Delay, and Cycle Duration



Device/Port: master/AUX

Outlet	Outlet Name	Outlet State		PwrOn Delay	PwrOff Delay	Cycle Duration	
1	Outlet 1	💡	Cycle	0	0	5	Edit
2	Outlet 2	💡	Cycle	0	0	5	Edit
3	Outlet 3	💡	Cycle	0	0	5	Edit
4	Outlet 4	💡	Cycle	0	0	5	Edit
5	Outlet 5	💡	Cycle	0	0	5	Edit
6	Outlet 6	💡	Cycle	0	0	5	Edit
7	Outlet 7	💡	Cycle	0	0	5	Edit
8	Outlet 8	💡	Cycle	0	0	5	Edit
9	Outlet 9	💡	Cycle	0	0	5	Edit
10	Outlet 10	💡	Cycle	0	0	5	Edit
11	Outlet 11	💡	Cycle	0	0	5	Edit
12	Outlet 12	💡	Cycle	0	0	5	Edit
13	Outlet 13	💡	Cycle	0	0	5	Edit

Under the “Outlet State” column, yellow light bulb icons indicate that outlets are powered on, and grey light bulb icons indicate that outlets are powered off. A “Cycle” button is active next to each outlet that is powered on.

The information in the PwrOn Delay, PwrOff Delay, and Cycle Duration columns can be modified by clicking the Edit button for each outlet.

You can also specify an alias for an outlet by clicking its Edit button.

▼ *To Turn On, Turn Off, or Power Cycle Outlets*

1. In Expert mode, go to Access>rPDU Power Management>Outlets Manager.

   The “Outlets Manager” form appears.

2. To turn an outlet on or off, click the adjacent light bulb.
3. To power an outlet off and quickly power it on again, click the adjacent “Cycle” button.
4. Click “apply changes.”

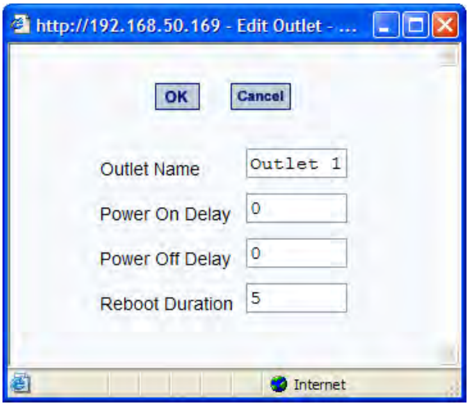
▼ To Edit an Outlet's PwrOn Delay, PwrOff Delay, or Cycle Duration

1. In Expert mode, go to Access>rPDU Power Management>Outlets Manager.

   The "Outlets Manager" form appears.

2. Click the Edit button adjacent to the Outlet you wish to modify.

   The Edit Outlet dialog box appears.



Outlet Name: Outlet 1

Power On Delay: 0

Power Off Delay: 0

Reboot Duration: 5

3. Enter the values as described below.

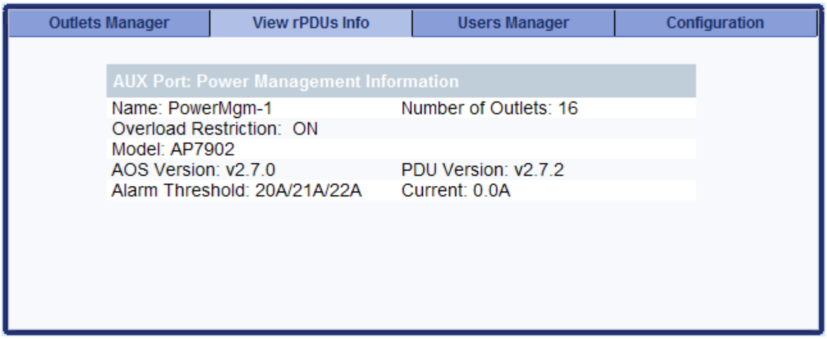
   - Outlet Name – Meaningful alias for the outlet up to 23 characters
   - Pwer On Delay – Time in seconds that the rPDU waits before powering on the outlet
   - Pwer Off Delay – Time in seconds that the rPDU waits before powering off the outlet
   - Reboot Duration – Time in seconds that the rPDU waits after powering off the outlet until it powers it on again

4. Click "apply changes."

View rPDU Info

On the “View rPDUs Info” form under Access>rPDU Power Management in Expert mode, you can view the following information about any connected rPDU:

- Name
- Number of outlets
- Overload restriction status
- AOS version
- PDU version
- Alarm threshold
- Current



AUX Port: Power Management Information

Name: PowerMgm-1	Number of Outlets: 16
Overload Restriction: ON	
Model: AP7902	
AOS Version: v2.7.0	PDU Version: v2.7.2
Alarm Threshold: 20A/21A/22A	Current: 0.0A

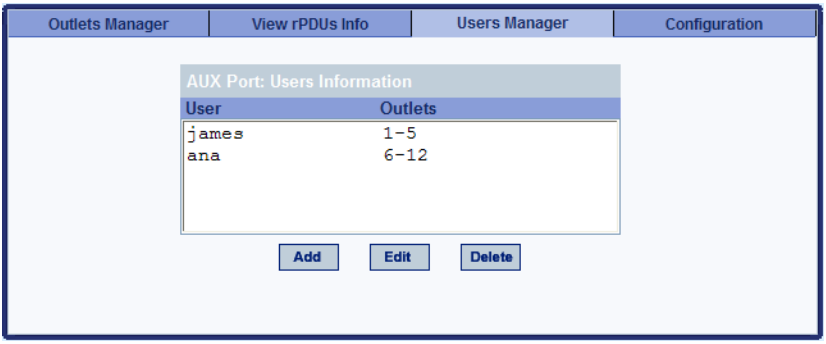
▼ To View rPDU Information

- In Expert mode, go to Access>rPDU Power Management>View rPDUs Info.

  The “View rPDUs Info” form appears.

Users Manager

On the “Users Manager” form under Access>rPDU Power Management in Expert mode, you can assign users to outlets.



AUX Port: Users Information

User	Outlets
james	1-5
ana	6-12

▼ *To Configure Users to Manage Specific Power Outlets*

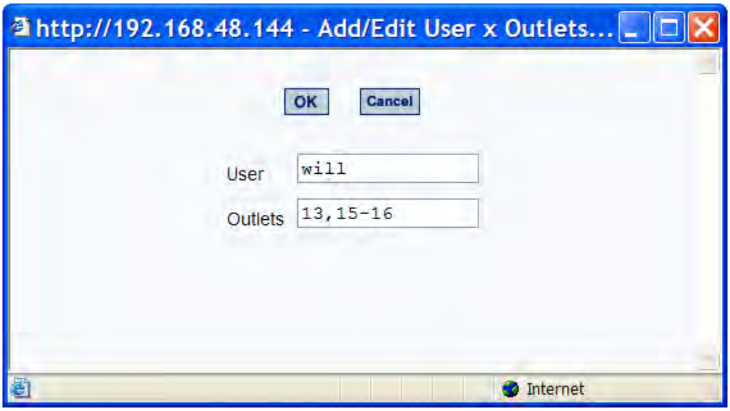
1. In Expert mode, go to Access>rPDU Power Management>Users Manager.

   The “Users Manager” form appears.

2. To remove a user’s ability to manage power, select the user name and click “Delete.”

3. To edit a user, select the user name from the view table and click “Edit.” Skip to Step 5.

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



User will

Outlets 13,15-16

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 user name 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, 6, 9-12). Do not use spaces.

6. Click OK.

7. Click “apply changes.”

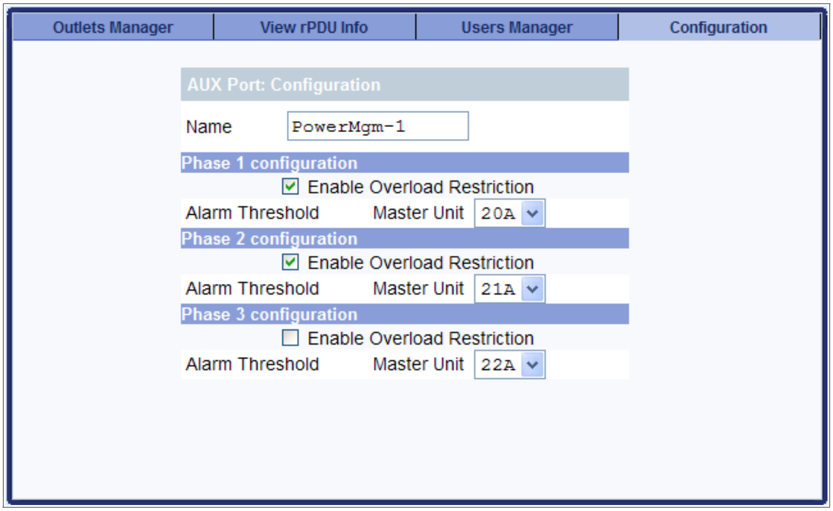
Configuration

On the “Configuration” form under Access>rPDU Power Management in Expert mode, you can specify the following:

- Whether syslog messages are generated for power management events
- Overload Restriction:
  - An alarm threshold
  - Whether a buzzer sounds whenever the current exceeds the defined threshold.

You can define the alarm threshold for both a master and a slave unit and define aliases for each connected rPDU.

The Configuration form shows the ports that are currently connected to rPDUs. The following figure displays an example form that appears for a 16-port IP KVM with an rPDU connected to the AUX port.



AUX Port: Configuration

Name PowerMgm-1

Phase 1 configuration

☑ Enable Overload Restriction

Alarm Threshold Master Unit 20A

Phase 2 configuration

☑ Enable Overload Restriction

Alarm Threshold Master Unit 21A

Phase 3 configuration

□ Enable Overload Restriction

Alarm Threshold Master Unit 22A

▼ *To Specify or Change the Alias of an rPDU*

1. In Expert mode, go to Access>rPDU Power Management>Configuration.

   The Configuration form displays entries for all ports configured for power management.

2. In the Name field, enter the alias of the rPDU.
3. Click “apply changes.”

▼ *To Configure Creation of Alarms and Syslog Files for rPDUs*

1. In Expert mode, go to Access>rPDU Power Management>Configuration.

   The Configuration form displays entries for all ports configured for power management.

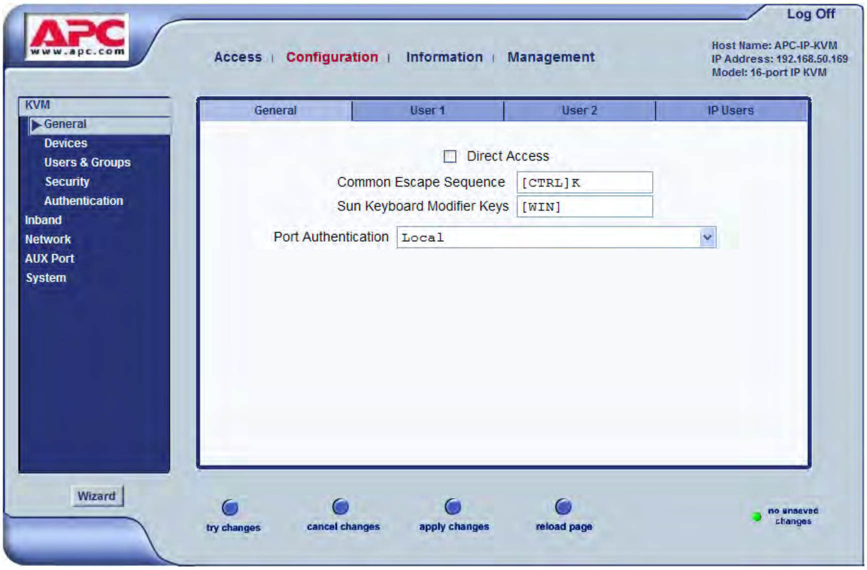
2. Click the appropriate check boxes to enable or disable Overload Restiction, the generation of Syslog files, and the sounding of a Buzzer if a defined threshold is exceeded.

   An alarm sounds on the rPDU, not the 16-port IP KVM.

3. If enabling the buzzer or alarm notification, select an Alarm Threshold (1-20 amps) from the drop-down list for the master and any slave unit.
4. Click “apply changes.”

Configuration

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



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

□ Direct Access

Common Escape Sequence [CTRL]K

Sun Keyboard Modifier Keys [WIN]

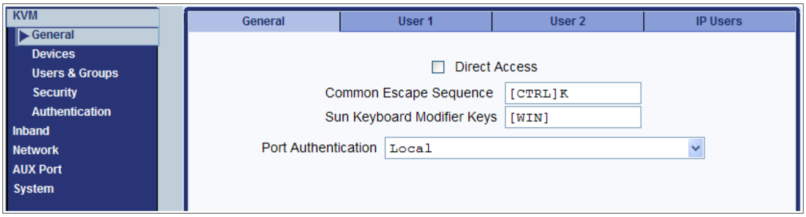
Port Authentication Local

See the following sections for details about the tasks performed using the forms under Configuration in Expert mode:

- “KVM” on page 132
- “Configuring In-band (RDP) Servers” on page 174
- “Network” on page 180
- “AUX Port” on page 218
- “System” on page 220

KVM

Selecting Configuration>KVM in Expert mode brings up five KVM options in the left menu as shown in the following figure.



☐ Direct Access

Common Escape Sequence [CTRL]K

Sun Keyboard Modifier Keys [WIN]

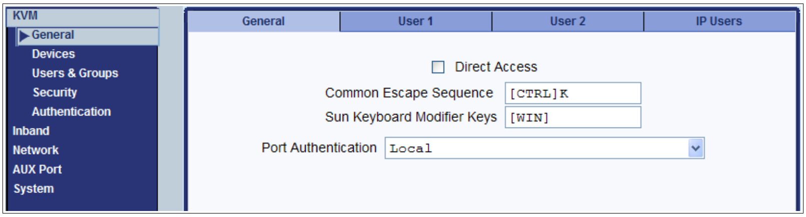
Port Authentication Local

You can use the KVM menu options for custom configuration of KVM ports. The following table provides links to the sections where the options are described.

Web Manager Form	Where Documented
General	“General” on page 133
Devices	• “Configuring Individual KVM Ports” on page 141 • “Configuring Cascaded KVM Units” on page 147
Users & Groups	“Users & Groups” on page 151
Security	“Security” on page 159
Authentication	• “Configuring an Authentication Method” on page 161 • “Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices” on page 164

General

Selecting Configuration>KVM>General in Expert mode brings up four tabs, as shown in the following figure.



□ Direct Access

Common Escape Sequence [CTRL]K

Sun Keyboard Modifier Keys [WIN]

Port Authentication Local

The following table provides links to the sections that describe how to use the forms under Configuration>KVM>General in Expert mode.

General	"General" on page 133.
User 1, User 2, and IP Users	"Local User and IP Users" on page 136

General

On the General form under Configuration>KVM>General in Expert mode, you can specify the parameters shown in the following table, which offers cross-references to where you can find more information on each parameter.

Parameter Name	Definition	Where Documented
Direct Access	Selecting this check box enables logins to KVM ports directly from the Web Manager Login screen.	• "Enabling Direct Access to KVM Ports" on page 134 • "To Enable Direct Access to KVM Ports" on page 134

Parameter Name	Definition	Where Documented
Common Escape Sequence	Redefines keyboard shortcuts used during KVM connections	• "Redefining KVM Connection Keyboard Shortcuts (Hot Keys)" on page 135 • "To Redefine KVM Session Keyboard Shortcuts" on page 135
Authentication Type	Allows you to choose whether authentication is required for KVM port logins. If needed, see the introduction to authentication on the 16-port IP KVM in "Authentication" on page 42.	• "To Configure an Authentication Method for 16-port IP KVM Logins" on page 162 • "To Configure an Authentication Method for KVM Port Logins" on page 163

Enabling Direct Access to KVM Ports

When direct access to KVM ports is enabled, users authorized to access KVM ports can use a port field on the Web Manager login screen to log on and connect directly to the port. See "To Log On to the Web Manager as Admin" on page 106, if desired, for an example of the login screen when direct login is enabled.

▼ *To Enable Direct Access to KVM Ports*

1. Go to Configuration>KVM>General in Expert mode.

   The General form appears.

2. Select the "Direct access" check box.
3. Click "apply changes."

Redefining KVM Connection Keyboard Shortcuts (Hot Keys)

You can use the four General forms (General, User 1, User 2, IP Users) to redefine a default set of keyboard shortcuts (called hot keys), which allow administrators to perform common actions while connected to KVM ports. You redefine the common escape sequence portion of each hot key separately from the command key.

The following table summarizes the format of the hot keys for KVM connections, the defaults, and where they can be redefined.

	Common Escape Sequence	**Command Key**	**Where Defined**
Format	"Ctrl" + "*letter key*"	"*letter key*"	• Configuration>KVM>General> General
Defaults	Ctrl+k	"p" to bring up the "power management" window, "q" to quit, and so forth. See Table 6-3, "Default KVM Connection Keyboard Shortcuts," on page 273 for all the default command keys.	• Configuration>KVM>General> User 1 • Configuration>KVM>General> User 2 • Configuration>KVM>General> IP Users

▼ *To Redefine KVM Session Keyboard Shortcuts*

1. Go to Configuration>KVM>General in Expert mode.

   The General form appears.

2. To redefine the "Common Escape Sequence" enter a key combination starting with the Ctrl key and followed by a letter, for example, **`Ctrl m`**.

3. To redefine the command key portion of any KVM-session keyboard shortcuts, do one of the following steps.

   - To change the command key for administrators who access KVM ports through the User 1 port, go to the User 1 tab.

- OR -

- To change the command key for administrators who access KVM ports through the User 2, go to the User 2 tab.

- OR -

- To change the command key for users who access KVM ports through the Web Manager, go to the IP Users tab.

4. On the “User 1,” “User 2,” or “IP Users” tab, redefine the command keys, if desired, in any of the following fields: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” “Port Info.”
5. Click “apply changes.”

Specifying Authentication for KVM Port Logins

By default, all users can log on to all ports. Using the Port Authentication drop-down list on the KVM>General page, you can configure a single authentication method that applies whenever anyone attempts to log on to a device connected to any KVM port.

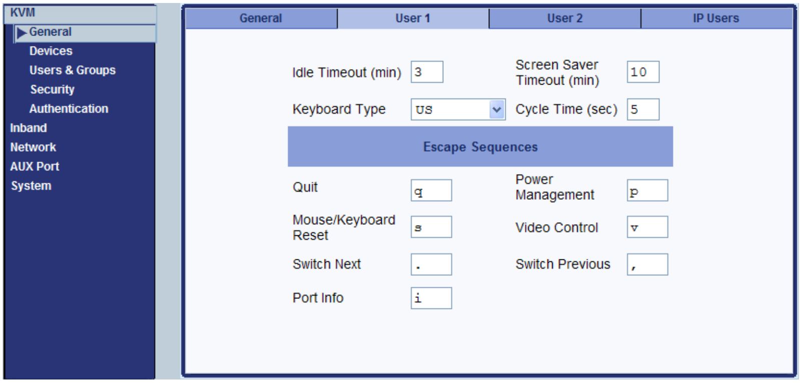
Choice of authentication types for KVM ports are:

- None
- Local
- Kerberos (either Kerberos or Kerberos/DownLocal),
- LDAP (either LDAP or LDAP/DownLocal)
- NTLM (either NTLM Windows NT/2000/2003 or NTLM/DownLocal)
- RADIUS (either RADIUS or RADIUS/DownLocal
- TACACS+ (either TACACS+, and TACACS+/DownLocal)

See “To Configure an Authentication Method for KVM Port Logins” on page 163 for the instructions on specifying an authentication method.

Local User and IP Users

Selecting Configuration>KVM>General>User 1 brings up a form with the fields shown in the following figure.



Idle Timeout (min) 3

Screen Saver Timeout (min) 10

Keyboard Type US

Cycle Time (sec) 5

Quit q

Power Management p

Mouse/Keyboard Reset s

Video Control v

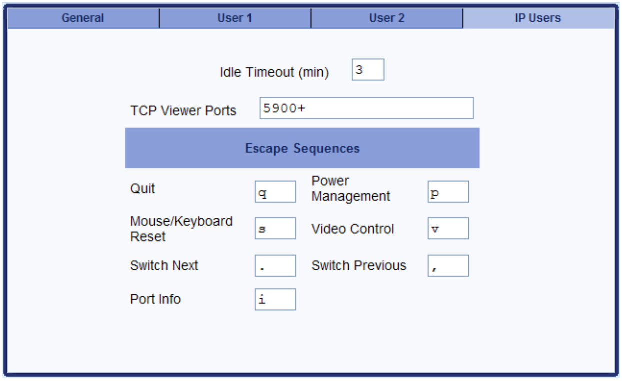
Switch Next .

Switch Previous ,

Port Info i

On the “User 1” form under Configuration>KVM>General in Expert mode you can redefine the default session parameters that apply when a user (called the *Local User*) is using the OSD through a direct connection to the KVM User 2 management port on the 16-port IP KVM. On the “User 2” form, you can redefine the default session parameters that apply when a user is using the OSD through a Console Extender connection to the User 2 port on the 16-port IP KVM.

Selecting Configuration>KVM>General>IP Users brings up a form with the fields shown in the following figure.



Idle Timeout (min) 3

TCP Viewer Ports 5900+

Quit q

Power Management p

Mouse/Keyboard Reset s

Video Control v

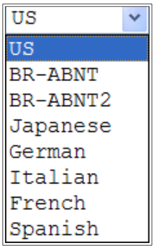
Switch Next .

Switch Previous ,

Port Info i

On the “IP Users” form under Configuration>KVM>General in Expert mode, you can define the default session parameters that apply when a remote user (called the *IP User*) is connected to a KVM port through the Web Manager (in a type of session called *KVM over IP*).

The following table lists and describes the parameters that appear on the forms for both types of users.

Field Name	Definition
Idle Timeout	Sets the maximum time (in minutes) for the session to be idle before it is closed. The maximum value is 60 minutes. A value of 0 disables the idle timeout.
Screen Save Timeout	Sets the time (in minutes) for the session to be idle before the screen saver activates. The maximum value is 60 minutes. A value of 0 disables the idle timeout. [User 1 and User 2 only.]
Keyboard Type	Sets the keyboard type. [User 1 and User 2 only.] Choose the type of keyboard connected to the User 1 and User 2 ports on the 16-port IP KVM. The options from the drop-down list are shown in the figure.  US US BR-ABNT BR-ABNT2 Japanese German Italian French Spanish
Cycle Time	Change the cycle time (in seconds) within the following range: 3 to 60 seconds. [User 1 and User 2 only.]
TCP Viewer Ports	Change the number of the TCP port used for the APC rPDU Viewer. [IP Users only.] The default is 5900+. You may need to change the default, for example, if your firewall is blocking port 5900. (For more details, see “TCP Ports” on page 21.) Port numbers 1-1024 are reserved. Indicate a range of ports by entering a plus sign (+) after the first port number (as in 2500+) or by entering a dash between two port numbers (as in 2500-2501). Indicate a set of nonadjacent port numbers by separating port numbers with commas (as in 2500, 2508).

On the “User 1” and “User 2” and “IP Users” forms, you can also redefine the command key portion of keyboard shortcuts for each type of user. For more information about redefining keyboard shortcuts, see “Redefining Keyboard Shortcuts (Hot Keys)” on page 34 and “To Redefine KVM Session Keyboard Shortcuts” on page 135 if needed.

The following table shows procedures you can perform using the Local User or IP Users forms.

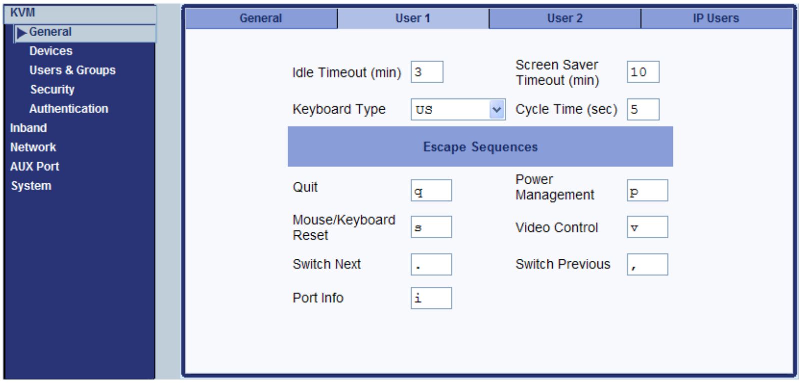
To Configure IP User (KVM Over IP) Sessions	Page 141
To Redefine KVM Session Keyboard Shortcuts	Page 135

▼ *To Configure Local User 1 and User 2 Sessions*

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a local user is directly logged on to the 16-port IP KVM.

1. In Expert mode, go to Configuration>KVM>General>.

2. To configure parameters for the User 1 port, select the User 1 tab.



Idle Timeout (min): 3
Screen Saver Timeout (min): 10
Keyboard Type: US
Cycle Time (sec): 5
Quit: q
Power Management: p
Mouse/Keyboard Reset: s
Video Control: v
Switch Next: .
Switch Previous: ,
Port Info: i

3. To configure parameters for the User 2 port, select the User 2 tab.

The User 1 and User 2 forms are identical except that User 1 modifies the User 1 port options, while User 2 modifies the User 2 port options.

4. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.

5. To change the screen saver timeout, enter a different number of minutes in the “Screen Saver Timeout” field.

6. To change the keyboard type, select a different keyboard from the “Keyboard type” drop-down list.

7. To change the cycle time, enter a different number of seconds in the “Cycle Time” field.

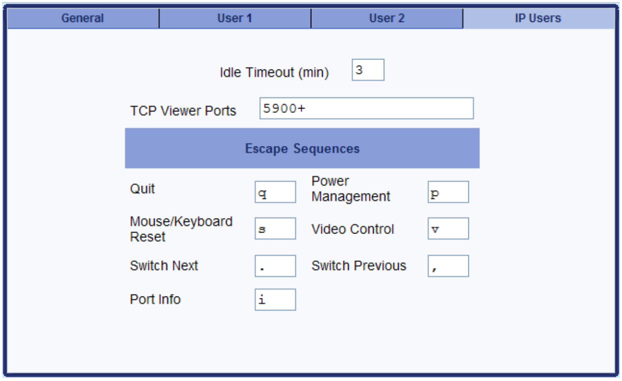
8. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.

9. Click “apply changes.”

▼ *To Configure IP User (KVM Over IP) Sessions*

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a remote user is connected through the Web Manager (in a KVM over IP session).

1. Go to Configuration>KVM>General>IP Users in Expert mode.



Idle Timeout (min) 3

TCP Viewer Ports 5900+

Escape Sequences

Quit	q	Power Management	p
Mouse/Keyboard Reset	s	Video Control	v
Switch Next	.	Switch Previous	,
Port Info	i		

2. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.
3. To change the TCP port number used by the Remote Viewer, enter another number in the “TCP Viewer Ports” field.
4. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
5. Click “apply changes.”

Configuring Individual KVM Ports

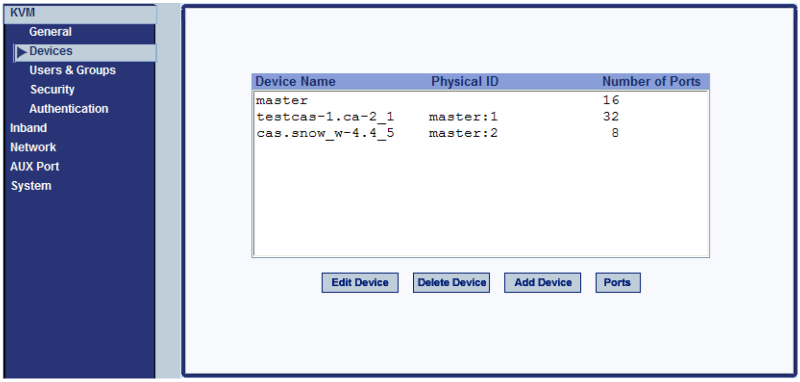
On the Modify Port dialog box, you can do the following:

- Configure an alias for a single KVM port
- Configure power management for the server that is connected to the KVM port while the user is logged on to the server
- Enable or disable KVM ports

The following table lists the related procedures with links to where they are described.

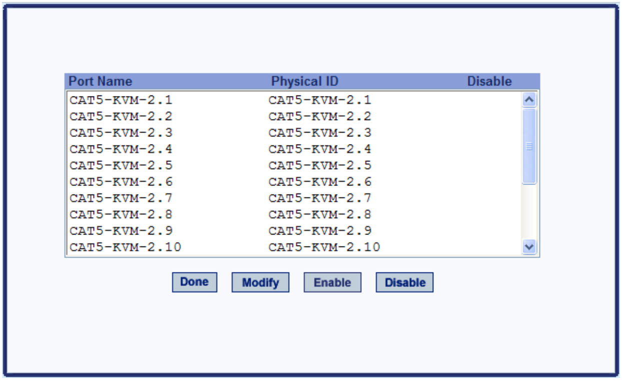
To Configure a KVM Port for Power Management	Page 143
To Specify or Change the Alias for a KVM Port	Page 146
To Enable or Disable a KVM Port	Page 146

Selecting Configuration>KVM>Devices in Expert mode brings up the form shown in the following figure.



Device Name	Physical ID	Number of Ports
master		16
testcas-1.ca-2_1	master:1	32
cas.snow_w-4.4_5	master:2	8

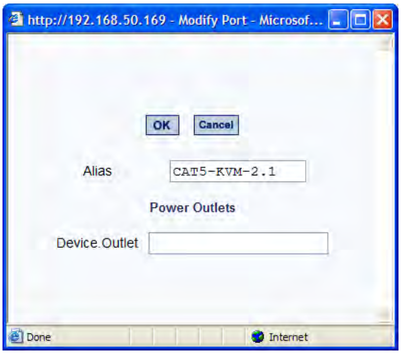
The device name “master” stands for the 16-port IP KVM, which is the master KVM unit in a cascaded configuration. Other device names may appear below “master” depending on the number of KVM units cascaded to the master. Selecting the name of a KVM unit in the list and clicking the “Ports” button brings up a list of the KVM ports on the 16-port IP KVM, as shown in the following figure.



Port Name	Physical ID	Disable
CAT5-KVM-2.1	CAT5-KVM-2.1	
CAT5-KVM-2.2	CAT5-KVM-2.2	
CAT5-KVM-2.3	CAT5-KVM-2.3	
CAT5-KVM-2.4	CAT5-KVM-2.4	
CAT5-KVM-2.5	CAT5-KVM-2.5	
CAT5-KVM-2.6	CAT5-KVM-2.6	
CAT5-KVM-2.7	CAT5-KVM-2.7	
CAT5-KVM-2.8	CAT5-KVM-2.8	
CAT5-KVM-2.9	CAT5-KVM-2.9	
CAT5-KVM-2.10	CAT5-KVM-2.10	

When you select one or more ports, you can enable or disable the KVM port(s) using the “Enable” or “Disable” buttons on the form.

When you select a port and click the “Modify” button, the dialog box shown in the following figure appears.



Alias CAT5-KVM-2.1

Power Outlets

Device.Outlet

▼ *To Configure a KVM Port for Power Management*

Perform this procedure to enable a user who is connected to a server through a KVM port to perform power management for the server while connected. When this procedure is completed, the user can manage up to two power connections for any one server. Before you start make sure the following prerequisites are complete:

- The computer is plugged into an rPDU connected to the 16-port IP KVM’s AUX port.
- The AUX port has been configured for power management.

See “To Configure the AUX Port for Use With an rPDU or an External Modem” on page 219, if needed.

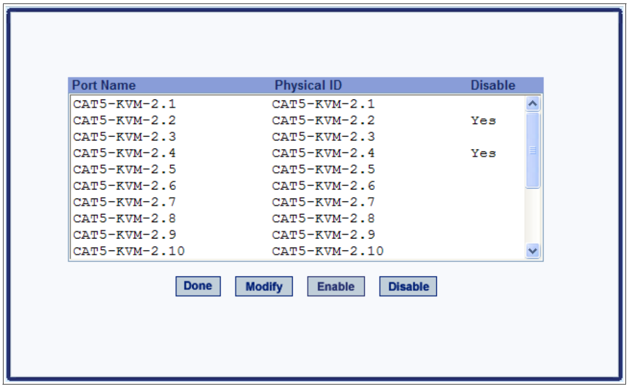
- You know the outlet number or numbers to which the computer’s power cable or cables are plugged.

1. In Expert mode, go to: Configuration>KVM>Devices.

   The Devices form appears.

2. Select the Device that contains the port(s) to be configured and click the Port button.

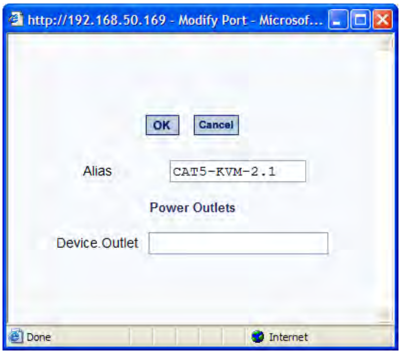
   The Port Name list appears.



Port Name	Physical ID	Disable
CAT5-KVM-2.1	CAT5-KVM-2.1	
CAT5-KVM-2.2	CAT5-KVM-2.2	Yes
CAT5-KVM-2.3	CAT5-KVM-2.3	
CAT5-KVM-2.4	CAT5-KVM-2.4	Yes
CAT5-KVM-2.5	CAT5-KVM-2.5	
CAT5-KVM-2.6	CAT5-KVM-2.6	
CAT5-KVM-2.7	CAT5-KVM-2.7	
CAT5-KVM-2.8	CAT5-KVM-2.8	
CAT5-KVM-2.9	CAT5-KVM-2.9	
CAT5-KVM-2.10	CAT5-KVM-2.10	

3. Select the port you want to modify and click the Modify button.

   The Modify Port dialog box appears.



Alias CAT5-KVM-2.1

Power Outlets

Device.Outlet

4. In the Alias field, type an alias for the port

5. In the Device.Outlet field, enter the device and the outlet of the rPDU that the server is plugged into.

6. Click the OK button.

7. Click the “apply changes” button to save your configuration.

▼ *To Specify or Change the Alias for a KVM Port*

1. Go to Configuration>KVM>Devices in Expert mode, select the device that includes the port(s) you wish to modify.
2. Click the “Ports” button.

   A list of all the selected ports appears.
3. Select a single port to be modified, and then select the “Modify” button.

   The “Modify Port” dialog box appears.
4. To change the port’s alias, do the following steps.
   a. Enter a new alias in the “Alias” field.
   b. Click OK on the dialog box.
5. Click “Done” on the form listing all the ports.
6. Click “apply changes.”

▼ *To Enable or Disable a KVM Port*

1. Go to Configuration>KVM>Devices in Expert mode, and select the device that contains the port(s) you wish to enable or disable.
2. Click the “Ports” button.

   A form listing all the selected ports appears.
3. Select the port(s) to be enabled or disabled, and then select the “Enable” or “Disable” button.
4. Click “Done” on the form listing all the ports.
5. Click “apply changes.”

Configuring Cascaded KVM Units

The Devices form allows you to configure one or more secondary KVM units to a primary KVM unit, a process also known as cascading or daisy-chaining. See “Cascaded Devices” on page 22 for background information.

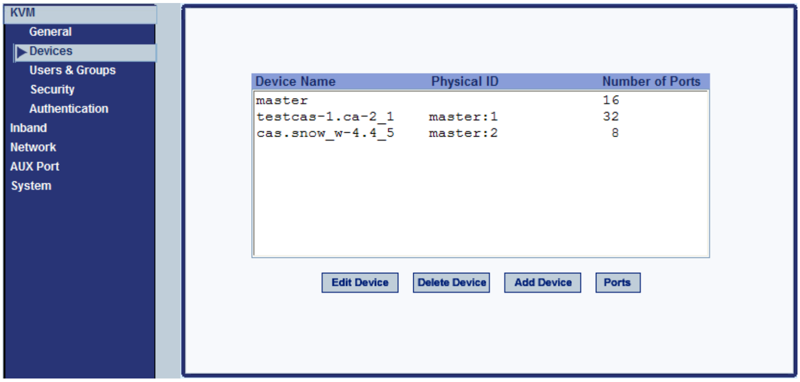
Selecting Configuration>KVM>Devices in Expert mode brings up the Devices form on which you can perform the following tasks:

- Add a secondary KVM unit to be cascaded from the master 16-port IP KVM.

  See “To Add a Secondary KVM Unit to be Cascaded from the Master 16-port IP KVM” on page 148
- Edit the configuration of a cascaded device.

  See “To Edit the Configuration of a Cascaded KVM Unit” on page 149
- Delete the configuration of a cascaded device.

  See “To Delete the Configuration of a Cascaded KVM Unit” on page 151

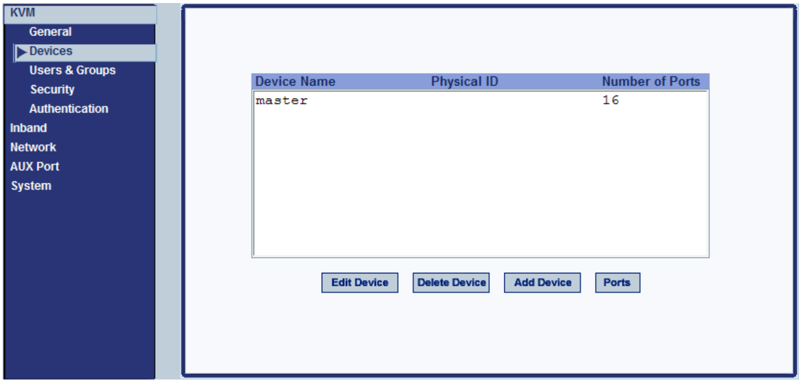


Device Name	Physical ID	Number of Ports
master		16
testcas-1.ca-2_1	master:1	32
cas.snow_w-4.4_5	master:2	8

▼ *To Add a Secondary KVM Unit to be Cascaded from the Master 16-port IP KVM*

1. In Expert mode, go to: Configuration>KVM>Devices.

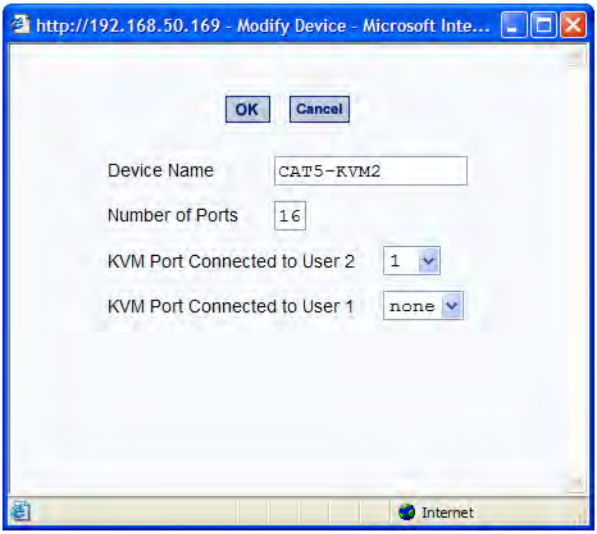
The Devices configuration form appears.



Device Name	Physical ID	Number of Ports
master		16

2. Click the Add Device button.

The Modify Device dialog box appears.



Device Name CAT5-KVM2

Number of Ports 16

KVM Port Connected to User 2 1

KVM Port Connected to User 1 none

3. In the Device Name field, specify a name for the secondary device or KVM unit.

4. In the Number of Ports field, enter the number of ports contained in the cascaded device.
5. In the KVM Port Connected to User 2 (KVM) drop-down list, enter the port number of the master 16-port IP KVM that is connected to the User 2 port of the secondary KVM device.

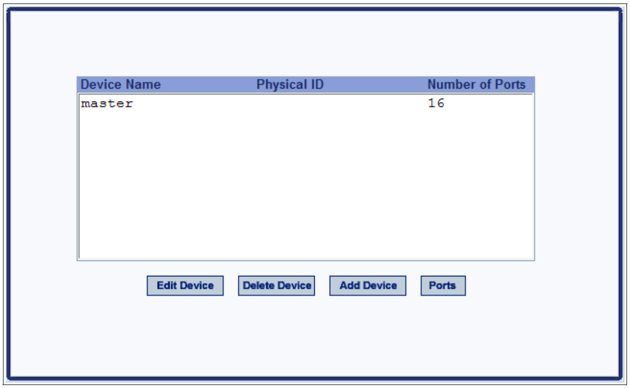
Note: See “Connecting Cascaded KVM Units to the Primary 16-port IP KVM” on page 95 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master 16-port IP KVM.

6. In the Port Connected to User 1 or (KVM) drop-down list, enter the secondary KVM port that is connected to the User 1 port of the primary 16-port IP KVM.
7. Click the OK button when done.
8. On the configuration window, select “apply changes” to save your configuration.

▼ *To Edit the Configuration of a Cascaded KVM Unit*

1. In Expert mode, go to: Configuration>KVM>Devices.

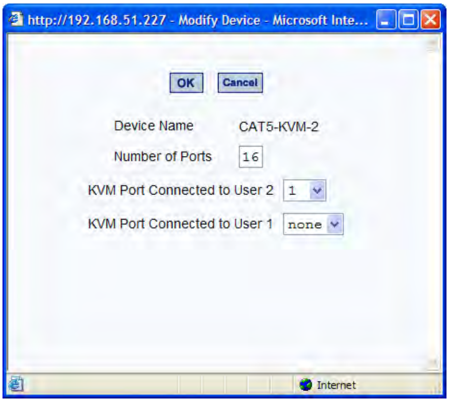
   The Devices form appears.



Device Name	Physical ID	Number of Ports
master		16

2. Select the item you wish to edit and click the Edit button.

   The Modify Port dialog box appears.



Device Name CAT5-KVM-2

Number of Ports 16

KVM Port Connected to User 2 1

KVM Port Connected to User 1 none

3. In the Number of Ports field, enter the number of ports contained on the cascaded device.

4. To enable one user to access the ports on the cascaded KVM unit, in the KVM Port Connected to User 2 (KVM) drop-down list, select the port number on the master 16-port IP KVM that is connected to the User 2 port on the secondary KVM device.

Note: See “Connecting Cascaded KVM Units to the Primary 16-port IP KVM” on page 95 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master 16-port IP KVM.

5. To enable two users to access the ports on the cascaded KVM unit, in the Port Connected to User 1 or (KVM) drop-down list, enter the secondary KVM port that is connected to the User 1 port of the primary 16-port IP KVM.

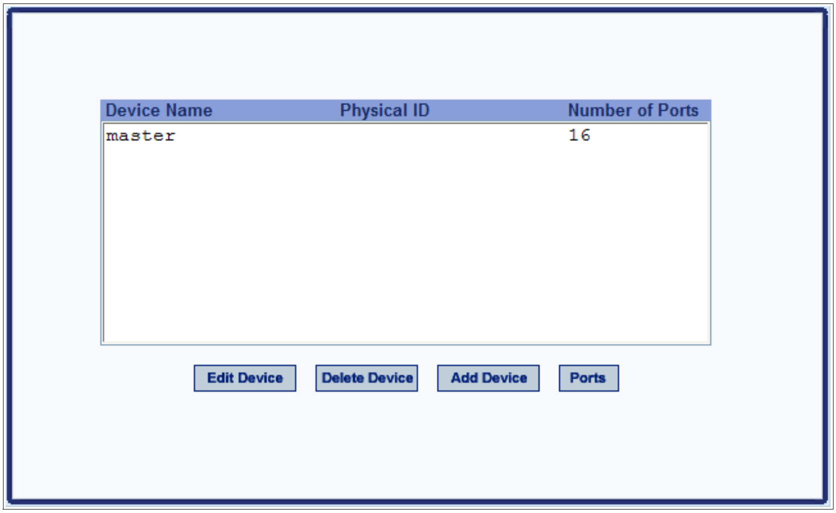
6. Click the OK button.

7. Click “apply changes” to save your configuration.

▼ *To Delete the Configuration of a Cascaded KVM Unit*

1. In Expert mode, go to: Configuration>KVM>Devices.

   The Devices form appears.



Device Name	Physical ID	Number of Ports
master		16

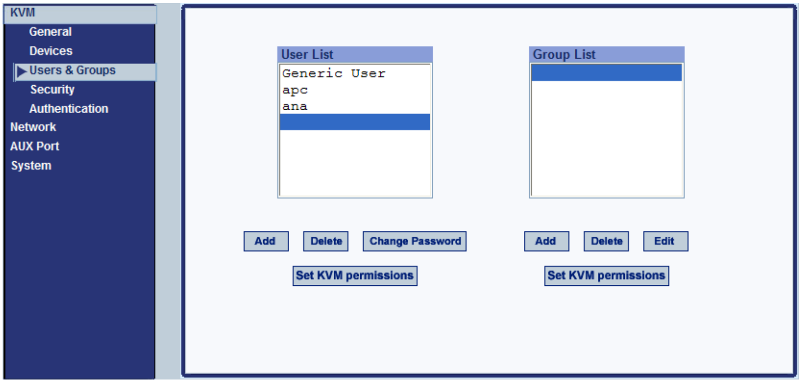
2. Select the item you wish to delete and click the Delete button.

   The system deletes the selected device.

3. Click “apply changes” to save your configuration.

Users & Groups

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



You can use the Users & Groups form to do the following:

- Add or delete users.
- Assign or change user passwords.
- Reset the permissions of the Generic User.

Note: Permissions assigned to the Generic User define the default permissions for regular users.

- Set unique permissions for individual users.
- Assign permissions by group.
- Add or delete user groups from the Group Access List and assign users to a group.
- Restrict all users’ access to devices connected to KVM ports by setting KVM permissions for users and groups of users for selected ports.

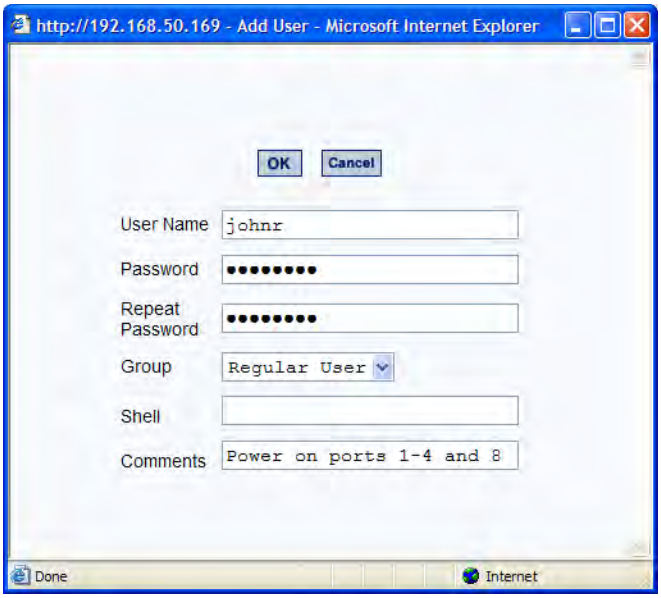
▼ *To Add a User [Expert]*

1. In Expert mode, go to Configuration>Users & Groups.

The Users & Groups form appears.

2. Click “Add.”

The “Add User” dialog box appears.


http://192.168.50.169 - Add User - Microsoft Internet Explorer
OK
Cancel
Done
Internet

User Name: johnr

Password: ●●●●●●●●●

Repeat Password: ●●●●●●●●●

Group: Regular User

Shell:

Comments: Power on ports 1-4 and 8

3. Either type the required information in the fields or select the desired option from the drop-down list as shown in the previous screen and defined in the following table.

Field Name	Definition
User Name	Name of the user to be added.
Password	The password associated with the user name.
Group	On the left drop-down list, select “Regular User [Default]” or “Admin.” **Note:** To configure a user to be able to perform all administrative functions, select the “Admin” group. See “Types of Users” on page 14 for more details.
Shell	Optional. The default shell when the user makes an `ssh` or `telnet` connection with the switch. Choices are: `sh` or `bash`. The default is `sh`.
Comments	Optional notes about the user’s role or configuration.

4. Click OK.
5. Click “apply changes.”

▼ *To Delete a User or Group [Expert]*

1. In Expert mode, go to Configuration>Users & Groups.

   The Users & Groups form appears.
2. Select the name of a user or group to delete.
3. Click “Delete.”
4. Click “apply changes.”

▼ *To Change a User’s Password [Expert]*

1. In Expert mode, go to Configuration>Users & Groups.

   The Users & Groups form appears.
2. Select the name of the user whose password you want to change.
3. Click “Change Password.”

   The Change User Password” dialog box appears.
4. Enter the new password in the “New Password” filed and enter it again in the “Repeat New Password” field.
5. Click OK.
6. Click “apply changes.”

▼ *To Add a Group*

1. In Expert mode, go to Configuration>Users & Groups.

   The Users & Groups form appears.
2. Under the list of groups, click “Add.”

   The “Add Group” dialog box appears.
3. Type the name for the new group.
4. Type the user names of the users you want to add to the group.

   Use commas to separate the names.

5. Click OK.
6. Click “apply changes.”

▼ To Modify a Group

1. In Expert mode, go to Configuration>Users & Groups.

   The Users & Groups form appears.
2. Select the name of a group to modify.
3. Click “Edit.”

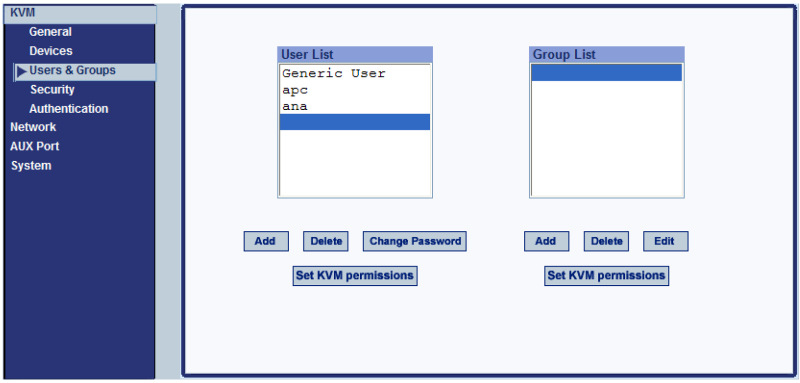
   The “Edit Group” form appears.
4. Add or delete users from the group as desired.
5. Click OK.
6. Click “apply changes.”

▼ To Select Users and Groups for Assigning KVM Port Access

Perform this procedure to select users to access computers connected to KVM ports.

1. Go to Expert>Configuration>Users & Groups.

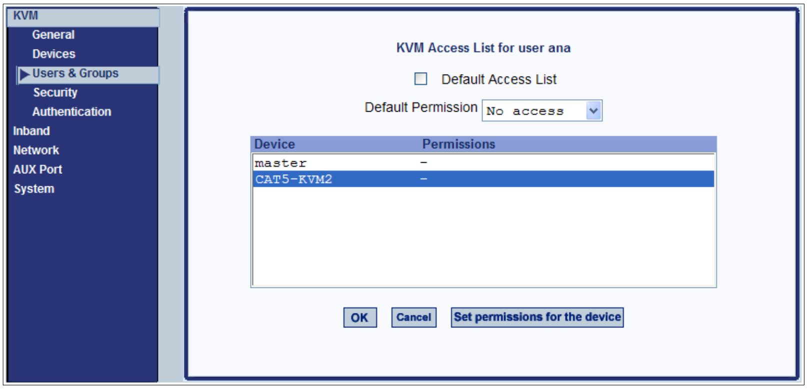
   The Users & Groups form appears.
2. To set KVM port access for a regular user, select the name of the user or of multiple users from User List.



3. To set KVM port access permissions for a group, select the name of the group from the Group List.

4. Click the “Set KVM Permissions” button.

   The “KVM Access list for “user name” or “groupname” dialog box appears.



KVM Access List for user ana

□ Default Access List

Default Permission No access

Device	Permissions
master	-
CAT5-KVM2	-

Note: When the “Default Access List” check box is checked, the user or group has the same permissions that are assigned to the Generic User. Changes made on this form when a user name is selected convert the user into a non-generic user.

---

5. Go to “To Assign KVM Port Access to a User or Group” on page 156.

▼ *To Assign KVM Port Access to a User or Group*

Perform this procedure when you want to specify the types of access a user or group of users can have to computers that are connected to the 16-port IP KVM’s KVM ports.

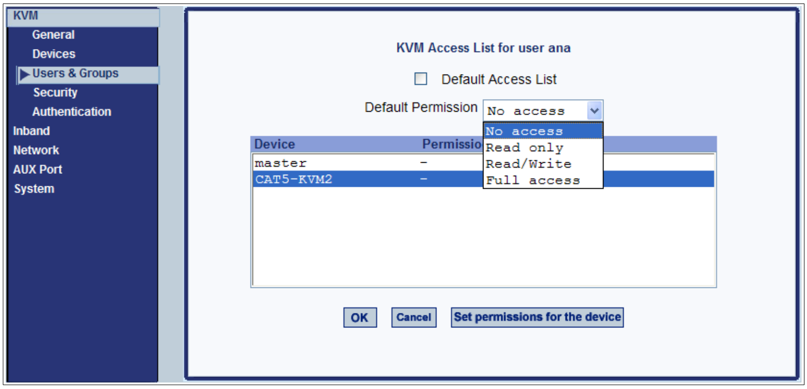
1. Go to Expert>Configuration>Users & Groups, and select a user or group.

   If needed see “To Select Users and Groups for Assigning KVM Port Access” on page 155.

2. To assign to the selected user or group the same permissions assigned to the Generic User, make sure the “Default Access List” check box is checked and click OK.

3. To re-define the KVM permissions for the selected user or group, clear the check box.

4. Select the desired access option from the “Default Permission:” drop-down list.



KVM Access List for user ana

□ Default Access List

Default Permission: No access

Device	Permission
master	-
CAT5-KVM2	-

As shown in the previous screen example, the options are: “No access,” “Read only,” “Read/Write,” “Full access.”

5. To configure access to a device and all of its ports, do the following:

   a. Select one or more devices from the Device list.

   b. From the Default Permissions drop-down list, select the permissions you wish to apply.

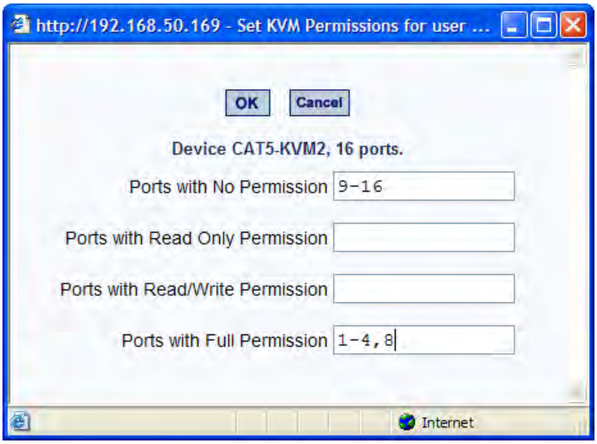
   c. Go to Step 8.

6. To configure access to individual ports or groups of ports, do the following:

   a. Select a device from the Device list.

   b. Click the “Set permissions for the device” button.

   The “Set KVM Permissions for the device” dialog box displays as shown in the following screen example. (The example shows the dialog box when the “master” device is selected.)



http://192.168.50.169 - Set KVM Permissions for user ...

Device CAT5-KVM2, 16 ports.

Ports with No Permission: 9-16

Ports with Read Only Permission:

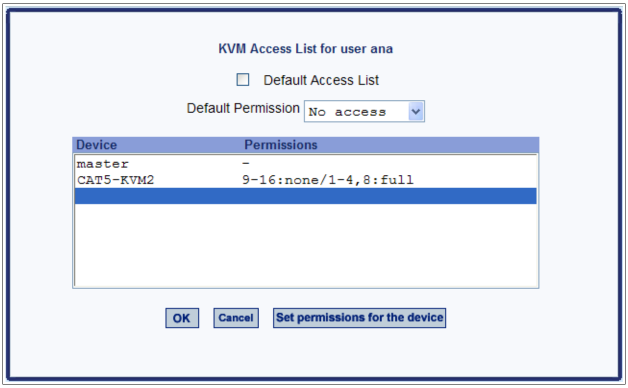
Ports with Read/Write Permission:

Ports with Full Permission: 1-4,8

In the fields for each desired category, type either port aliases or numbers, separating them either by commas or dashes.

7. Click OK.

The newly set permissions appear next to the Device name in the Permissions column, as shown in the following screen example, which shows the restrictions applied to the user name “johnr.”



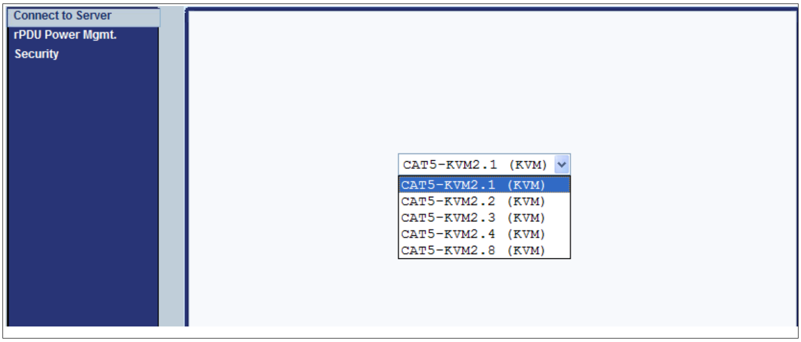
KVM Access List for user ana

□ Default Access List

Default Permission: No access

Device	Permissions
master	-
CAT5-KVM2	9-16:none/1-4,8:full

The following screen example illustrates how the previous settings affect access to ports. When an individual or member of a group with the access permissions shown in the previous screen logs into the Web Manager, the list of ports displayed does not include ports 9 to 16 (because they were configured with no access).



CAT5-KVM2.1 (KVM)

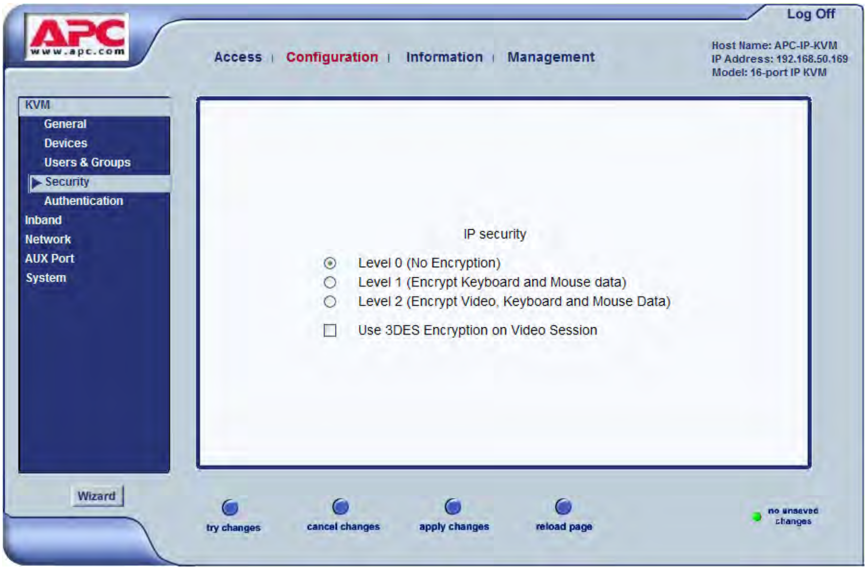
CAT5-KVM2.1 (KVM)
CAT5-KVM2.2 (KVM)
CAT5-KVM2.3 (KVM)
CAT5-KVM2.4 (KVM)
CAT5-KVM2.8 (KVM)

8. Click OK.

9. Click “apply changes.”

Security

Selecting Configuration>KVM>Security in Expert mode brings up the form shown in the following figure. Administrators can specify that communications are encrypted between the 16-port IP KVM and any computer attached to a KVM port.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

IP security

● Level 0 (No Encryption)
○ Level 1 (Encrypt Keyboard and Mouse data)
○ Level 2 (Encrypt Video, Keyboard and Mouse Data)

□ Use 3DES Encryption on Video Session

The Security form allows you to configure your IP security with the following levels:

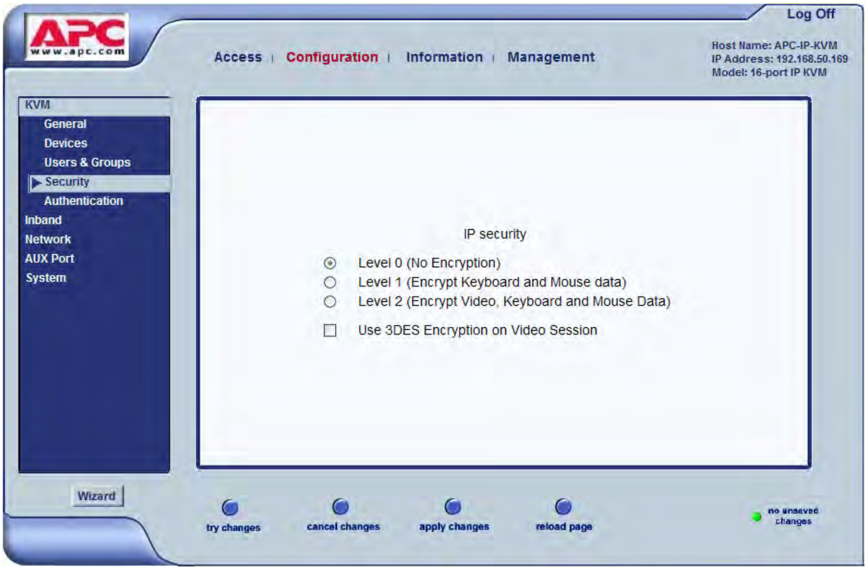
- Level 0 (No Encryption)
- Level 1 (Encrypt Keyboard and Mouse data)
- Level 2 (Encrypt Video, Keyboard and Mouse Data)

In addition, you can select 3DES (Triple Data Encryption Standard) for video sessions in stead of RC4 (Rivest Cipher four), the system default. Though RC4 is faster than 3DES, it is less secure.

▼ *To Configure Encryption on Port Connections [Expert]*

1. In Expert mode, go to: Configuration>KVM>Security.

The Security form appears.



IP security

● Level 0 (No Encryption)
○ Level 1 (Encrypt Keyboard and Mouse data)
○ Level 2 (Encrypt Video, Keyboard and Mouse Data)

□ Use 3DES Encryption on Video Session

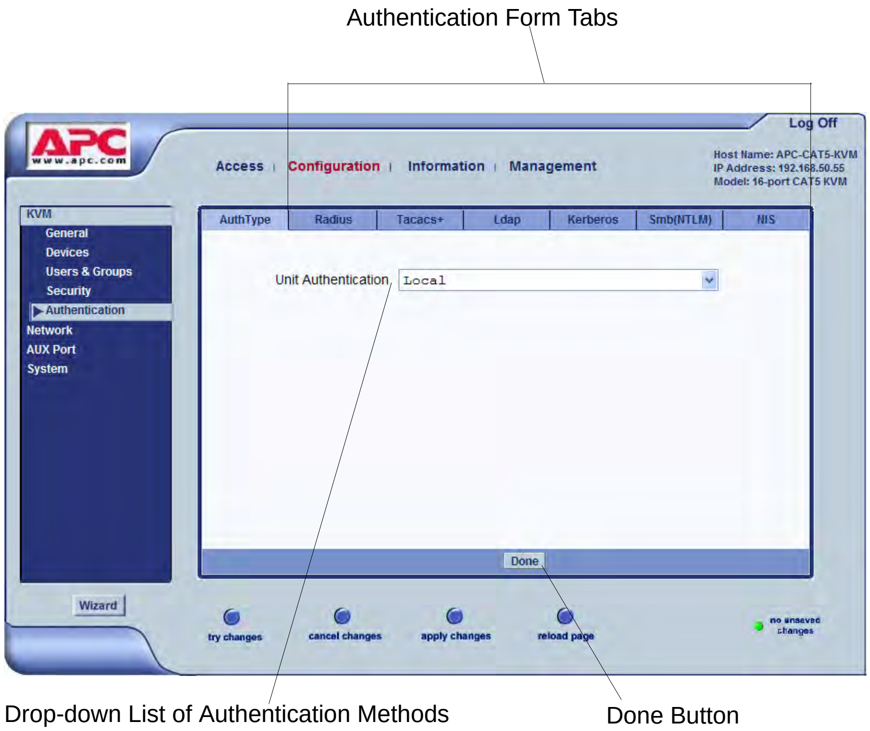
2. Check the appropriate radio buttons.

RC4 is the default encryption if 3DES is not selected. See “Security” on page 159, if needed, for more information.

3. Click “apply changes” to complete the procedure.

Configuring an Authentication Method

Configuration>KVM>Authentication in Expert mode brings up the form shown in the following figure.



Host Name: APC-CAT5-KVM
IP Address: 192.168.50.55
Model: 16-port CAT5 KVM

Unit Authentication: Local

The administrator uses the Authentication forms for two main purposes:

- To select an authentication method for the 16-port IP KVM *only.*

  The default authentication method for the 16-port IP KVM is Local. The administrator can either accept the default or select one of the other authentication methods from the drop-down list on the AuthType form.

  See “To Configure an Authentication Method for 16-port IP KVM Logins” on page 162 for the procedure.

  Any authentication method chosen for the 16-port IP KVM is used for authentication of any users attempting access through `telnet`, `ssh`, or the Web Manager.

See “Authentication” on page 42 for more details.

- To configure all authentication servers for the 16-port IP KVM ports.

  The administrator fills out one of the tabbed forms to set up an authentication server for each authentication method to be used by the 16-port IP KVM and by any of its ports: RADIUS, TACACS+, LDAP, Kerberos, SMB (ports only), NIS. See “Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices” on page 164.

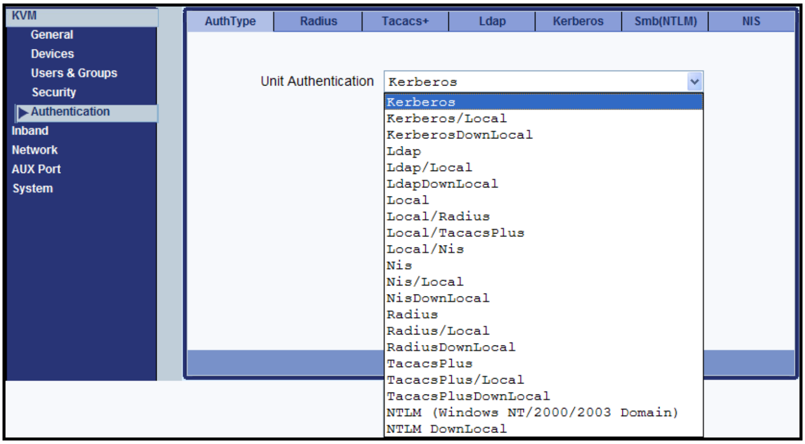
See “To Configure an Authentication Method for 16-port IP KVM Logins” on page 162 for instruction on how to specify an authentication method for ports.

▼ To Configure an Authentication Method for 16-port IP KVM Logins

See “Configuring an Authentication Method” on page 161, if needed, for background information.

1. Go to Configuration>KVM>Authentication in Expert mode.

   The AuthType form displays, as shown in the following figure.



Unit Authentication: Kerberos

2. To specify an authentication method for logins to the 16-port IP KVM, select a method from the Authentication drop-down list.

3. Make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices” on page 164.

▼ *To Configure an Authentication Method for KVM Port Logins*

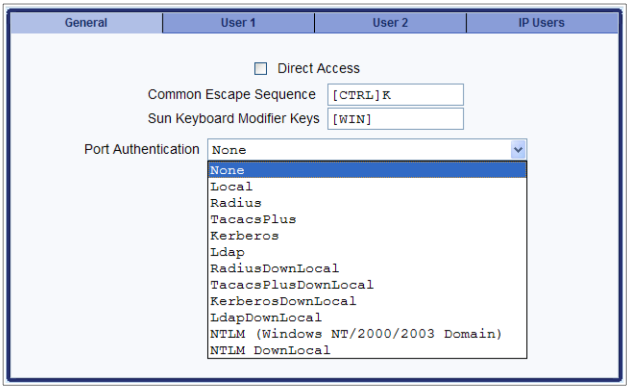
This procedure configures a single authentication method that applies whenever anyone attempts to log on to a device through a connected KVM port.

1. Go to Configuration>KVM>General in Expert mode.

   The General form appears.

2. Select an authentication method from the Port Authentication drop-down list.

   The default option is None.



□ Direct Access

Common Escape Sequence [CTRL]K

Sun Keyboard Modifier Keys [WIN]

Port Authentication None

3. Click “Done.”

4. Click “apply changes.”

   The changes are stored in `/etc/kvmd.conf` on the 16-port IP KVM.

5. If you select any authentication method other than None or Local, make sure that an authentication server is specified for the selected authentication type.

   See “Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices” on page 164.

Configuring Authentication Servers for Logins to the 16-port IP KVM and Connected Devices

The administrator fills out the appropriate form to set up an authentication server for every authentication method to be used by the 16-port IP KVM and by any of its ports: Kerberos, LDAP, NIS, NTLM/SMB (ports only), RADIUS, TACACS+.

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

Method	Variations	Procedures
Kerberos	Kerberos, Local/Kerberos, Kerberos/Local, or Kerberos/DownLocal	"To Identify a Kerberos Authentication Server" on page 165
LDAP	LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal	"To Identify an LDAP Authentication Server" on page 167
NIS	NIS, Local/NIS, NIS/Local, or NIS/DownLocal	"To Configure a NIS Authentication Server" on page 171
NTLM (Windows NT/2000/2003 Domain)	NTLM (Windows NT/2000/2003 Domain), or NTLM/DownLocal	"To Configure an SMB(NTLM) Authentication Server" on page 169
RADIUS	RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal	"To Identify a RADIUS Authentication Server" on page 172
TACACS+	TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal	"To Identify a TACACS+ Authentication Server" on page 173

▼ *To Identify a Kerberos Authentication Server*

Perform this procedure to identify the authentication server when the 16-port IP KVM or any of its ports is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/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 16-port IP KVM and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If Kerberos authentication is specified for the 16-port IP KVM, accounts for all users who need to log on to the 16-port IP KVM to administer connected devices.
- If Kerberos authentication is specified for KVM ports, accounts for users who need administrative access to connected devices

1. Make sure an entry for the 16-port IP KVM and the Kerberos server exist in the 16-port IP KVM's `/etc/hosts` file.

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

      The "Host Table" form appears.

   b. Add an entry for 16-port IP KVM 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. If desired, enter an optional alias in the "Alias" field.

2. Make sure that timezone and time and date settings are synchronized on the 16-port IP KVM and on the Kerberos server.

   Time and date synchronization is most easily achieved by setting both to use the same NTP server.

   a. To specify an NTP server, follow the procedure under “To Set The Time and Date With NTP” on page 223.

   b. To manually set the time and date on the 16-port IP KVM, follow “To Set the 16-port IP KVM’s Date and Time Manually” on page 222.

   c. Work with the authentication server’s administrator to synchronize the time and date between the 16-port IP KVM and the server.

3. If the 16-port IP KVM is not located in the PST time zone, set the timezone on the 16-port IP KVM.

   a. Make a console connection to the 16-port IP KVM and log on as root,

```
KVM login: root
Password: ********
```

The root prompt appears.

```
[root@kvm root]#
```

   b. Enter **set_timezone**.

   A list of timezones appears followed by a prompt asking you to enter a number of a timezone.

```
[root@kvm root]# set_timezone
Please choose the time zone where this machine is located.
0) GMT
1) 1h West GMT
2)10h West GMT
...
26) 9h East GMT
Enter your option:
```

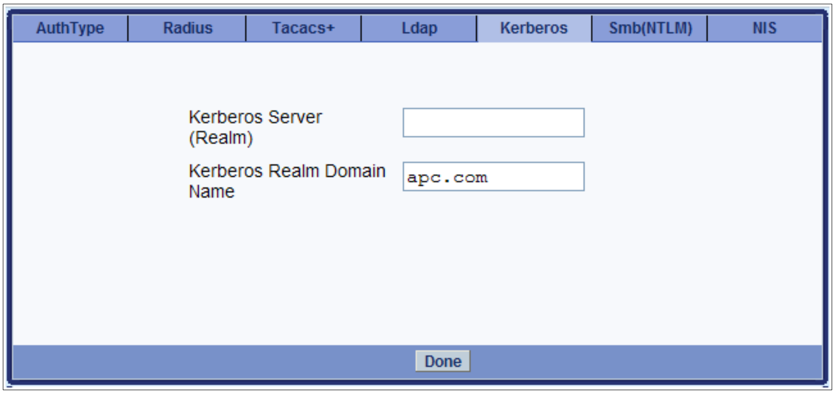
c. Enter the number of the timezone where the 16-port IP KVM is located.

```
Enter your option: 10
```

d. Log off of the console session and close the terminal.

4. In the Web Manager Expert mode, go to Configuration>Authentication> Kerberos.

   The Kerberos form displays as shown in the following figure.



Kerberos Server (Realm)

Kerberos Realm Domain Name: apc.com

5. Fill in the form according to your local setup of the Kerberos server.
6. Click “Done.”
7. Click “apply changes.”

▼ *To Identify an LDAP Authentication Server*

Perform this procedure to identify the authentication server when the 16-port IP KVM or any of its ports is configured to use the LDAP authentication method or any of its variations (LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal).

Before starting this procedure, find out the following information from the LDAP server’s 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 two fields, but an entry is not required:

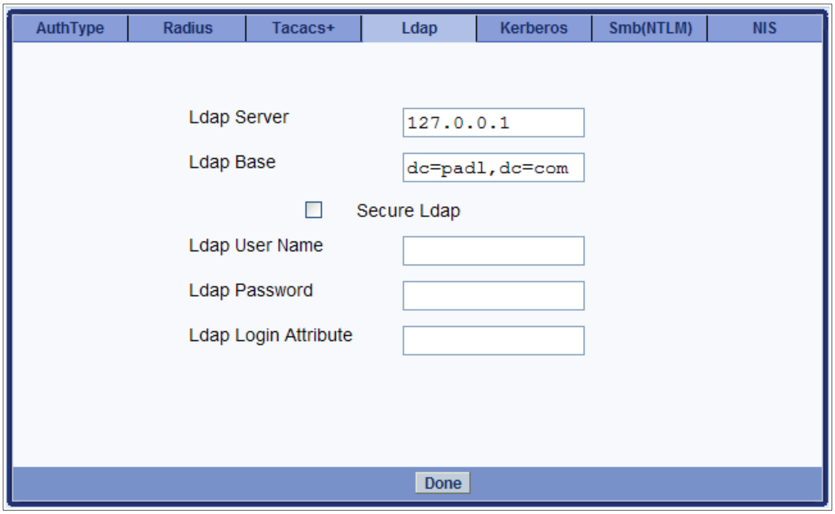
- The LDAP password
- The LDAP user name

Work with the LDAP server’s administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the 16-port IP KVM and connected devices know the passwords assigned to the accounts:

- An account for “admin”
- If LDAP authentication is specified for the 16-port IP KVM, accounts for all users who need to log on to the 16-port IP KVM to administer connected devices.
- If LDAP authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.

1. Go to Configuration>Authentication>LDAP in Expert mode.

   The “LDAP” form displays with “LDAP Server” and “LDAP Search Base” fields filled in from the current values in the `/etc/ldap.conf` file.



Ldap Server: 127.0.0.1

Ldap Base: dc=padl,dc=com

□ Secure Ldap

Ldap User Name:

Ldap Password:

Ldap Login Attribute:

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 base 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. Click “Done.”

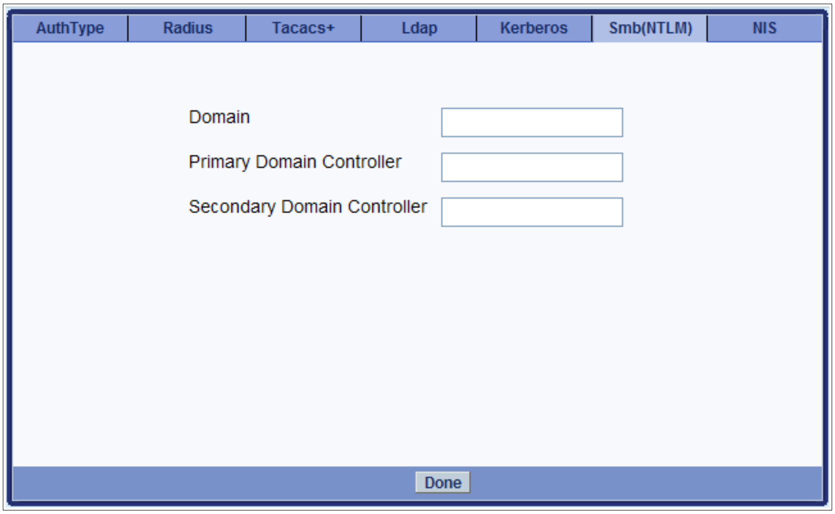
6. Click “apply changes.”

   The changes are stored in `/etc/ldap.conf` on the 16-port IP KVM.

▼ *To Configure an SMB(NTLM) Authentication Server*

Perform the following to identify the authentication server if any of the ports is configured to use the NTLM (Windows NT/2000/2003 Domain) authentication method or NTLM/Downlocal.

1. Go to Configuration>Authentication>SMB(NTLM) in Expert mode. The SMB(NTLM) form displays as shown in the following figure.



Domain

Primary Domain Controller

Secondary Domain Controller

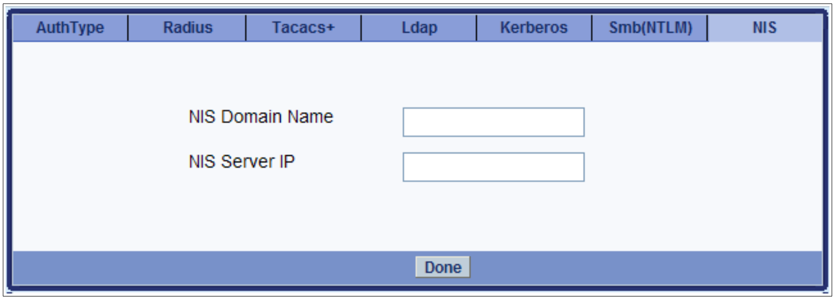
2. Fill in the form according to your configuration of the SMB server.
3. Click "Done."
4. Click "apply changes."

▼ *To Configure a NIS Authentication Server*

Perform this procedure to identify the authentication server when the 16-port IP KVM or any of its ports is configured to use the NIS authentication method or any of its variations (Local/NIS, NIS/Local, or NIS/DownLocal).

1. Go to Configuration>Authentication>NIS in Expert mode.

   The NIS form displays as shown in the following figure.



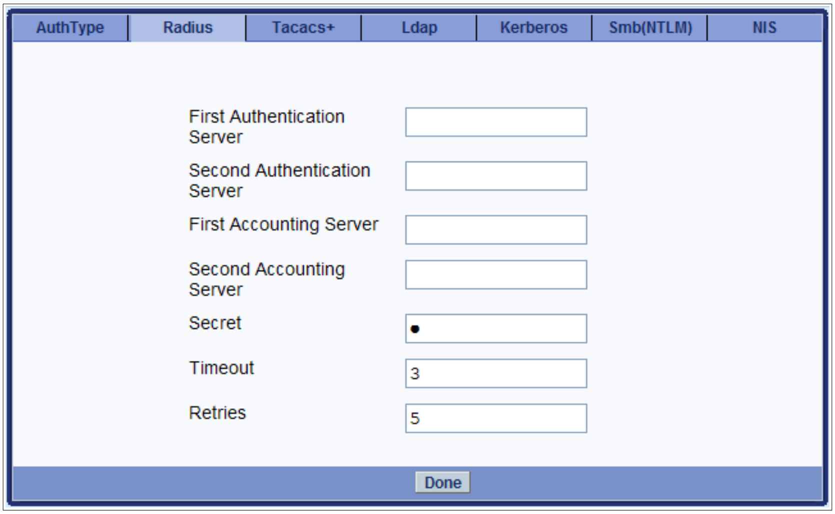
2. Fill in the form according to your configuration of the NIS server.
3. Click “Done.”
4. Click “apply changes.”

▼ To Identify a RADIUS Authentication Server

Perform this procedure to identify the authentication server when the 16-port IP KVM or any of its ports is configured to use the RADIUS authentication method or any of its variations (Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal).

1. Go to Configuration>Authentication>RADIUS in Expert mode.

The RADIUS form displays as shown in the following figure.



First Authentication Server	
Second Authentication Server	
First Accounting Server	
Second Accounting Server	
Secret	•
Timeout	3
Retries	5

2. Fill in the form according to your local setup of the RADIUS server or servers.

3. Click “Done.”

4. Click “apply changes.”

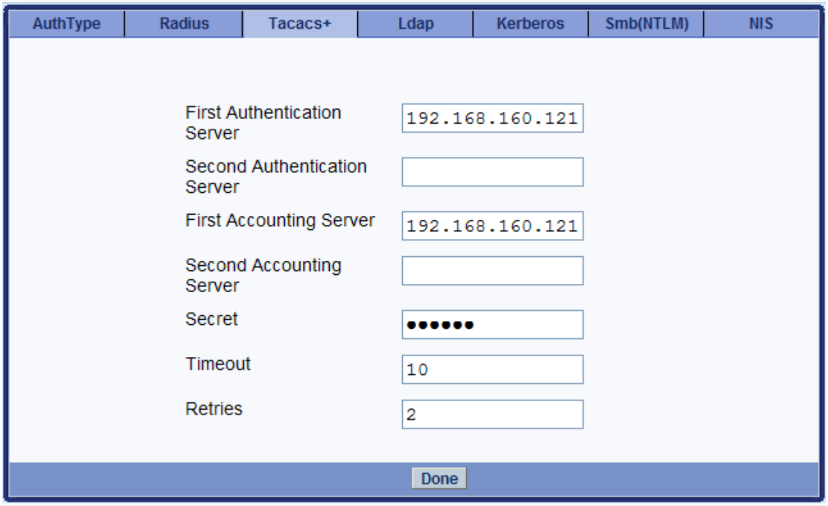
The changes are stored in `/etc/raddb/server` on the 16-port IP KVM.

▼ *To Identify a TACACS+ Authentication Server*

Perform this procedure to identify the authentication server when the 16-port IP KVM or any of its ports is configured to use the TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal).

1. Go to Configuration>Authentication>TACACS+ in Expert mode.

   The TACACS+ form appears.

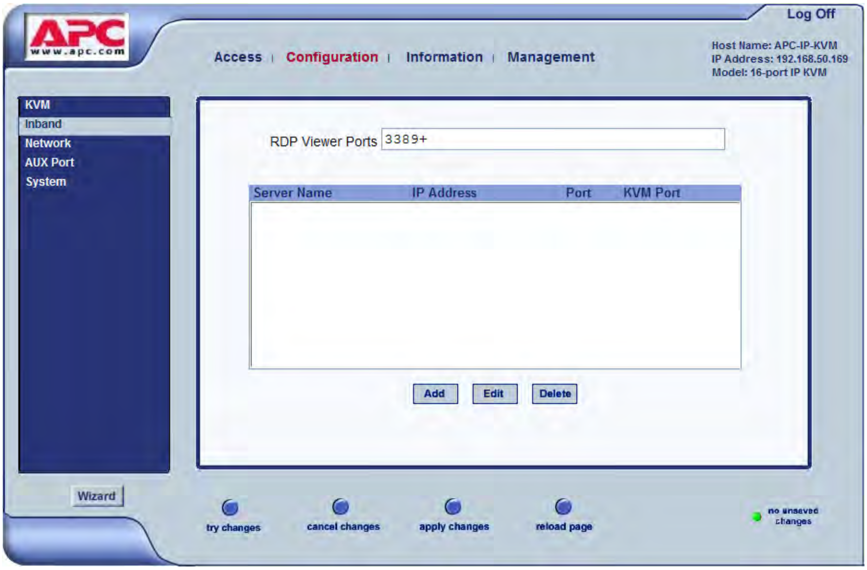


First Authentication Server	192.168.160.121
Second Authentication Server	
First Accounting Server	192.168.160.121
Second Accounting Server	
Secret	••••••
Timeout	10
Retries	2

2. Fill in the form according to your local setup of the TACACS+ server or servers.
3. Click “Done.”
4. Click “apply changes.”
5. The changes are stored in `/etc/tacplus.conf` on the 16-port IP KVM.

Configuring In-band (RDP) Servers

Selecting Configuration>Inband in Expert mode brings up the form displayed in the following figure.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

RDP Viewer Ports: 3389+

You can use the Add, Modify, and Delete buttons to configure in-band server connections to Windows Terminal Servers using RDP. Up to 16 in-band servers can be configured on a 16-port IP KVM.

If secondary 16-port IP KVM units are cascaded to the master 16-port IP KVM, administrators can configure additional in-band servers. The total number of in-band servers configured is the same as the total number of KVM ports in the whole infrastructure (master and cascaded devices). Even though it is possible to configure a KVM port on the master or on any cascaded device for each in-band server, all in-band configuration and connections are done through the master 16-port IP KVM.

For more complete access and as a backup to in-band connection failures, in-band servers can also be connected to KVM ports on the 16-port IP KVM. This enables out-of-band access to the in-band server so that if the in-band connection fails, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

See “Server Access: In-band and Out of Band” on page 28, for a description of the differences between in-band and KVM connections.

Prerequisites for In-band Access to RDP Servers

The following prerequisites must be met in order for a 16-port IP KVM in-band connection to work:

- The connected server must be a Windows (Win2000, 2003, XP, and NT) Terminal Server with RDP enabled.

  Windows Terminal Servers do not have RDP enabled by default: The administrator of these servers must enable RDP on the server in order for the 16-port IP KVM in-band connection to work.
- A 16-port IP KVM user who needs to access any in-band server must have the following:
  - A valid account created on the in-band server.

    The 16-port IP KVM does not authenticate or offer permissions configuration for in-band connections.
  - Internet access and Microsoft Internet Explorer 6 on a remote Windows client machine.
- The Windows Terminal Server must be configured on the Inband page of the Web Manager. See “To Add or Modify an In-band (RDP) Server” on page 176 for configuration instructions.
- If you want to enable an out-of-band, KVM connection as back up for an in-band connection failure or if you want to view the BIOS, POST, and boot messages on the server, the RDP server must be connected to a KVM port on the master 16-port IP KVM or on a cascaded and configured KVM unit.

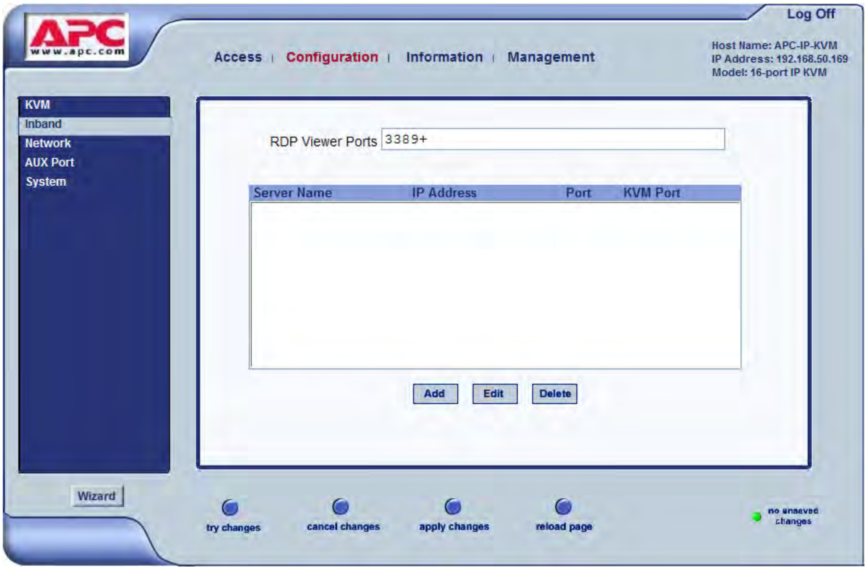
  See “To Connect Computers to KVM Ports” on page 60 for instructions on physically connecting a server to a 16-port IP KVM port.

▼ *To Add or Modify an In-band (RDP) Server*

See the previous section “Prerequisites for In-band Access to RDP Servers” on page 175 for prerequisite information to this procedure.

1. In Expert mode, go to: Configuration>Inband.

The Inband form appears.

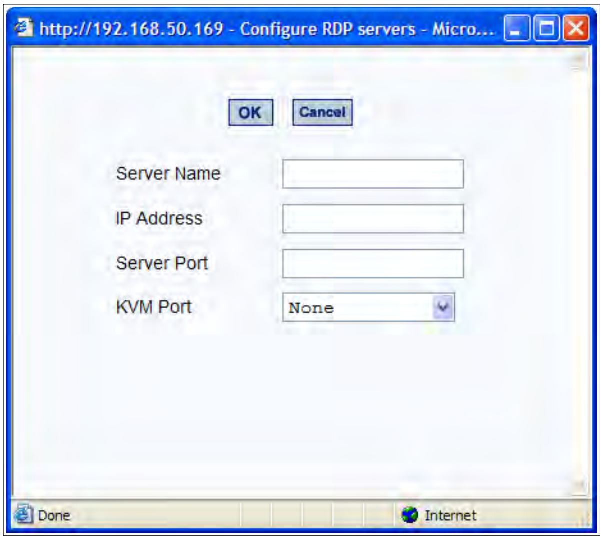


RDP Viewer Ports 3389+

Server Name	IP Address	Port	KVM Port

2. To add a server to the list, click Add.

The Configure RDP Servers dialog box appears.



Server Name

IP Address

Server Port

KVM Port: None

The connected server must be a Windows (Win2000 or NT) Terminal Server with RDP enabled.

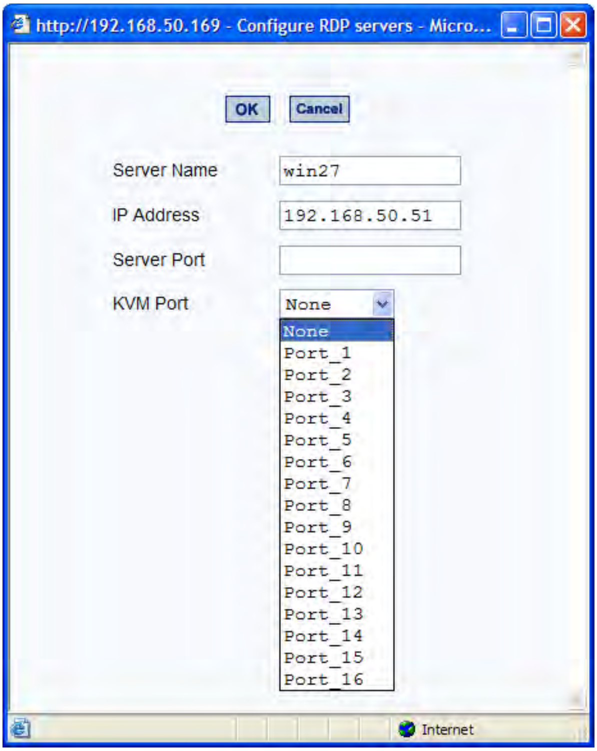
3. To modify a server, select the server on the list and click Modify.
4. In the Server Name field, specify a unique name for the in-band server.

   This name will appear in the drop-down list on the Connect to Server form.

Note: Once a name is given to an in-band server, it cannot be modified. In order to change the name of an in-band server, you must delete the server configuration and add the server again to the 16-port IP KVM.

5. In the IP Address field, enter the IP address of the in-band server.
6. (Optional) In the Server Port field, specify a port to be used if it differs from the default which is 3389.

   All servers with RDP enabled are configured with 3389 as the default port unless the administrator of the RDP server changes it.
7. To enable a back up KVM connection for the in-band server, from the KVM Port drop-down list, select the KVM port to which the in-band server is connected.



Server Name: win27

IP Address: 192.168.50.51

Server Port:

KVM Port: None

None
Port_1
Port_2
Port_3
Port_4
Port_5
Port_6
Port_7
Port_8
Port_9
Port_10
Port_11
Port_12
Port_13
Port_14
Port_15
Port_16

This enables both in-band and out-of-band access to the connected server. If the in-band connection fails or if an RDP session already exists, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

8. Click OK to close the dialog box.

9. Specify the TCP ports or a range of TCP ports to be used in the RDP Viewer Ports field.

   You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the 16-port IP KVM.

   For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”.

   You can request valid TCP ports from your network administrator.

10. Click “apply changes.”

11. Repeat steps 1-9 for every in-band server connection required.

    The 16-port IP KVM supports the configuration of up to 16 in-band servers.

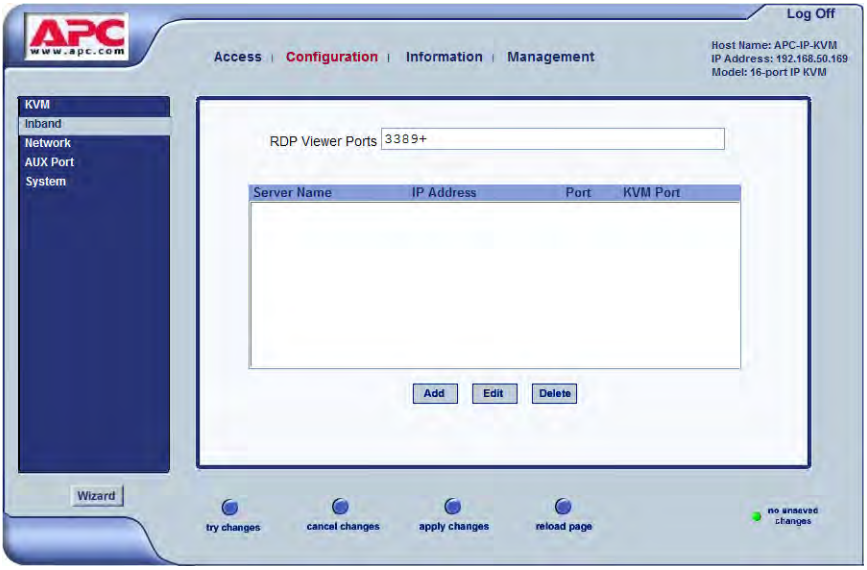
12. To connect to the in-band server, in Expert mode, go to Access>Connect to Server.

    See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 266.

▼ To Delete an In-band (RDP) Server

1. In Expert mode, go to: Configuration>Inband.

   The Inband form appears.

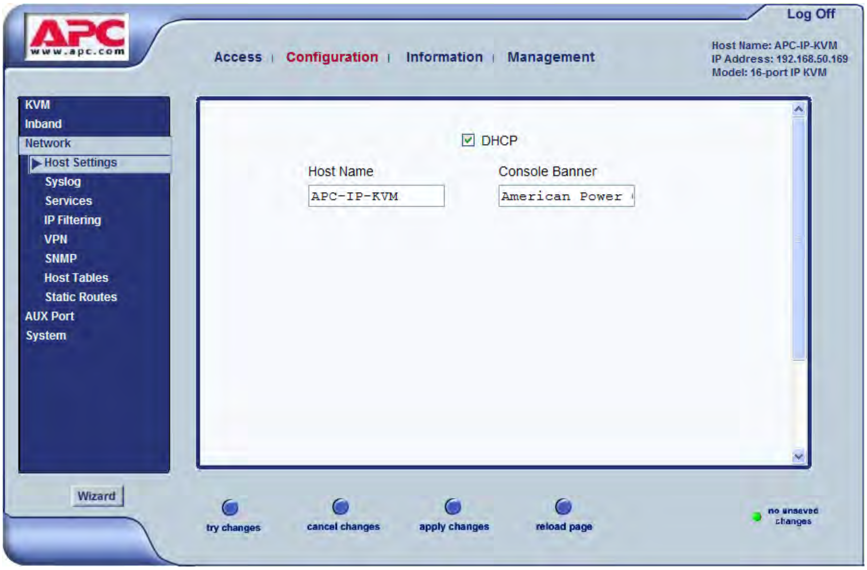


RDP Viewer Ports 3389+

2. Select the in-band server from the list and click Delete.
3. Click “apply changes.”

Network

Selecting Configuration>Network in Expert mode brings up the following form.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

☑ DHCP

Host Name: APC-IP-KVM

Console Banner: American Power

Network configuration comprises eight forms:

Table 4-1: Network Forms

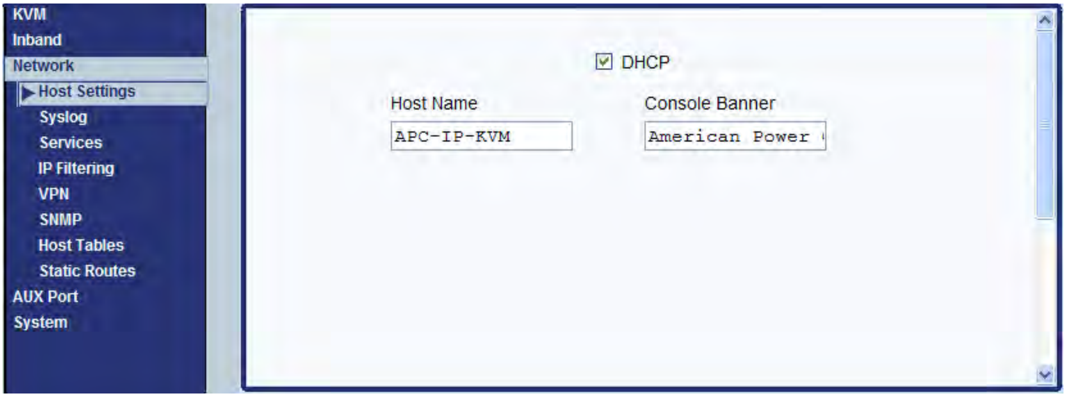
Form	Use this form to:	Where Documented
Host Settings	Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.	"Host Settings" on page 181
Syslog	Define the Syslog Servers to enable system logging.	"Syslog" on page 185
Services	Define or activate the method of access (for example, Telnet, SSH, SNMP, Client, or NTP).	"Services" on page 187

Table 4-1: Network Forms (Continued)

Form	Use this form to:	Where Documented
IP Filtering	Configure the selective filtering of packets that may potentially crack your network system or generate unnecessary traffic.	"IP Filtering" on page 188
VPN	Configure IPsec tunnels to establish a secure connection between 16-port IP KVM and a security gateway machine.	"VPN" on page 205
SNMP	Configure the SNMP server to manage complex networks.	"SNMP" on page 209
Host Table	View hosts list and add, edit, and delete hosts.	"Host Tables" on page 213
Static Routes	View, create, and delete routes from the table.	"Static Routes" on page 215

Host Settings

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.

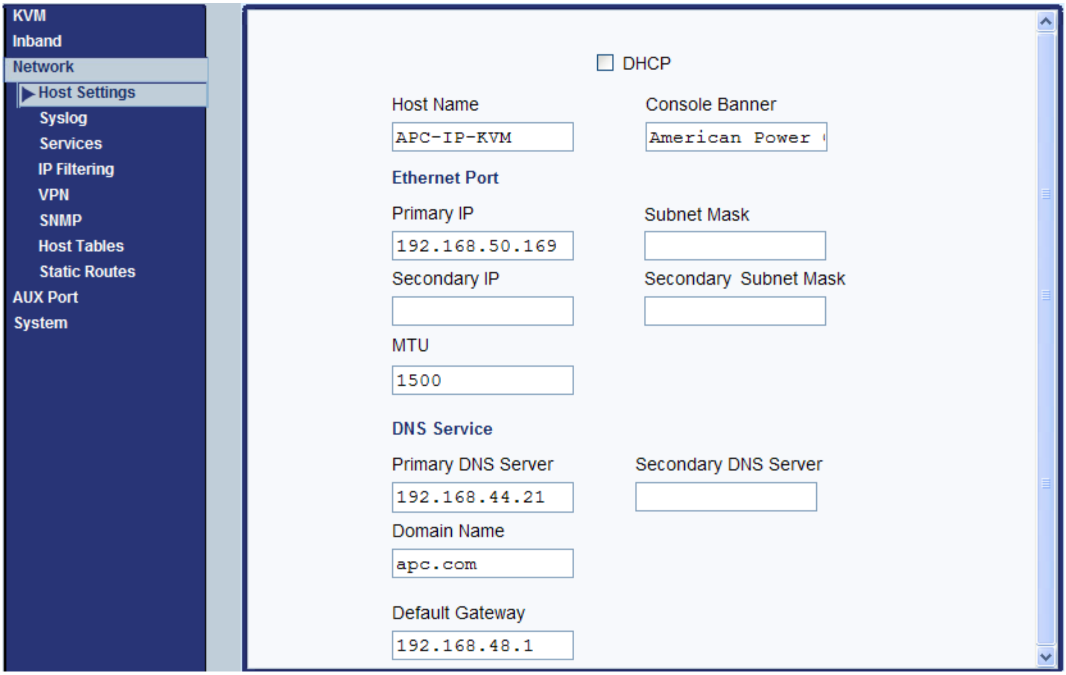


☑ DHCP

Host Name: APC-IP-KVM

Console Banner: American Power

If the “DHCP” check box is not checked, then other options appear on the form as shown in the following example.



☐ DHCP

Host Name: APC-IP-KVM

Console Banner: American Power (

Ethernet Port

Primary IP: 192.168.50.169

Subnet Mask:

Secondary IP:

Secondary Subnet Mask:

MTU: 1500

DNS Service

Primary DNS Server: 192.168.44.21

Secondary DNS Server:

Domain Name: apc.com

Default Gateway: 192.168.48.1

▼ *To Configure Host Settings [Expert]*

The Host Settings form allows you to configure the network settings for the 16-port IP KVM.

1. Go to Expert>Network>Host Settings.

   The Host Settings form appears.

2. By default, the DHCP is enabled. To disable DHCP, clear the DHCP check box.

   The system adds the Ethernet Port and DNS Service sections.

3. Complete or edit the fields described in the following table as necessary.

Table 4-2: Host Settings Configuration Fields

Field Name	Definition
Host Name	The fully qualified domain name identifying the specific host computer within the Internet.
Console Banner	A text string designed to appear on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection.
Ethernet Port	
Primary IP	The 32-bit numeric IP address of the 16-port IP KVM unit on the Internet.
Subnet Mask	The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for this IP network/subnet/supernet.
Secondary IP	The 32-bit numeric, secondary IP address of the 16-port IP KVM unit on the Internet.
Secondary Subnet Mask	The subnet mask of the secondary IP.
MTU	Maximum Transmission Unit used by the TCP protocol.
DNS Service	
Primary DNS Server	Address of the Domain Name Server.
Secondary DNS Server	Address of the backup Domain Name Server.

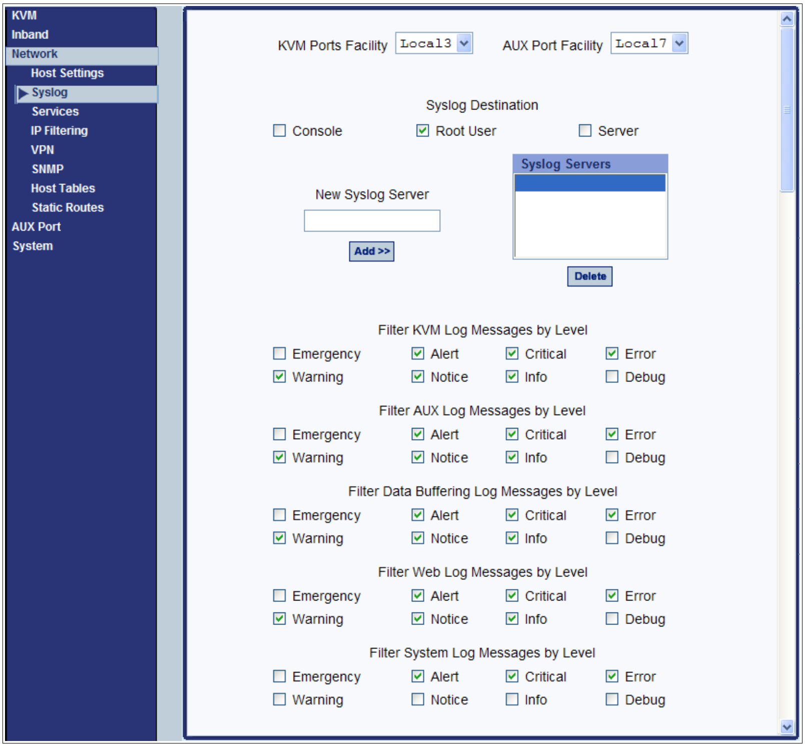
Table 4-2: Host Settings Configuration Fields (Continued)

Field Name	Definition
Domain Name	The name that identifies the domain (for example, domainname.com).
DefaultGateway	The gateway numeric identification number.

4. Select “apply changes” when done to save your configuration to flash.

Syslog

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.



KVM Ports Facility Local3 AUX Port Facility Local7

Syslog Destination

☐ Console ☑ Root User ☐ Server

New Syslog Server

Syslog Servers

Filter KVM Log Messages by Level

☐ Emergency	☑ Alert	☑ Critical	☑ Error
☑ Warning	☑ Notice	☑ Info	☐ Debug

Filter AUX Log Messages by Level

☐ Emergency	☑ Alert	☑ Critical	☑ Error
☑ Warning	☑ Notice	☑ Info	☐ Debug

Filter Data Buffering Log Messages by Level

☐ Emergency	☑ Alert	☑ Critical	☑ Error
☑ Warning	☑ Notice	☑ Info	☐ Debug

Filter Web Log Messages by Level

☐ Emergency	☑ Alert	☑ Critical	☑ Error
☑ Warning	☑ Notice	☑ Info	☐ Debug

Filter System Log Messages by Level

☐ Emergency	☑ Alert	☑ Critical	☑ Error
☐ Warning	☐ Notice	☐ Info	☐ Debug

You can use the Syslog form to configure how the 16-port IP KVM handles syslog 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 of the form is used to tell the 16-port IP KVM where to send syslog messages:

- You can specify one facility number for messages from AUXports and another facility number for messages from KVM ports.

  Obtain the facility numbers to use from the syslog server's administrator. See "To Add a Syslog Server [Wizard]" on page 119 for how syslogging is configured for the 16-port IP KVM under the Configuration>General form. You can specify the same or different syslog servers and the same or duplicate facility numbers according to your site's configuration.
- You can send 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, or to one or more syslog servers.
- You can add or delete entries for syslog servers.

The bottom of the form has check boxes for specifying which types of messages are forwarded based on the following criteria:

- Their severity level: "Emergency," "Alert," "Critical," "Error," "Warning," "Notice," "Info," "Debug"
- Their category "CAS/AUX log;" "KVM log;" "Data Buffering log;" "Web log;" or "System log."

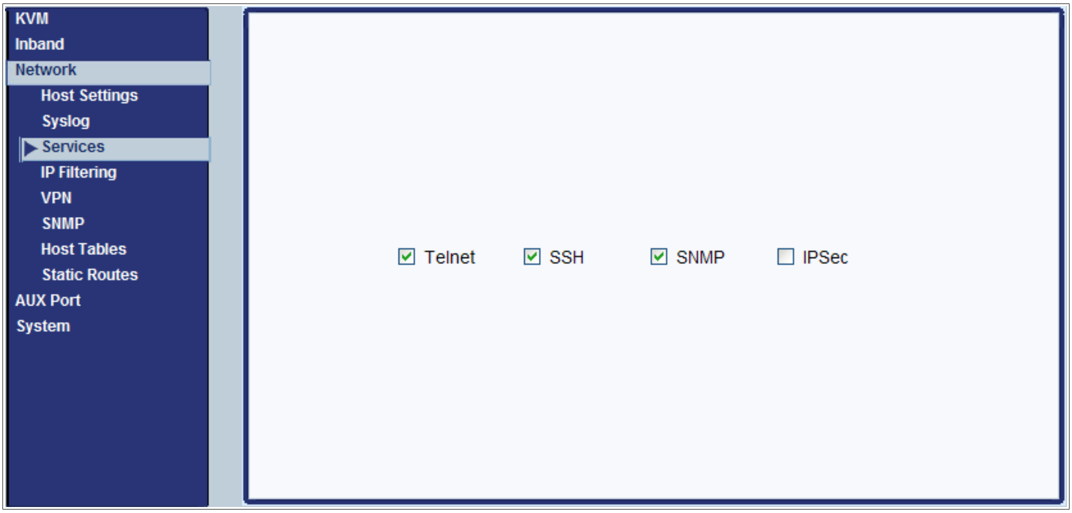
▼ To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]

1. Go to Configuration>Network>Syslog in Expert mode.

   The Syslog form appears.
2. Select a destination for the Syslog messages by clicking the check box next to one or all of the options: "Console," "Root User," or "Server."
3. 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.
4. Select a facility number for messages generated by KVM or AUX ports by selecting the number from the "CAS/AUX Ports Facility" drop-down list.
5. Select a facility number for messages generated by KVM ports by selecting the number from the "KVM Ports Facility" drop-down list.
6. Click "apply changes."

Services

Selecting Configuration>Network>Services in Expert Mode, brings up the following form.



☑ Telnet ☑ SSH ☑ SNMP □ IPSec

By selecting the appropriate box, the Services form allows you to enable or disable the daemons to use to allow different incoming connections.

Note: If you plan on using VPN, make sure to enable IPsec.

Depending on the security requirements of your site, you may want to enable or disable the daemons that support the following types of connections:

- telnet [enabled by default]
- SSH [enabled by default]
- SNMP [enabled by default]
- IPSec

Each of these services is required when telnet, ssh, SNMP, or VPN are configured, as described in the following table.

Service Name	Notes and Where Documented
Telnet	Enable telnet if users need to access the 16-port IP KVM through telnet.
SNMP	Enable “SNMP” if you configure SNMP in “To Configure SNMP” on page 210.
IPsec	Enable “IPsec” if you configure VPN in “To Configure VPN” on page 206.

▼ *To Select the Daemons Used for Incoming Connections*

1. In Expert mode got to: Configuration>Network>Services.

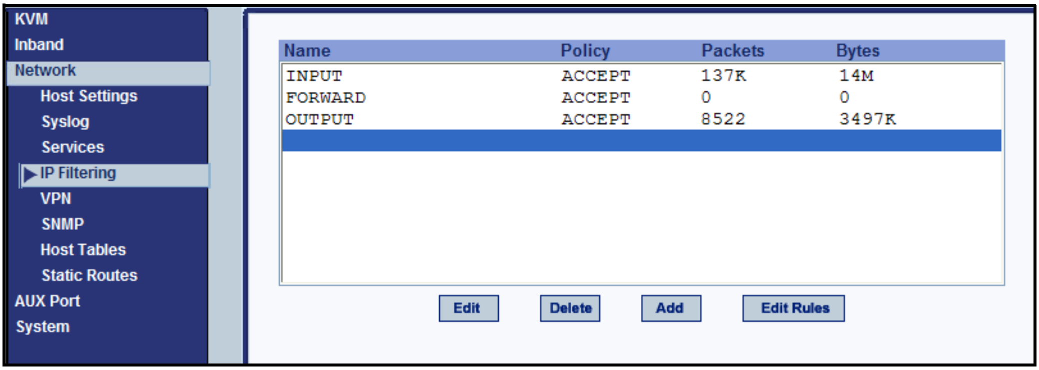
   The Services form appears.

2. Select or clear the check boxes next to the desired service(s) to enable or disable the service.

3. Select “apply changes” when done.

IP Filtering

Selecting Configure>Network>IP Filtering in Expert mode brings up the IP Filtering form as shown in the following figure.



Name	Policy	Packets	Bytes
INPUT	ACCEPT	137K	14M
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	8522	3497K

You can use the IP Filtering form to filter traffic to and from the 16-port IP KVM and block traffic according to rules you define.

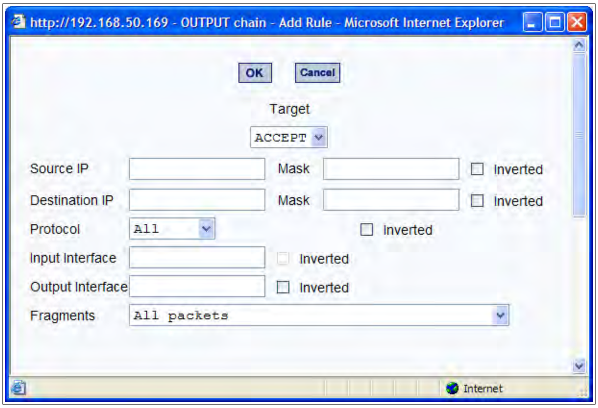
The 16-port IP KVM uses chains and rules for filtering packets like a firewall. Each entry in the list represents a chain with a set of rules.

The form 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 form to do the following to specify packet filtering:

- Add a new chain and specify rules for that chain
- Add new rules
- Delete existing chains and rules.

Add Rule and Edit Rule Options

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


http://192.168.50.169 - OUTPUT chain - Add Rule - Microsoft Internet Explorer
OK
Cancel
Internet

Target: ACCEPT

Source IP ____ Mask ____ □ Inverted

Destination IP ____ Mask ____ □ Inverted

Protocol: All □ Inverted

Input Interface ____ □ Inverted

Output Interface ____ □ Inverted

Fragments: All packets

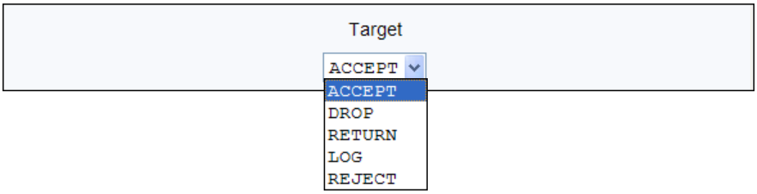
Inverted Check Boxes

If you check the “Inverted” check box on any line, the target action is performed on packets that do not match any of the criteria specified in that line when any other specified criteria are also met.

For example, if you select DROP as the target action, check “Inverted” on the line with a source IP address specified, 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 Drop-down List Options

The “Target” is the action to be performed on an IP packet that matches all the criteria specified in a rule.The target drop-down list is shown in the following figure.



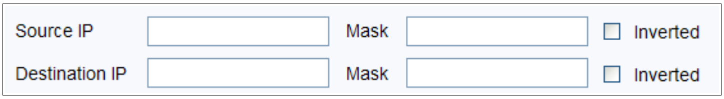
If the “LOG” and “REJECT” targets are selected, additional fields appear as described under “LOG Target” on page 194 and “REJECT Target” on page 195.

Source or Destination IP and Mask

If you fill in the “Source IP” field, incoming packets are filtered for the specified IP address. If you fill in the “Destination IP” field, outgoing packets are filtered for the specified IP address.

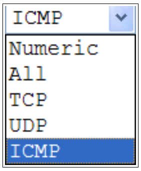
If you fill in either “Mask” field, incoming or outgoing packets are filtered for IP addresses from the network in the specified netmask.

The source and destination IP and related fields are shown in the following figure.



Protocol

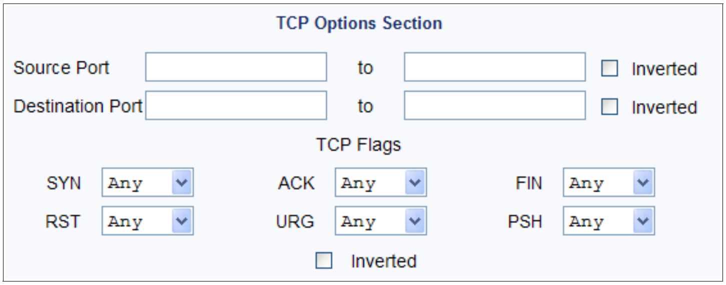
You can select a protocol for filtering from the “Protocol” drop-down list, which is shown in the following figure.



The additional fields that appear for each protocol are explained in the following sections.

TCP Protocol Fields

If you select TCP as the protocol when specifying a rule, the additional fields shown in the following figure appear for you to fill out at the bottom of the form.



TCP Options Section

Source Port ____ to ____ □ Inverted

Destination Port ____ to ____ □ Inverted

TCP Flags

SYN	Any	ACK	Any	FIN	Any
RST	Any	URG	Any	PSH	Any

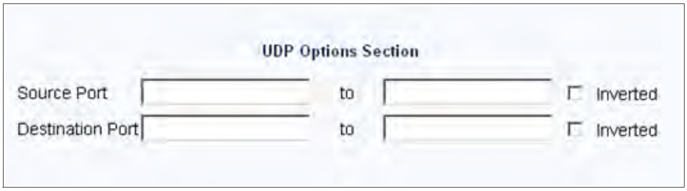
□ Inverted

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

Field/Menu Option	Definition
Source Port - OR - **Destination Port** -AND- **to**	You can specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.
TCP Flags	You can select the check box next to any of the TCP flags: “SYN” (synchronize), “ACK” (acknowledge), “FIN” (finish), “RST” (reset), “URG” (urgent), or “PSH” (push) and select either “Any,” “Set,” or “Unset,” TCP packets are filtered for the specified flag and the selected condition.

UDP Protocol Fields

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



UDP Options Section

Source Port ______ to ______ □ Inverted

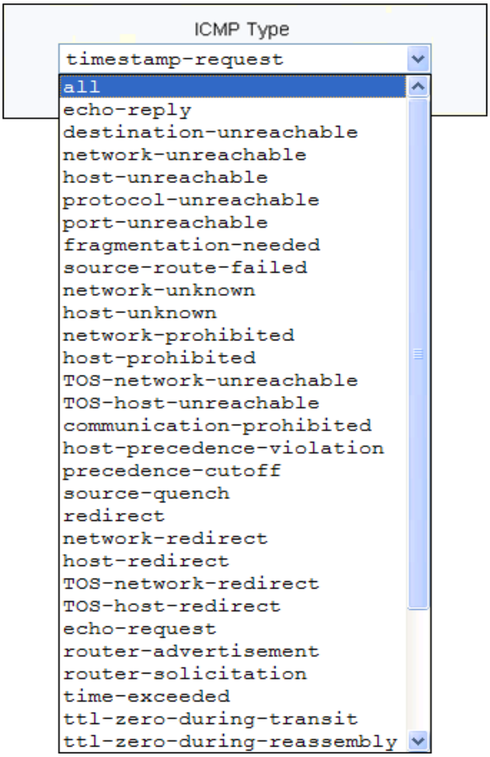
Destination Port ______ to ______ □ Inverted

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

Field	Definition
Source Port - OR - **Destination Port** -AND- **to**	Specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. You can specify a source or destination port number for filtering in the “Source Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.

ICMP Protocol Fields

If you select ICMP as a protocol when specifying a rule, the ICMP Type drop-down list appears in the ICMP Options Section at the bottom of the IP Filtering form. The following figure shows the options.



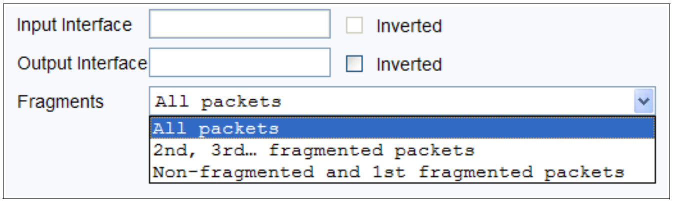
ICMP Type

timestamp-request

Input Interface, Output Interface, and Fragments

If you enter an interface (such as `eth0` or `eth1`) in the “Input Interface” field, incoming packets are filtered for the specified interface. If you enter an interface in the “Output Interface” field, outgoing packets are filtered for the specified interface.

These fields are shown in the following figure.



Input Interface ☐ Inverted

Output Interface ☐ Inverted

Fragments All packets

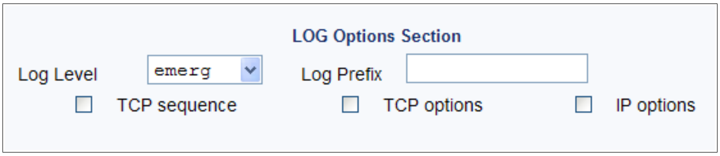
All packets
2nd, 3rd… fragmented packets
Non-fragmented and 1st fragmented packets

The following table defines the fields in the previous figure.

Field	Definition
Input Interface	The input interface (eth*N*) for the packet
Output Interface	The output interface (eth*N*) for the packet
Fragments	The types of packets to be filtered: All packets 2nd, 3rd... fragmented packets Non-fragmented and 1st fragmented packets

LOG Target

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

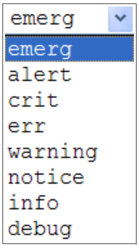


LOG Options Section

Log Level emerg Log Prefix

□ TCP sequence □ TCP options □ IP options

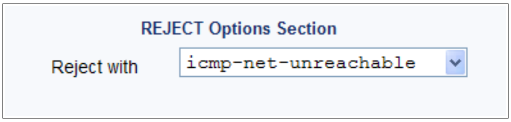
The following table defines the menu options, field, and check boxes in the “LOG Options Section.”

Field or Menu Name	Definition
Log Level	One of the options in the drop-down list:  emerg emerg alert crit err warning notice info debug
Log Prefix	The prefix to use in the log entry.

Field or Menu Name	Definition
TCP Sequence	Checking the box includes the TCP sequence in the log.
TCP Options	Checking the box includes TCP options in the log.
IP Options	Checking the box includes IP options in the log.

REJECT Target

If you select REJECT from the Target drop-down list, the following drop-down list appears



REJECT Options Section

Reject with icmp-net-unreachable

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

Firewall Configuration Procedures

The following table has links to the procedures for defining packet filtering:

To Add a Chain	Page 195
To Edit a Chain	Page 196
To Edit a Rule for IP Filtering	Page 197
To Add a Packet Filtering Rule	Page 198

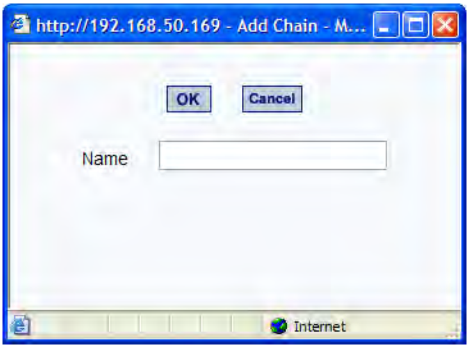
▼ *To Add a Chain*

1. Go to Configuration>Network>Firewall Configuration in Expert Mode.

   The IP Filtering form appears.

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.

   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 “To Add a Rule for IP Filtering” on page 200.

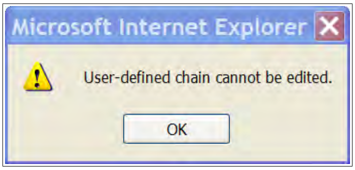
▼ *To Edit a Chain*

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

Note: User-defined chains cannot be edited.

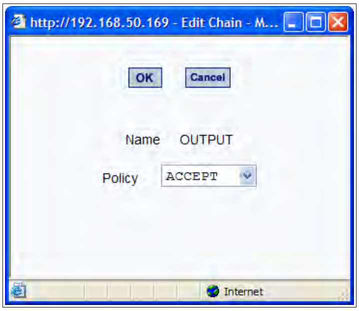
1. Go to Configuration>Network>Firewall Configuration in Expert Mode.
2. Select one of the default chains from Chain list, and then click the “Edit” button.

   If you select a user-defined chain, the following dialog box appears.



User-defined chain cannot be edited.

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



Name OUTPUT

Policy ACCEPT

3. Select the desired policy from the Policy drop-down list, and then click OK.
4. Click “apply changes.”
5. To edit any rules for this chain, go to “To Edit a Rule.”

▼ *To Edit a Rule for IP Filtering*

1. In Expert mode go to: Configuration>Network>IP Filtering.

   The IP Filtering configuration form appears.

   See “To Add a Rule for IP Filtering” on page 200 procedure section for a definition of the user input fields.
2. Select a chain whose rule you want to edit.
3. Click the Edit Rule button.

   The Edit Rules form appears. Each line represents a rule for the selected chain.
4. Select the Chain you wish to edit from the Chain list, and click the Edit Rule button.

   The Edit Rules form appears.
5. Specify the rule as desired.

   See “IP Filtering” on page 188 for a definition of the input fields, if needed.
6. Click on the “apply changes” button to complete the procedure.

▼ To Add a Packet Filtering Rule

1. Go to Configuration>Network>Firewall Configuration in Expert Mode.
2. Select the chain whose rule you want to edit from Chain list, and then and then click the “Edit Rules” button.
3. Click the “Edit Rule” button.

   The “Edit Rule for Chain” dialog box appears.
4. Specify the rule as desired.
5. Click the “Add” button.

   The “Add Rule” dialog box appears.
6. Complete the Add Rule dialog box.
7. Click “apply changes.”

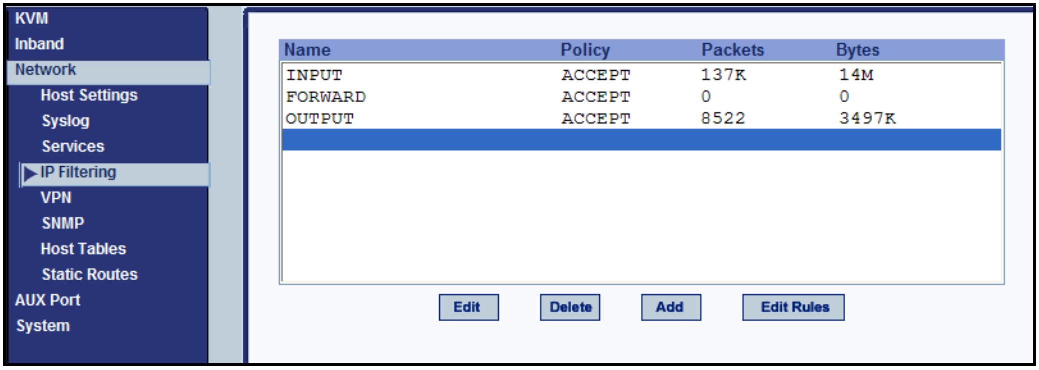
You can perform the following task from the IP Filtering Form:

- “To Add a Chain for IP Filtering” on page 198
- “To Edit A Chain for IP Filtering” on page 199
- “To Add a Rule for IP Filtering” on page 200
- “To Edit a Rule for IP Filtering” on page 197

▼ To Add a Chain for IP Filtering

1. In Expert mode go to: Configuration>Network>IP Filtering.

   The IP Filtering configuration form appears.

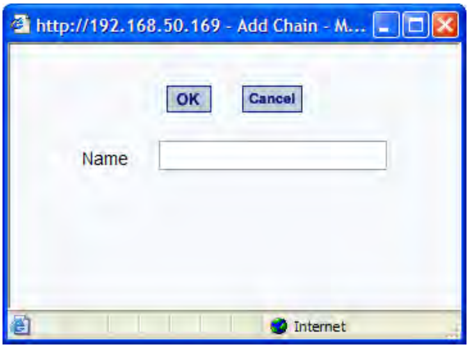


Name	Policy	Packets	Bytes
INPUT	ACCEPT	137K	14M
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	8522	3497K

Each line in the list box represents a chain. For a definition or explanation of the field columns, refer to the introductory section of this procedure or to the field definitions for the Edit Rule dialog box, next section.

2. To add a chain, select the Add button.

   The Add Chain dialog box appears.



3. Enter the name of the chain that you are adding to the filter table, and then select OK. (Spaces are not allowed in the chain name.)
4. After entering a new chain name, click on the Edit Rules button to enter the rules for that chain.
5. Select OK to commit your changes.
6. To add rules to your new chain, see “To Add a Rule for IP Filtering” on page 200.

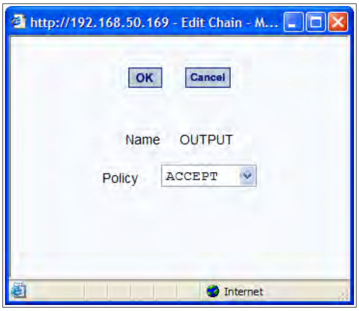
▼ *To Edit A Chain for IP Filtering*

1. In Expert mode go to: Configuration>Network>IP Filtering.

   The IP Filtering configuration form appears.

2. Select the Chain you wish to edit from the Chain list box (or filter table), and select the Edit button.

   The Edit Chain dialog box appears.



Name OUTPUT

Policy ACCEPT

3. Modify the Policy field, as needed, and select OK.

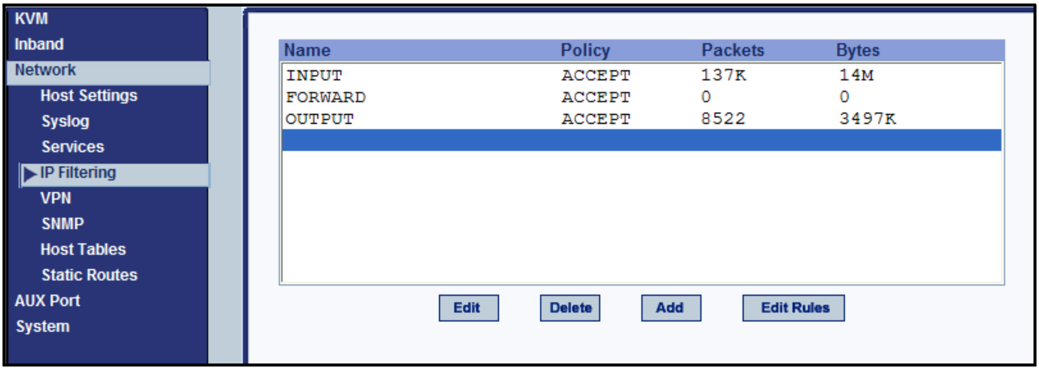
4. Verify your entry from the main form and click “apply changes” to save your changes.

5. If you need to add any rules for this chain, go to “To Add a Rule for IP Filtering” on page 200.

▼ *To Add a Rule for IP Filtering*

1. In Expert mode go to: Configuration>Network>IP Filtering.

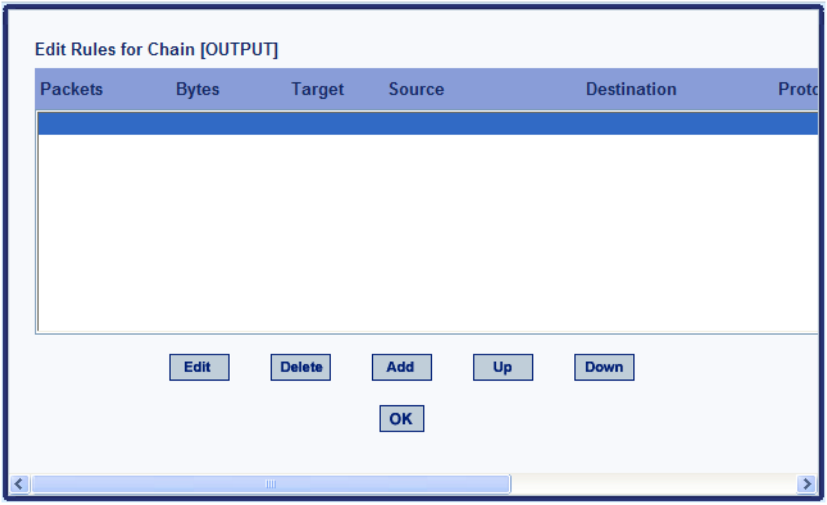
   The IP Filtering configuration form appears.



Name	Policy	Packets	Bytes
INPUT	ACCEPT	137K	14M
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	8522	3497K

2. Click the Edit Rule button.

   The Edit Ruels for Chain configuration form appears.

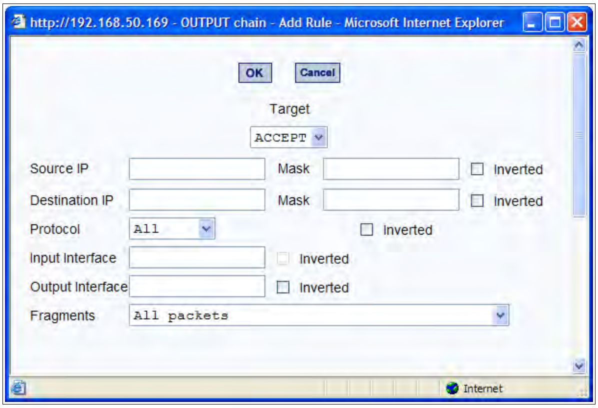


Edit Rules for Chain [OUTPUT]

Packets	Bytes	Target	Source	Destination	Proto

3. Click the Add button.

   The Add Rule dialog box appears.


http://192.168.50.169 - OUTPUT chain - Add Rule - Microsoft Internet Explorer
OK
Cancel
Internet

Target: ACCEPT

Source IP: Mask: □ Inverted

Destination IP: Mask: □ Inverted

Protocol: All □ Inverted

Input Interface: □ Inverted

Output Interface: □ Inverted

Fragments: All packets

4. Complete the following data fields as necessary:

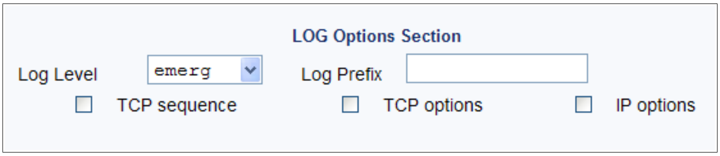
Field Name	Definition
Target	Indicates the action to be performed to the IP packet when it matches the rule. For example, the kernel can ACCEPT DROP, RETURN, LOG or REJECT the packet by sending a message, translating the source or the destination IP address/port or sending the packet to another user-defined chain.
Source IP	The source IP address.
Mask	Source network mask. Required when a network should be included in the rule.
Inverted	Select the check box adjacent to Source IP to invert the target action. For example, the action assigned to the target will be performed to all source IPs/Masks except to the one just defined.
Destination IP	Destination IP address.
Mask	Destination network mask.

Field Name	Definition
Inverted	Select the check box adjacent to Destination IP to invert the target action. For example, the action assigned to the target will be performed to all Destination/ Mask IPs except to the one just defined.
Protocol	The transport protocol to check. If the numeric value is available, select Numeric and type the value in the adjacent field; otherwise, select one of the other options.
Inverted	Select the check box adjacent to Protocol to invert the target action. For example, the action assigned to the target will be performed to all protocols except to the one just defined.
Input Interface	The interface where the IP packet should pass. The Input Interface option appears only for the INPUT and FORWARD chains.
Inverted	Select the check box adjacent to Input Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.
Output Interface	The interface where the IP packet should pass. The Output interface option will appear for the chains FORWARD and OUTPUT.
Inverted	Select box adjacent to Output Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.

Field Name	Definition
Fragments	Indicates the fragments or unfragmented packets to be checked. The IP Tables can check for: • All Packets • 2nd, 3rd... fragmented packets • Non-fragmented and 1st fragmented packets
ICMP Type	This dropdown list box contains all the ICMP types that may be applied to the current rule.
Inverted	This ICMP option will be applied to all rules except the currently selected rule.

5. Complete the following additional fields as necessary:

- If you selected Log from the Target field, the following options also appear.



LOG Options Section

Log Level: emerg

Log Prefix:

□ TCP sequence

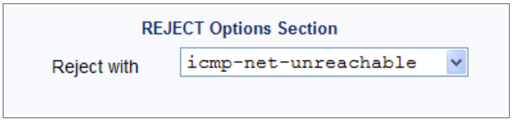
□ TCP options

□ IP options

Field Name	Definition
Log Level	The log level classification to be used based on the type of error message (such as, alert, warning, info, debug, and so on.).
Log Prefix	The prefix that will identify the log.
TCP Sequence	Check box to include TCP sequence in the log.
TCP Options	Check box to include TCP options in the log.

Field Name	Definition
IP Options	Check box to include IP options in the log.

- If you selected Reject from the Target field, the following field appears:



Reject with: icmp-net-unreachable

"Reject with" means that the filter drops the input packet and sends back a reply packet according to any of the reject types listed below.

Using tcp flags and appropriate reject type, the packets are matched with the REJECT target. The following options are available:

- icmp-net-unreachable – ICMP network unreachable alias
- icmp-host-unreachable – ICMP host unreachable alias
- icmp-port-unreachable – ICMP port unreachable alias
- icmp-proto-unreachable – ICMP protocol unreachable alias
- icmp-net-prohibited – ICMP network prohibited alias
- icmp-host-prohibited – ICMP host prohibited alias
- echo-reply – Echo reply alias
- tcp-reset – TCP RST packet alias

6. Click on the OK button when done.
7. Click on "apply changes."

VPN

When VPN Connections is selected under Configuration>Network in Expert mode, you can configure one or more VPN connections.

Selecting one of the existing VPN connections and clicking the edit button or the add button launches a dialog box to prompt for the details of the connection. Complete the fields in the dialog box. The RSA keys may be entered using the Copy and Paste feature of your Browser.

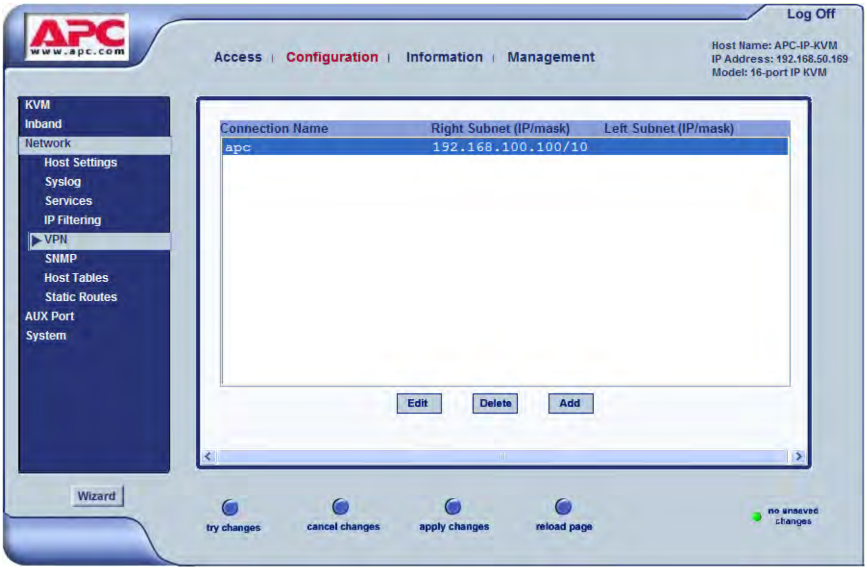
If needed, see "VPN and the 16-port IP KVM" on page 48 for background information.

▼ *To Configure VPN*

For the VPN to function to properly, ensure that you have also enabled IPsec on the Services form. See “To Select the Daemons Used for Incoming Connections” on page 188 for instructions on configuring IPsec.

1. In Expert mode, go to: Configure>Network>VPN.

The VPN form appears.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

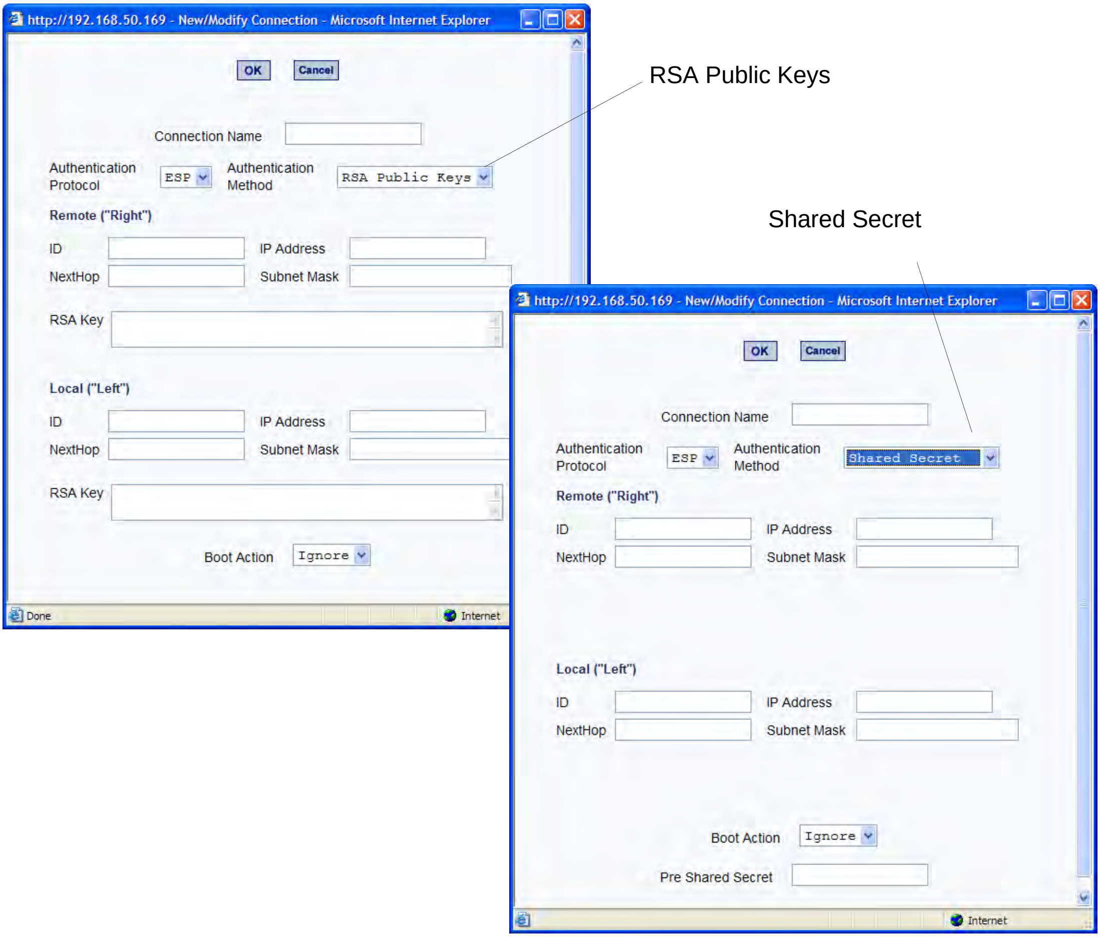
Connection Name	Right Subnet (IP/mask)	Left Subnet (IP/mask)
apc	192.168.100.100/10	

2. To edit a VPN connection, select the VPN connection that you wish to edit from the form, and then select the Edit button.

- OR -

To add a VPN Connection, select the Add button.

The New/Modify Connection dialog box appears.



Authentication Protocol: ESP
Authentication Method: RSA Public Keys
Boot Action: Ignore

Authentication Protocol: ESP
Authentication Method: Shared Secret
Boot Action: Ignore

RSA Public Keys

Shared Secret

Note: If the selected authentication method is RSA Public Keys, the dialog box on the left of the previous figure is used; if the authentication method is Shared Secret, the dialog box on the right is used.

3. Edit or complete the appropriate fields as follows.

Field Name	Definition
Connector Name	Name of the VPN connection.

Field Name	Definition
Authentication Protocol	Authentication protocol used to establish a VPN connection.
Authentication Method	Authentication method used to establish a VPN connection.
Remote ("Right")	
ID	The identification name of the remote host, commonly referred to as the "right" host.
IP Address	Remote IP address.
NextHop	The router to which the Console Server sends packets in order to deliver them to the left.
Subnet Mask	As indicated.
RSA Key	You may use the copy and paste feature of your browser to enter the RSA key.
Local ("Left")	
ID	The identification name of the local host, commonly referred to as the "left" host.
IP Address	The IP address of the local or left host.
NextHop	The router to which the Console Server sends packets in order to deliver them to the right.
Subnet Mask	As indicated
RSA Key	You may use the copy and paste feature of your browser to enter the RSA key.

Field Name	Definition
Boot Action	The boot action configured for the local host.
Pre-Shared Secret	Pre-shared password between left and right users.

4. Select the OK button when done.
5. Select the “apply changes” button to save your configuration.

SNMP

Short for Simple Network Management Protocol, SNMP is a set of protocols for managing network devices. 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 16-port IP KVM uses the Net-SNMP package (http://www.net-snmp.org/). The Net-SNMP package contains various tools relating to the Simple Network Management Protocol including an extensible agent, an SNMP library, tools to request or set information from SNMP agents, tools to generate and handle SNMP traps, a version of the unix 'netstat' command using SNMP, and a Tk/Perl mib browser.

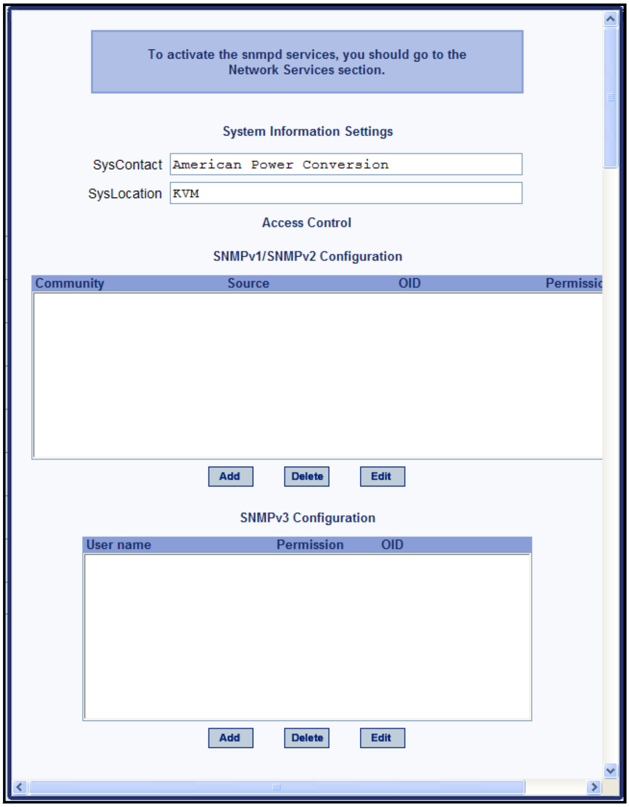
SNMP is configured with community names, OID and user names. The 16-port IP KVM supports SNMP v1, v2, and v3. The two versions require different configurations. SNMP v1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

Important: Check the SNMP configuration before gathering information about 16-port IP KVM by SNMP. An unauthorized user can implement different types of attacks to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in 16-port IP KVM cannot permit the public community to read SNMP information.

▼ *To Configure SNMP*

1. In Expert Mode go to: Configuration>Networks>SNMP.

The SNMP form appears.



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

System Information Settings

SysContact: American Power Conversion

SysLocation: KVM

Access Control

SNMPv1/SNMPv2 Configuration

Community	Source	OID	Permissic

SNMPv3 Configuration

User name	Permission	OID

2. Enter the following system information, as necessary:

Field Name	Definition
Community	The community name acts as a password 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.
SysContact	The email of the person to contact regarding the host on which the agent is running (for example, me@mymachine.mydomain)
SysLocation	The physical location of the system (for example, mydomain).

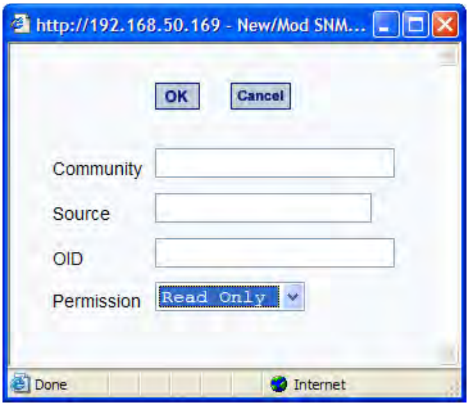
If you are using SNMPv3, skip to Step 6.

3. To Add an SNMP agent using SNMPv1/SNMP2 Configuration, select the Add button located at the bottom of this view table.

   OR

   To edit an SNMP agent, select the Edit button.

   The New/Modify SNMP Daemon Configuration dialog box appears.



Community

Source

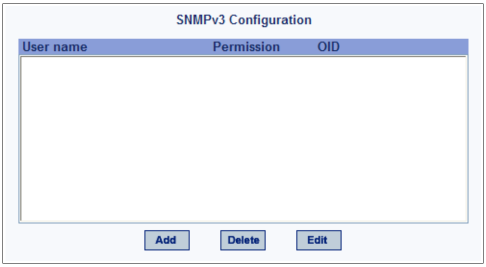
OID

Permission Read Only

4. Complete the dialog box as follows:

Field Name	Definition
Community	The community name acts as a password 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.
Source	The source IP address or range of IP address.
OID	Object Identifier.
Permission	Select the permission type: • Read Only – Read-only access to the entire MIB except for SNMP configuration objects. • Read/Write – Read-write access to the entire MIB except for SNMP configuration objects. • Admin – Read-write access to the entire MIB.

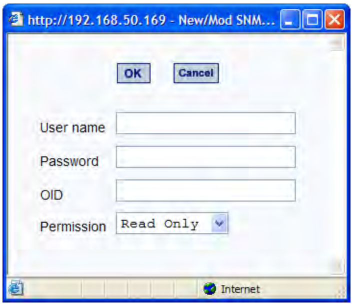
5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form and select the Add button located at the bottom of this view table



6. To add an SNMP agent using SNMPv3, click Add.

7. To edit an SNMP agent using SNMPv3, click Edit.

   The New/Modify SNMP Daemon Configuration dialog box.



User name

Password

OID

Permission Read Only

8. Complete the form and when done.

Field Name	Definition
User Name	Name of user account accessing the 16-port IP KVM.
Source	The source IP address or range of IP address.
OID	Object Identifier.
Permission	Select the permission type: • Read Only – Read-only access to the entire MIB except for SNMP configuration objects. • Read/Write – Read-write access to the entire MIB except for SNMP configuration objects.

9. Click the OK button.

10. Verify your entry or modification on the SNMP form.

11. Click “apply changes” to complete the procedure.

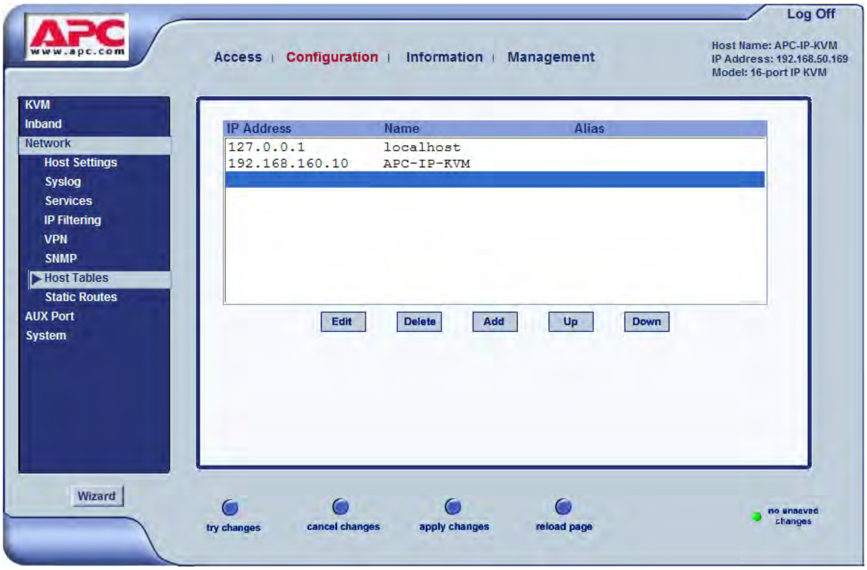
Host Tables

The Host Tables form enables you to keep a table of host names and IP addresses that comprise your local network, and thus provide information about your network environment.

▼ To Configure Hosts

1. In Expert Mode, go to: Configuration>Network>Host Tables.

   The Host Tables form appears.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

IP Address	Name	Alias
127.0.0.1	localhost	
192.168.160.10	APC-IP-KVM	

2. Do on of the following:

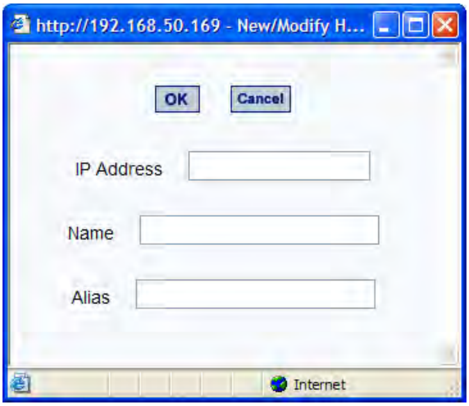
   - To edit a host, select the host IP address from the Host Table and then click the Edit button.

     If the list is long, use the Up and Down buttons to go through each item in the list.

   - OR -

   - To add a host, click the Add button.

   The New/Modify Host dialog box appears.



3. Enter the new or modified host address in the IP Address field and the host name in the Name field.

4. Click the OK button.

5. To delete a host, select the host you wish to delete from the Host Table form, and select the Delete button on the form.

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

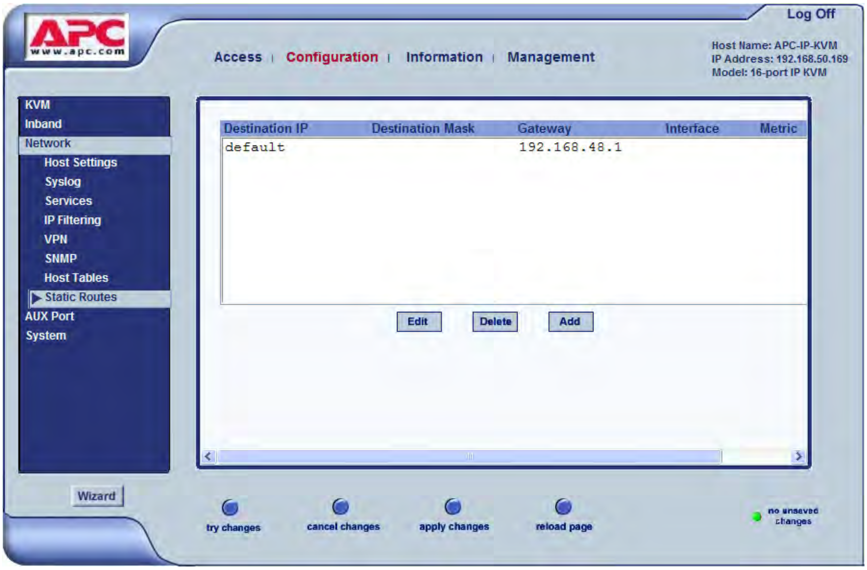
Static Routes

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.

▼ *To Add, Edit, or Delete a Static Route*

1. In Expert mode, go to: Configure>Network>>Static Routes.

   The Static Routes table form appears.



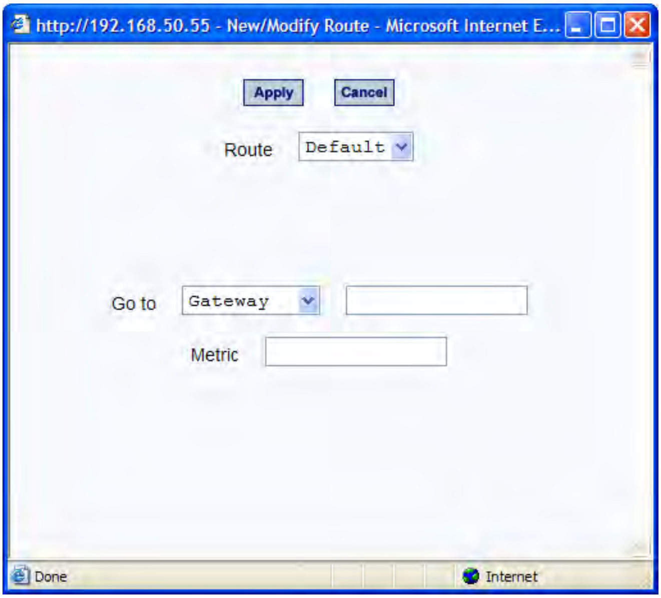
Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Destination IP	Destination Mask	Gateway	Interface	Metric
default		192.168.48.1		

2. Do one of the following:

- To edit a static route, select a route from the Static Routes form, and click the Edit button.
- To add a static route, select the Add button from the form.

The New/Modify Route dialog box appears.


http://192.168.50.55 - New/Modify Route - Microsoft Internet E...
Apply
Cancel
Done
Internet

Route: Default

Go to: Gateway

Metric

3. Complete the dialog box as follows:

Table 4-3: Add/Modify Static Routes Fields

Field Name	Definition
Route	Select Default, Network, or Host.
Network IP	The address of the destination network. This field appears only if Network is selected.
Network Mask	The mask of the destination network. This field appears only if Network is selected.
Host IP	The IP address of the destination host. This field appears only if Host is selected.
Go to	Select Gateway or Interface.

Table 4-3: Add/Modify Static Routes Fields

Field Name	Definition
Field Adjacent to Go to	The address of the gateway or interface.
Metric	The number of hops.

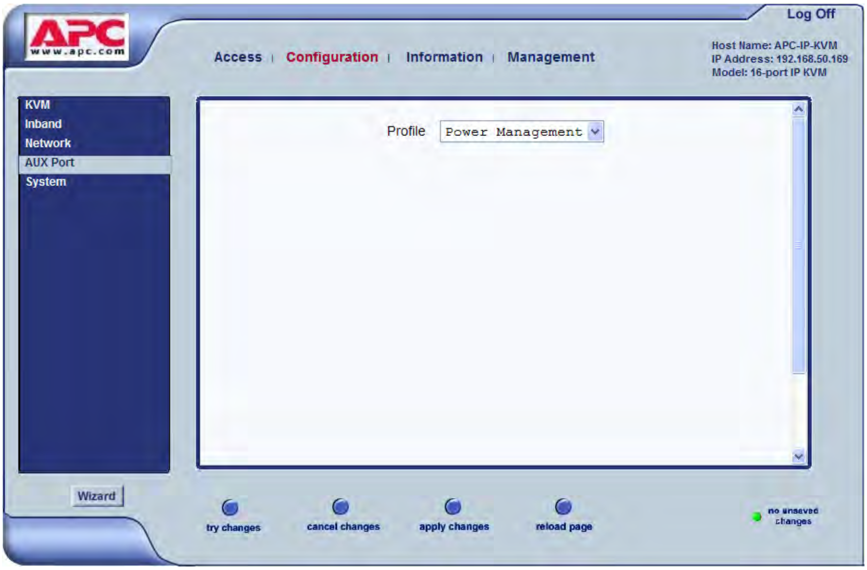
4. Click the Apply button to close the dialog box.

   The new or modified route appears in the list.

5. To delete a static route, select a route from the list and click Delete.
6. Click “apply changes.”

AUX Port

Selecting Configuration>AUX Port in Expert mode brings up the following form.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Profile: Power Management

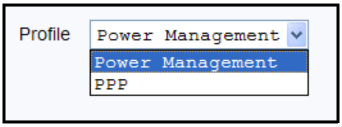
The AUX Port form is used to configure the AUX port for use with an APC rPDU or an external modem or an external modem.

▼ To Configure the AUX Port for Use With an rPDU or an External Modem

1. In Expert mode, go to: Configuration>AUX Port.

   The Aux Port form appears.

2. To configure the AUX port for Power Management, make sure that Power Management is selected in the Profile drop-down list.



Profile Power Management

3. Click "apply changes."

See "Power Management" on page 38 for background information on power management and lists of related tasks.

4. To configure the AUX port for an external modem, make sure that PPP is selected in the Profile field.

   Additional fields appear on the form.

5. Complete the fields as shown below.

Table 4-4: PPP Fields for Configuring the AUX Port

Field Name	Definition
Profile	Select the device to be connected. For **PPP**, the following input fields are used:
Baud Rate	The port speed.
Flow Control	Gateway or interface address used for the route.
Data Size	The number of data bits.
Parity	None, even or odd.
Stop Bits	The number of stop bits.

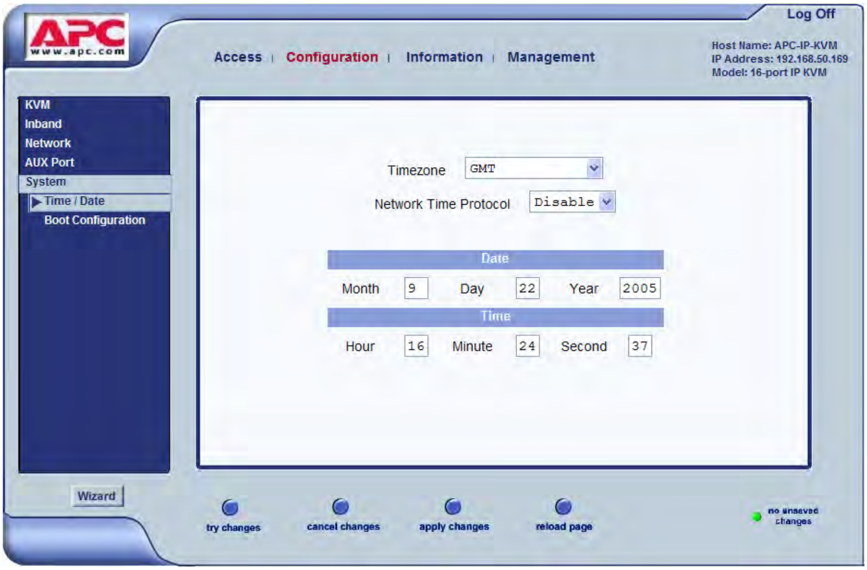
Table 4-4: PPP Fields for Configuring the AUX Port (Continued)

Field Name	Definition
Modem Initialization	The modem initialization string.
Local IP Address	The IP address of the 16-port IP KVM.
Remote IP Address	The remote IP address
Authentication Required	Select check box if authentication is required.
MTU/MRU	The maximum transmission unit / maximum receive units for the PPP.
PPP Options	The options for this protocol.

6. Click “apply changes.”

System

Selecting Configuration>System in Expert mode brings up the System form as shown in the following figure.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Timezone: GMT

Network Time Protocol: Disable

Date

Month 9 Day 22 Year 2005

Time

Hour 16 Minute 24 Second 37

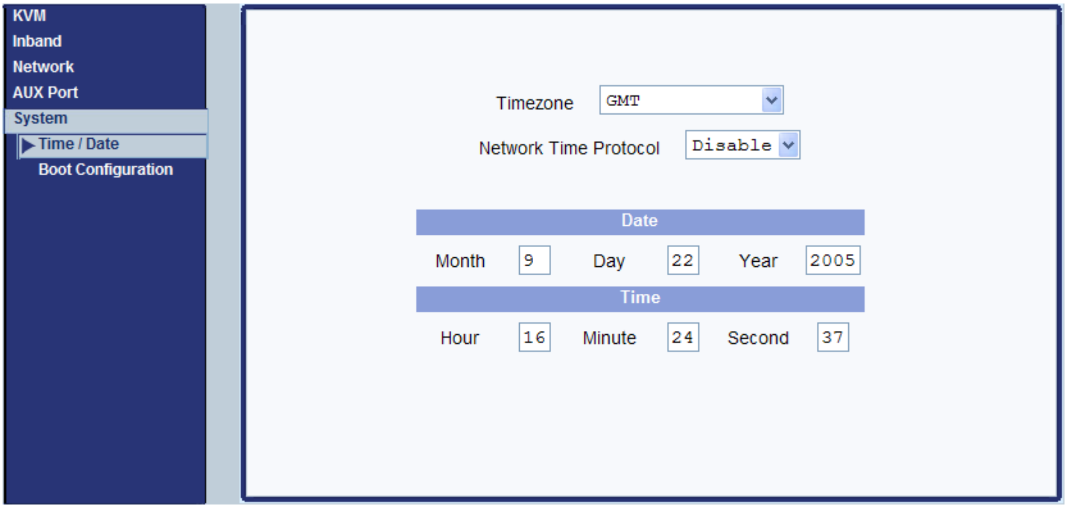
With the System form administrators can set the time and date on the 16-port IP KVM and reboot the 16-port IP KVM if necessary. The following procedures are available on the System form:

- “To Set the 16-port IP KVM’s Date and Time Manually” on page 222
- “To Set The Time and Date With NTP” on page 223
- “To Set the Time and Date to the 16-port IP KVM’s Local GMT” on page 223
- “To Configure 16-port IP KVM Boot” on page 226

Time/Date

With the Time/Date form, you have three options for setting the time and date of your 16-port IP KVM system:

- “To Set the 16-port IP KVM’s Date and Time Manually” on page 222
- “To Set The Time and Date With NTP” on page 223
- “To Set the Time and Date to the 16-port IP KVM’s Local GMT” on page 223



Timezone GMT

Network Time Protocol Disable

Date

Month 9 Day 22 Year 2005

Time

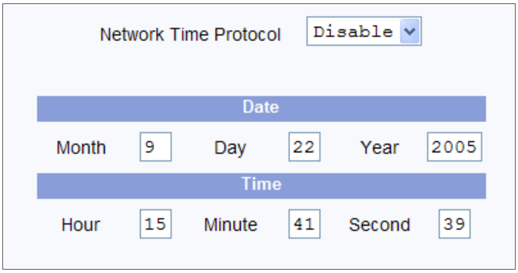
Hour 16 Minute 24 Second 37

▼ *To Set the 16-port IP KVM's Date and Time Manually*

1. In Expert Mode, go to: Configuration>System>Time/Date.

   The Date/Time form appears.

2. Make sure that Disabled is selected in the Network Time Protocol drop-down list.



Network Time Protocol Disable

Date

Month 9 Day 22 Year 2005

Time

Hour 15 Minute 41 Second 39

3. Fill in the date and time fields by selecting the appropriate numbers from the drop-down lists.

4. Click "apply changes."

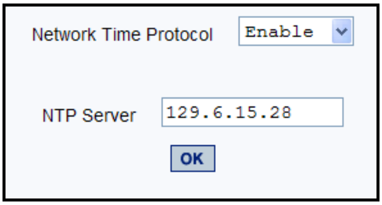
▼ *To Set The Time and Date With NTP*

1. In Expert Mode, go to: Configuration>System>Time/Date.

   The Date/Time form appears.

2. Choose Enable from the Network Time Protocol drop-down list.

   The NTP Server field appears.



Network Time Protocol: Enable

NTP Server: 129.6.15.28

3. Enter the address of the NTP server in the NTP Server field.

4. Click the “apply changes” button.

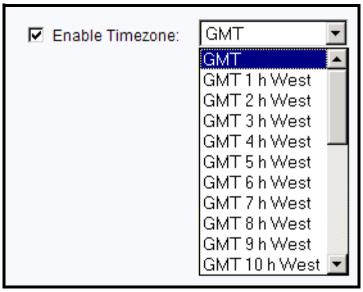
▼ *To Set the Time and Date to the 16-port IP KVM’s Local GMT*

1. Select Administration from the top menu bar.

2. Select Time/Date from the left menu panel.

   The Time/Date form appears.

3. Select the appropriate GMT from the Timezone drop-down list. Only official time zones are available.

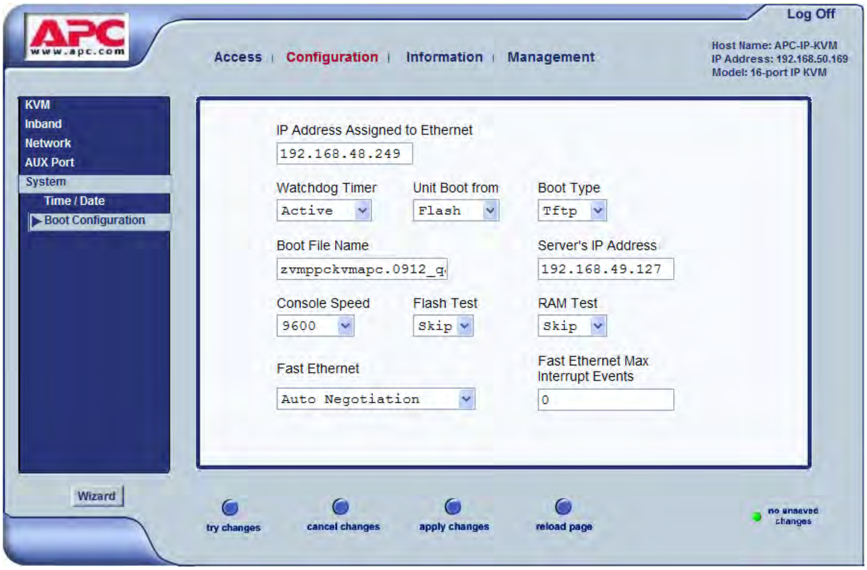


☑ Enable Timezone: GMT

4. Click “apply changes.”

Boot Configuration

Selecting Configuration>System>Boot Configuration brings up the following form.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

IP Address Assigned to Ethernet: 192.168.48.249

Watchdog Timer: Active

Unit Boot from: Flash

Boot Type: Tftp

Boot File Name: zvmppckvmapc.0912_q

Server's IP Address: 192.168.49.127

Console Speed: 9600

Flash Test: Skip

RAM Test: Skip

Fast Ethernet: Auto Negotiation

Fast Ethernet Max Interrupt Events: 0

On the Boot Configuration form, you can redefine the location from which the 16-port IP KVM boots.

By default, the 16-port IP KVM boots from a boot file in the on-board Flash memory.

You can select “Network” and configure a boot server to boot from the network instead, if desired.

A network boot has the following prerequisites:

- A TFTP or BOOTP server must be available to the 16-port IP KVM on the network.
- An upgraded 16-port IP KVM boot image file must be downloaded from APC and available on the boot server.
- The 16-port IP KVM must have a fixed IP address and you must know the address.
- You must know the boot filename and the IP address of the TFTP server.

These and other boot related options are described in the following table.

Table 4-5: Boot Configuration Fields and Options

Field or Value Name	Description
IP Address assigned to Ethernet	A new IP address for the 16-port IP KVM.
Watchdog Timer	Whether the watchdog timer is active. If the watchdog timer is active the 16-port IP KVM reboots if the software crashes. See “Boot Configuration” on page 224 for how the watchdog timer can be activated or deactivated.
Unit boot from	Choose “Flash” to boot from an image downloaded to the Flash or choose “Network” to perform a network boot.
Boot File Name	An alternative name for the boot file.
Server’s IP Address	An IP address for a boot server.
Console Speed	An alternative console speed from 4800 to 115200 (9600 is the default).
Fast Ethernet	The speed of the Ethernet connection: Auto Negotiation, 100 BaseT Half-Duplex, 100 BaseT Full-Duplex, 10 BaseT Half-Duplex, 10 BaseT Full-Duplex
Fast Ethernet Max Interrupt Events	An alternate number of maximum interrupt events to improve performance (0 is the default)

▼ *To Configure 16-port IP KVM Boot*

For more information about the fields in the “Boot Configuration” form, see Table 4-5 on page 225, if desired.

1. Go to Configuration>System>Boot Configuration in Expert mode.

   The Boot Configuration form appears.

2. Enter the IP address of the 16-port IP KVM in the “IP Address assigned to Ethernet” field.
3. Accept or change the selected option in the “Watchdog Timer” field.
4. Choose to boot either from “Flash” or “Network” from the “Unit boot from” menu.
5. Accept or change the filename of the boot program in the “Boot File Name” field.
6. If specifying network boot, do the following steps.
   a. Enter the IP address of the tftp server in the “Server’s IP Address” field.
   b. Select a console speed to match the speed of the tftp server from the “Console Speed” drop-down list.
   c. Choose an Ethernet speed from the “Fast Ethernet” drop-down list.
   d. Specify the maximum number of packets that the CPU handles before an interrupt in the “Fast Ethernet Max. Interrupt Events” field.
7. Click “apply changes.”

Viewing System Information

The Information menu provides three forms for viewing information about your 16-port IP KVM:

- General
- Port Status
- Read Sensor

General

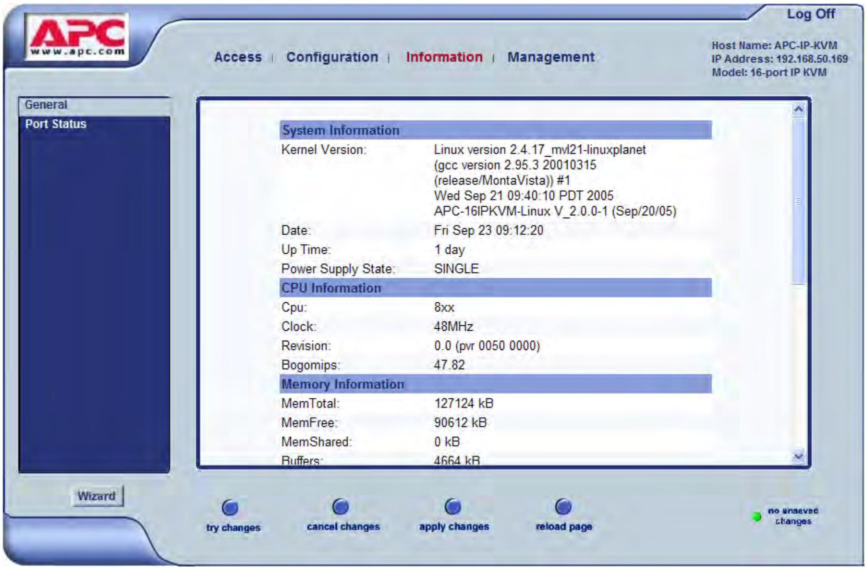
Use the General form to view system information in the following categories:

- System – Kernel version, date, uptime, power supply
- CPU – CPU, clock, revision, Bogomips
- Memory – Total, free, cached, active/inactive, and so on.
- Ram Disk Usage – 1k-blocks, used/available, percent used, and mounted
- Fan Status – Rotations per minute

▼ *To View General Information for Your 16-port IP KVM*

1. In Expert mode, go to: Information>General.

   The General information form appears.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

System Information	
Kernel Version:	Linux version 2.4.17_mvl21-linuxplanet (gcc version 2.95.3 20010315 (release/MontaVista)) #1 Wed Sep 21 09:40:10 PDT 2005 APC-16IPKVM-Linux V_2.0.0-1 (Sep/20/05)
Date:	Fri Sep 23 09:12:20
Up Time:	1 day
Power Supply State:	SINGLE
CPU Information	
Cpu:	8xx
Clock:	48MHz
Revision:	0.0 (pvr 0050 0000)
Bogomips:	47.82
Memory Information	
MemTotal:	127124 kB
MemFree:	90612 kB
MemShared:	0 kB
Buffers:	4664 kB

Port Status

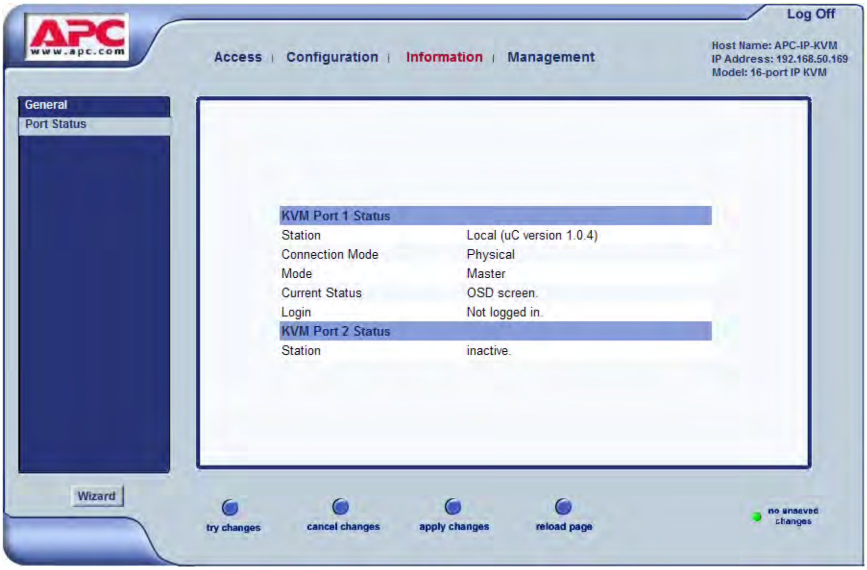
Use the Port Status form to view the system status of each KVM port on the 16-port IP KVM.

Note: Remote port status does not appear on the Port Status form unless one or more remote ports is configured in the system.

▼ To View Port Status

1. In Expert mode, go to: Information>Port Status.

   The Port Status form appears.



KVM Port 1 Status	
Station	Local (uC version 1.0.4)
Connection Mode	Physical
Mode	Master
Current Status	OSD screen.
Login	Not logged in.
KVM Port 2 Status	
Station	inactive.

The following table describes the information displayed for each port on the Port Status form.

Table 4-6: Port Status Information

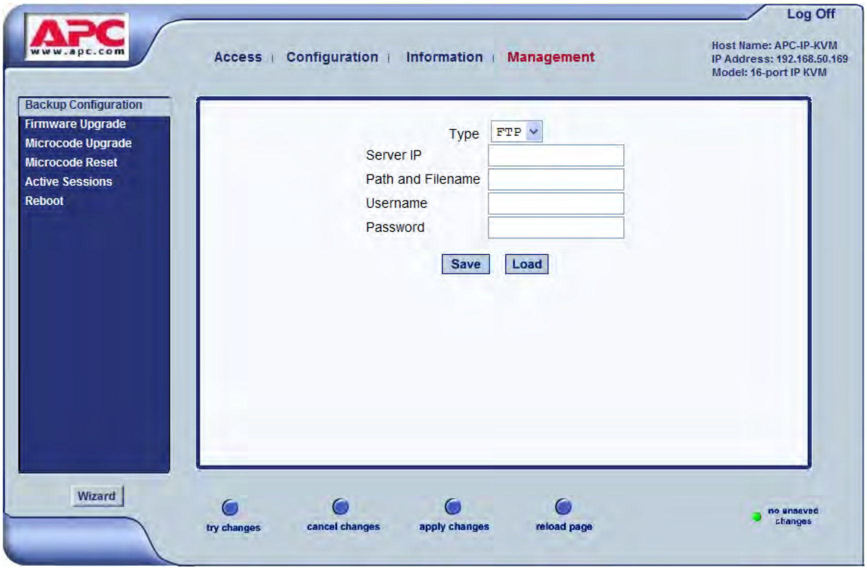
Field	Information
Station	Displays whether the station is Local, Remote, or Inactive and lists the microcontroller version used. This field also displays whether the 16-port IP KVM is a Master or Slave and lists the model number of the master 16-port IP KVM.
Connection mode	Displays whether the connection is **Network** or **Physical** or if the system is **Trying to connect** (if the cable is disconnected).
Current status	Displays the name of the current active page for that session.
Login	If a user is logged in, displays the user name and duration of the session in seconds.

Table 4-6: Port Status Information

Field	Information
Current server	When connected to a port, displays the server name.
Connection status	When connected to a port, displays the type of switch and version number used.
Current permissions	When connected to a port, displays the permissions the current user has on that port.
Cycle	When connected to a port and in Cycle Mode, this field displays the time in seconds that the system has been cycling.

Management

Selecting Management in Expert mode brings up the Management form as displayed in the following figure.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Type FTP
Server IP
Path and Filename
Username
Password

Administrators can use the management menu to perform system and software management such as booting, backing up, upgrading firmware, and handling configuration data.

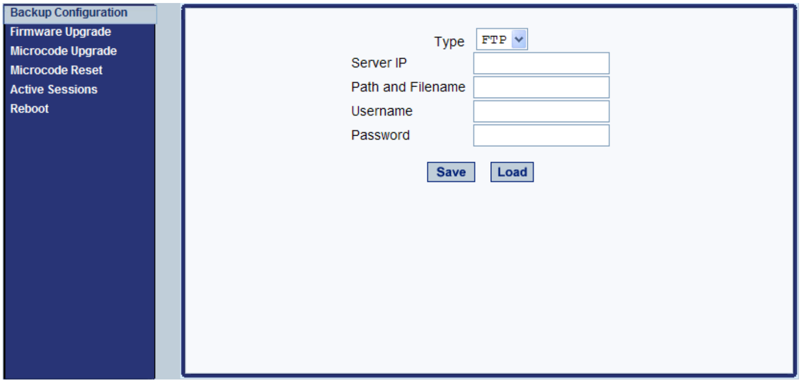
Menu Selection	Use this menu to:
Backup Configuration	Use a FTP server to save or retrieve your configuration data.
Firmware Upgrade	Upload firmware from the web to the 16-port IP KVM and save the new software version or update.
Microcode Upgrade	Update any of the microcontroller microcodes that are stored in the KVM Server Module, main 16-port IP KVM, local 16-port IP KVM, and internal 16-port IP KVM switch.
Microcode Reset	Reset any of the micro controller microcodes.
Active Sessions	View the status of all active sessions as well as reset or kill sessions.
Reboot	Reboot the system.

Backup Configuration

The Backup Configuration form allows you to set the 16-port IP KVM to use an FTP server to save and retrieve its configuration data.

For the backup configuration to work, the FTP server must be on the same subnet as the 16-port IP KVM. Ping the FTP server, to ensure that it is accessible from the 16-port IP KVM.

Selecting Management>Backup Configuration in Expert mode brings up the form shown in the following figure.



You can use the form to specify an FTP server for saving the 16-port IP KVM configuration, so you can retrieve the configuration if it is ever erased. You can also use the form for retrieving a copy of the backed up configuration file from the FTP server.

The FTP server must be on the same subnet. Ensure that it is accessible by pinging the FTP server.

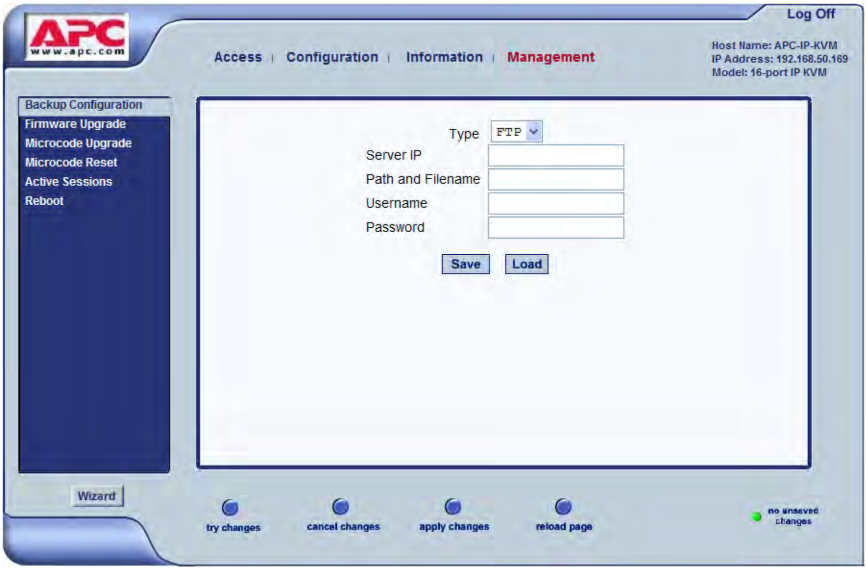
The following table describes the information you need to enter in the fields on the “Backup Configuration” form when FTP is selected from the “Type” drop-down list.

Field	**Definition**
Server IP	IP address of the FTP server
Path and Filename	Path of a directory on the FTP server where you have write access for saving the backup copy of the configuration file. Specify a filename if you want to save the file under another name. For example, to save the configuration file in a file whose name identifies its origin and date (such as `KVM8802config040406`) in a directory called “`upload`” on the FTP server, you would enter the following in the “Path and Filename” field: `upload/KVM8802config040406`.
User Name and Password	User Name for accessing FTP server (check with the FTP server’s administrator, if needed to obtain the user name and password to use),

▼ *To Back Up or Retrieve 16-port IP KVM Configuration Data*

1. In Expert mode, go to: Management>Backup Configuration.

The Backup Configuration form appears.

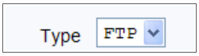


Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Type FTP

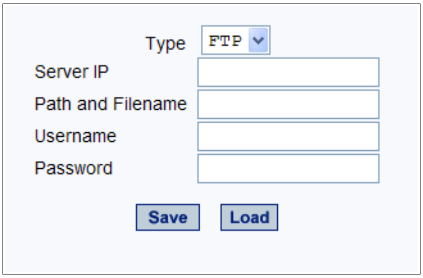
2. To save or retrieve data from an FTP server, do the following:

a. From the Type drop-down list, select FTP.



Type FTP

Selecting FTP (default) brings up the fields displayed in the following figure.



Type FTP

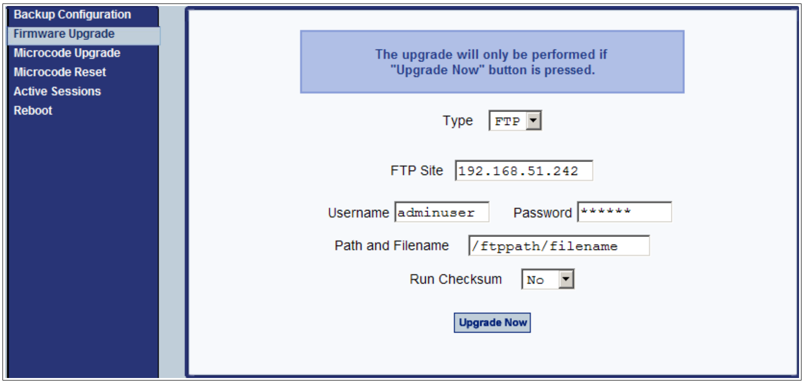
b. Fill in the following fields with appropriate connection information:

- Server IP
- Path and Filename
- User Name
- Password

3. Click Save to save the configuration to the selected location.
4. Click Load to load the configuration from the selected location.
5. Click “apply changes.”
6. To run the loaded configuration, reboot the 16-port IP KVM.

Firmware Upgrade

Selecting Management>Firmware Upgrade in Expert mode brings up the form shown in the following figure.



The upgrade will only be performed if "Upgrade Now" button is pressed.

Type FTP

FTP Site 192.168.51.242

Username adminuser Password ******

Path and Filename /ftppath/filename

Run Checksum No

The following table defines the information you need to supply on the form.

Field/Menu Name	Definition
Type	FTP is the only supported type.
FTP Site	The address of the FTP server where the code is located. You can use any FTP server if you download the firmware on it first. The APC download site is: `http://www.apc.com/tools/download/`. If desired, see “To Upgrade Firmware” on page 236 for instructions on how to download the firmware for installation on your own local FTP server.
User Name	User Name recognized by the FTP server.
Password	Password associated with the User Name.
Path and FIle Name	The pathname of the software on an accessible FTP server.

The following table has links to the related procedures.

To Download Firmware/microcode from the APC Web Site	Page 236
To Upgrade Firmware	Page 236
To Upgrade Microcode From an FTP Server	Page 238

▼ *To Download Firmware/microcode from the APC Web Site*

1. In a web browser, go to `http://www.apc.com/tools/download/`.
2. Use the “Filter by Software/Firmware” drop-down list or the “Filter by Hardware” drop-down list to find the firmware/microcode for the 16-port IP KVM.
3. If prompted, enter a username and password or create a new APC account.
4. Use the “Continue” buttons to locate the desired updates.
5. Download the file to an FTP server that is accessible to the 16-port IP KVM.
6. See “To Upgrade Firmware” on page 236 for instructions on using the 16-port IP KVM Web Manager to upgrade firmware.

▼ *To Upgrade Firmware*

This procedure assumes that you have downloaded the appropriate firmware upgrade files from the APC web site and loaded them onto an FTP server that is accessible to the 16-port IP KVM. See “To Download Firmware/microcode from the APC Web Site” on page 236 for instructions if needed.

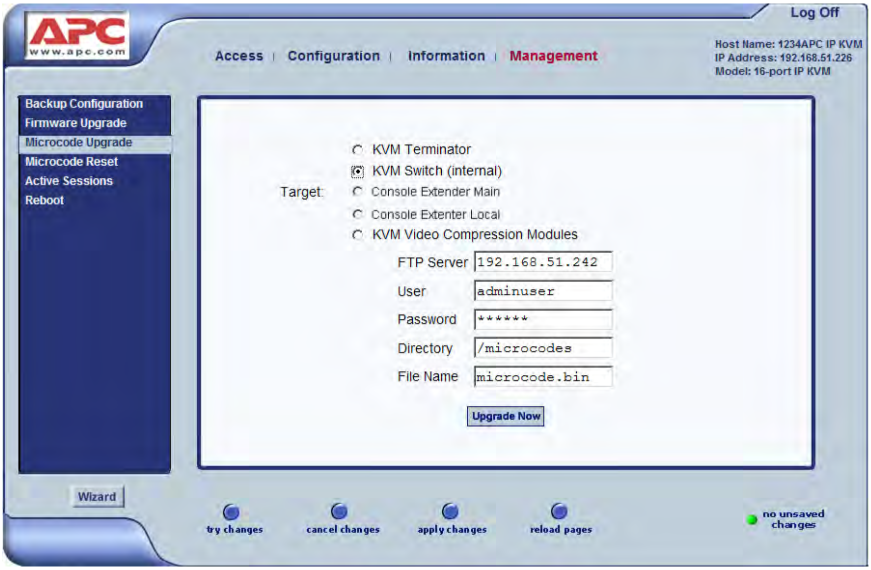
1. In the Web Manager, go to Management>Firmware Upgrade in Expert mode.

   The Firmware Update form appears.
2. Choose FTP from the Type menu.
3. Enter the name of the FTP server in the “FTP Site” field.

4. Enter the user name recognized by the FTP server in the “User Name” field.
5. Enter the password associated with the user name on the FTP server in the “Password” field.
6. Enter the pathname of the file on the FTP server in the “Path and Filename” field.
7. Press the “Upgrade Now” button.
8. Click “apply changes.”

Microcode Upgrade

Selecting Management>Microcode Upgrade in Expert mode bring sup the following form.



Host Name: 1234APC IP KVM
IP Address: 192.168.51.226
Model: 16-port IP KVM

Target:
○ KVM Terminator
● KVM Switch (internal)
○ Console Extender Main
○ Console Extenter Local
○ KVM Video Compression Modules

FTP Server: 192.168.51.242
User: adminuser
Password: ******
Directory: /microcodes
File Name: microcode.bin

You can specify a local FTP server where you have previously downloaded the microcode. See “To Download Firmware/microcode from the APC Web Site” on page 236 for instructions if needed.

You need to enter the actual pathname components in the “Directory” and “File Name” fields.

The following table defines the information you need to supply on the form.

Field Name	Definition
Target	The name of the component whose microcode you wish to upgrade.
FTP Server	The address of the FTP server where the microcode is located. You can use any FTP server if you download the firmware on it first.
User Name	User Name recognized by the FTP server.
Password	Password associated with the User Name.
Directory	The pathname where the microcode resides on the FTP server.
File Name	The file name of the microcode for the “Target.”

▼ *To Upgrade Microcode From an FTP Server*

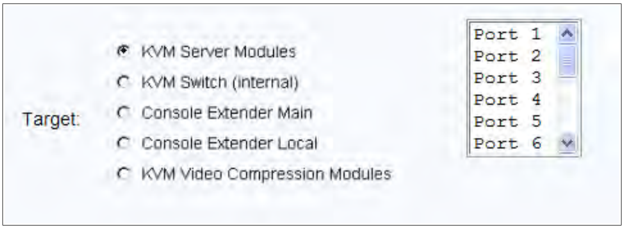
This procedure assumes that you have downloaded the appropriate microcode upgrade files from the APC web site and loaded them onto an FTP server that is accessible to the 16-port IP KVM. See “To Download Firmware/microcode from the APC Web Site” on page 236 for instructions if needed.

1. Go to Management>Microcode Upgrade in Expert mode.

   The Microcode form appears.

2. Click the radio button next to the “Target” whose microcode you want to update.

   If you select the KVM Server Modules radio button, a scrollable port list appears next to the Target list.



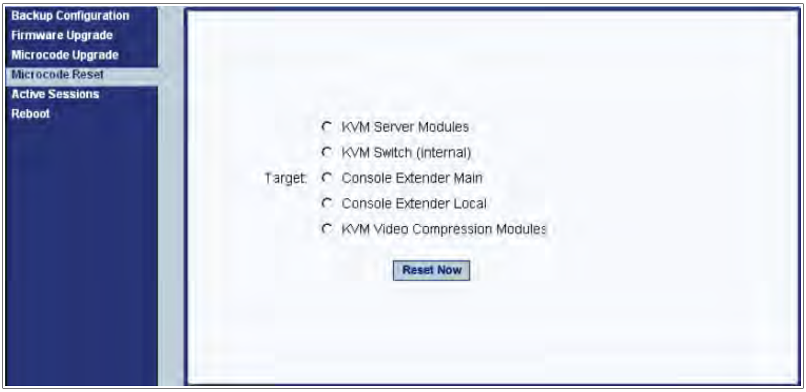
Target:
● KVM Server Modules
○ KVM Switch (internal)
○ Console Extender Main
○ Console Extender Local
○ KVM Video Compression Modules

Port 1
Port 2
Port 3
Port 4
Port 5
Port 6

3. To download microcode for a KVM Server Module, select a port from the scrollable port list.
4. Enter the IP address or name of the FTP server in the “FTP Server” field.
5. Enter the user name recognized by the FTP server in the “User” field.
6. Enter the password associated with the user name on the FTP server in the “Password” field.
7. Enter the pathname to the directory where the microcode resides on the FTP server. in the “Directory” field.
8. Enter the name of the microcode file in the “File Name” field.
9. Click the “Upgrade Now” button.
10. Click “apply changes.”
11. Go to “To Reset the Microcode After Upgrade” on page 239.

Microcode Reset

Selecting Management>Microcode Reset in Expert mode brings up the form shown in the following figure.



Target: ○ KVM Server Modules
○ KVM Switch (internal)
○ Console Extender Main
○ Console Extender Local
○ KVM Video Compression Modules

You can use the form to reset the microcode after an upgrade.

▼ To Reset the Microcode After Upgrade

Perform this procedure if you have upgraded microcode as described in “To Upgrade Microcode From an FTP Server” on page 238.

1. From the top menu, select Management; from the side menu, select Microcode Reset.

   The Microcode Reset form appears.

2. To reset the microcode in a KVM Server Module, do the following steps.

   a. Click the KVM Server Module radio button.

      A scrollable list of KVM ports appears.

   b. Select the port to which the KVM Server Module is connected from the port list.

3. To reset another type of microcode, select the radio button next to the target you want to upgrade, either “KVM Switch (internal),” or “KVM Video Compression Modules.”

4. Press the “Reset Now” button.

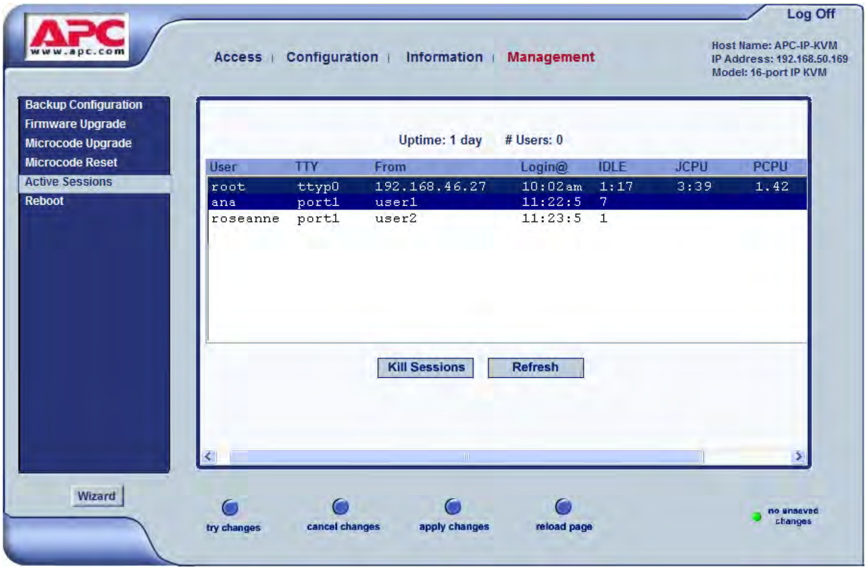
Active Sessions

The Active Sessions form is designed to provide you quick status and usage information pertaining to all active server sessions. Administrators may also kill sessions from this form.

▼ To View Active Sessions Information

1. In Expert mode, go to Management>Active Sessions.

   The Active Sessions window appears.



Host Name: APC-IP-KVM
IP Address: 192.168.50.169
Model: 16-port IP KVM

Uptime: 1 day # Users: 0

User	TTY	From	Login@	IDLE	JCPU	PCPU
root	ttyp0	192.168.46.27	10:02am	1:17	3:39	1.42
ana	port1	user1	11:22:5	7		
roseanne	port1	user2	11:23:5	1		

2. Review the session information as described in the following table.

Column	Definition
Uptime	Time the 16-port IP KVM has been on in minutes and seconds (mm:ss).
# Users	Number of users connected to server.
User	The user who initiated the session.

Column	Definition
TTY	The name of the KVM port.
From	The network machine to which the port is connected.
Login@	The day and time of the last login.
Idle	The time when the session or server became inactive.
JCPU	The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.
PCPU	The time used by the current process that is named in the What column.
What	The current process attached to the tty.

3. Select the Refresh button to update the form with current information.

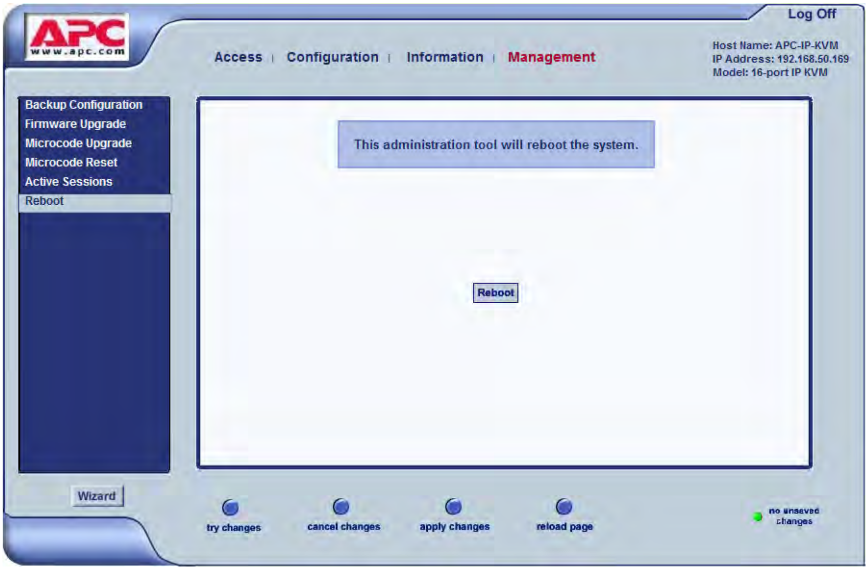
▼ *To Kill an Active Session*

1. In Expert mode, go to Management>Active Sessions.

   The Active Sessions window appears.
2. Select the sessions you wish to kill.
3. Click Kill Session.
4. Click “apply changes.”

Reboot

Selecting Management>Reboot in Expert mode, brings up the following form.

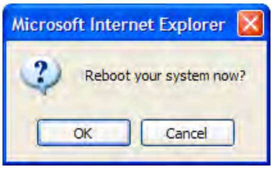


This administration tool will reboot the system.

Selecting the Reboot button allows you to reboot the system without physically turning off the hardware.

▼ To Reboot the 16-port IP KVM From a Remote Location

1. In Expert mode, go to: Management>Reboot
2. Click the Reboot button.
3. A confirmation page appears.



Reboot your system now?

4. Click OK to reboot the system.

Chapter 5
Web Manager for Regular Users

With the 16-port IP KVM Web Manager, regular users can connect to PCs with USB or PS/2 connectors or Sun servers with USB connectors through out-of-band, KVM connections and manage power of devices connected to APC rPDUs from anywhere on a network. Regular users can also connect to Windows Terminal Servers through in-band connections.

For more information on in-band and out-of-band connections see “Server Access: In-band and Out of Band” on page 28.

For more information on power management, see “Power Management for Regular Users” on page 250.

For procedures on how to operate the 16-port IP KVM as an administrator, see Chapter 4: Web Manager for Administrators.

Web Manager for Regular Users

When users without administrative privileges log on to the 16-port IP KVM, the Web Manager appears with three menu options:

- Connect to Server – Form used to connect to servers with either an in-band or a KVM connection.

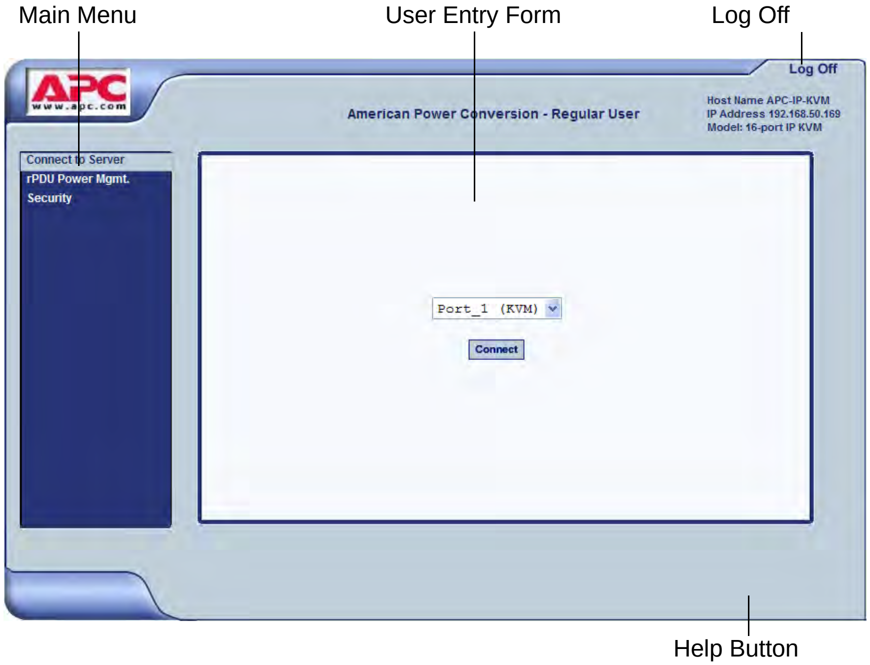
  See “Connecting to Servers Remotely Through the Web Manager” on page 266.
- rPDU Power Management – Form used to control the power of devices plugged in to APC rPDUs.

  See “Power Management for Regular Users” on page 250.
- Security – Form used to change your password.

  See “Changing Your 16-port IP KVM Password” on page 251.

The rPDU Power Management and Security forms can be accessed by clicking the corresponding menu items.

The Web Manager interface provides you with a static main menu and a user entry form as displayed in Figure 5-1. The content of the user entry form changes based on your menu selection.



American Power Conversion - Regular User

Host Name APC-IP-KVM
IP Address 192.168.50.169
Model: 16-port IP KVM

Figure 5-1:APC 16-port IP KVM Web Manager

Prerequisites for Logging in to the Web Manager

You must collect the following information from your 16-port IP KVM administrator before accessing and logging into the 16-port IP KVM:

- 16-port IP KVM IP address
- User Name
- Password

See the “Prerequisites for Accessing Servers With KVM Connections” on page 258 for prerequisites for accessing servers.

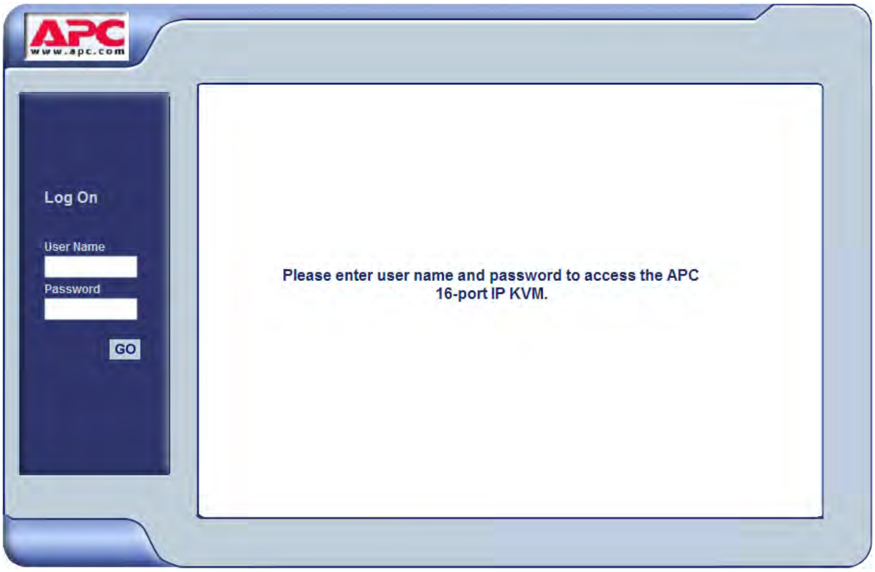
See the following sections for prerequisites for accessing servers with KVM and in-band connections:

- "Prerequisites for Accessing Servers With In-band Connections" on page 258
- "Prerequisites for Accessing Servers With KVM Connections" on page 258

▼ *To Log Onto the 16-port IP KVM Web Manager as a Regular User*

1. Launch a supported browser and type the 16-port IP KVM IP address (for example http://10.0.0.1/) into the browser's URL field.

   The APC 16-port IP KVM log on screen appears.

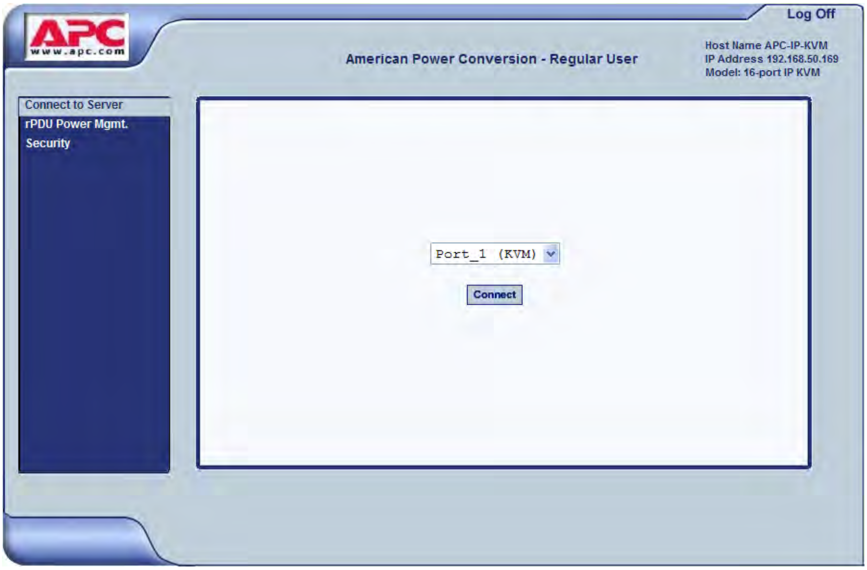


Please enter user name and password to access the APC 16-port IP KVM.

2. Enter your user name and password as provided to you by your 16-port IP KVM administrator

3. Click Go.

   The Connect form appears.



See “Web Manager for Regular Users” on page 246 for an introduction to using the Web Manager and links to more detailed information.

Power Management for Regular Users

The 16-port IP KVM offers two modes of controlling power:

- Power control of any device plugged into a rPDU that is configured on the 16-port IP KVM.

  See “Power Control of Any Device Plugged Into an APC rPDU on the 16-port IP KVM” on page 250.
- Power control of a server while connected to that server through a KVM port.

  See “Controlling Power of a KVM-connected Server” on page 279.

Power Control of Any Device Plugged Into an APC rPDU on the 16-port IP KVM

Depending on your access rights, the 16-port IP KVM allows you to remotely view and manage connected rPDU to the 16-port IP KVM. Regular users can go to the rPDU Power Management menu on the Web Manager and use the Outlets Manager and the View rPDU Info forms to manage and view the status of rPDU and the devices plugged into them. The following table lists the power management tasks available to regular users through the Web Manager and links to the associated procedures.

Table 5-1: Power Management Tasks Available to Regular Users

Task	Where Documented
Switch on/off; reboot network devices.	• “Outlets Manager” on page 124 • “To Turn On, Turn Off, or Power Cycle Outlets” on page 125
View rPDU information by ports and slaves.	• “View rPDU Info” on page 127 • “To Turn On, Turn Off, or Power Cycle Outlets” on page 125
Switch on/off outlets; reboot servers connected to KVM ports.	“To Power On, Power Off, or Reboot the Connected Server” on page 280

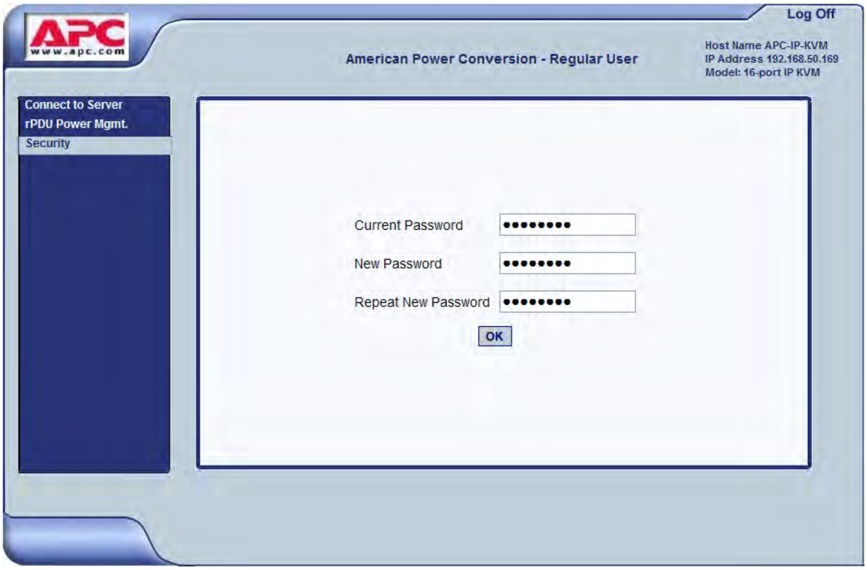
Changing Your 16-port IP KVM Password

On the Security form on the 16-port IP KVM Web Manager, you can change your old password to a new password.

▼ *To Change Your 16-port IP KVM Password*

1. Log in to the Web Manager.
2. Select Security in the Main Menu.

   The Security Form appears.



Current Password •••••••••

New Password •••••••••

Repeat New Password •••••••••

3. Type your current password in the Current Password field.
4. Type your new password in the New Password field and again in the Repeat New Password field.
5. Click OK.

Chapter 6

Accessing Connected Devices

With the 16-port CAT5 KVM, users and administrators can connect to any PC or USB Sun servers through out-of-band, KVM connections and manage power of devices connected to APC rPDUs from anywhere on a network with the Web Manager or locally with the OSD. Users and administrators can also connect to Windows Terminal Servers through in-band connections. .

This chapter gives an overview of the options for accessing servers that are connected to ports on the 16-port CAT5 KVM.

The following table lists the procedures in this chapter.

To Close a KVM Connection	Page 280
To Power On, Power Off, or Cycle Devices Plugged into rPDU Outlets	Page 288
To Configure a PPP Connection on a Remote Computer	Page 291
To Make a PPP Connection From a Remote Computer	Page 292

Who Can Access Connected Devices

Authorized users have the permissions they need to access one or more servers or other devices that are connected to ports on the 16-port CAT5 KVM. See “Types of Users” on page 14 and “Port Permissions” on page 23 for more information.

Authorized users and 16-port CAT5 KVM administrators have the following options for accessing connected devices:

- Use the Web Manager for most connections to devices.

  See “APC Web Manager” on page 19 and “Prerequisites for Using the Web Manager” on page 19 for background information about the Web Manager, if needed.

  See “Connecting to Servers Remotely Through the Web Manager” on page 266 for instructions on how to log on to the Web Manager and connect to devices.
- Use the on-screen display (OSD) to access devices that are connected to the 16-port CAT5 KVM’s KVM ports.

  Local users and administrators who have access to a directly connected Local User station can use the OSD Connect menu.

  Chapter 7: “On Screen Display” describes how to access connected devices through the OSD.
- Dial into the 16-port CAT5 KVM through a modem

  See “Modem Connections” on page 290.

Server Connections: What You See

Once connected to a server, one or two windows appear depending on the type of server connection being made:

- KVM connections
  - Remote Viewer is launched with the same interface as if you were directly logging into the connected server.
  - The Access Window with an interface for managing up to four server connections.

  See “Viewing KVM Connections” on page 256.
- In-band connections

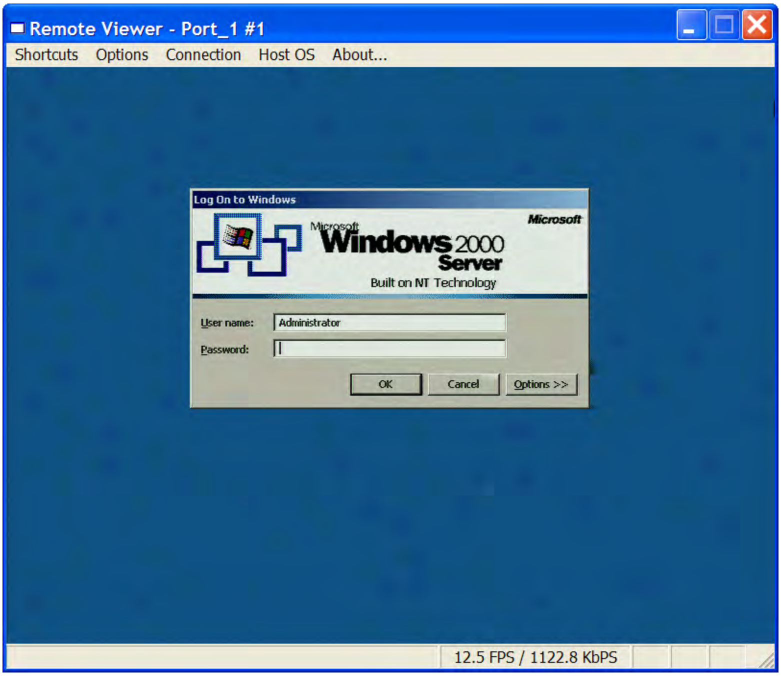
  An ActiveX viewer is launched with the same interface as if you were directly logging into the connected server.

  See “Viewing In-band Connections” on page 257.

Viewing KVM Connections

The Remote Viewer is the interface you use to manage servers over KVM over IP connections. Logins persist across connection sessions. If you close a connection without logging out, you are still logged in the next time you connect, unless the system has closed your session. If you are not currently logged in, you see a login screen or prompt.

The connected servers's login prompt appears. The following example shows a login prompt for a Windows 2000 server displayed by the Remote Viewer. If you are connected to a Linux server without a graphical display, you see a "Login:" prompt.



User name: Administrator

Password:

Figure 6-1: Remote Viewer for KVM Connections

See “Remote Viewer Settings” on page 283 for more detailed information about using the Remote Viewer.

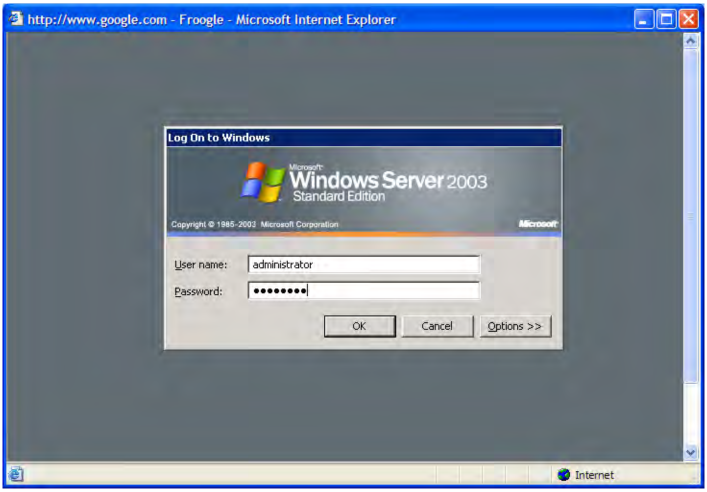
Local KVM connections through the OSD do not use the Remote Viewer. Instead, the view of the connected server takes up the entire screen of local work station. See “Controlling KVM Port Connections” on page 272 for more information on local KVM connections.

Viewing In-band Connections

The ActiveX viewer is the interface you use to manage servers over an in-band connection.

Note: Internet Explorer and Netscape 8 support ActiveX viewer. If you are using Netscape 8 make surer to select Internet Explorer rendering engine and enable the ActiveX option.

The following graphic displays the login screen of a server running Windows 2003 in the ActiveX viewer for in-band connections.



http://www.google.com - Froogle - Microsoft Internet Explorer

Log On to Windows

User name: administrator

Password: ●●●●●●●●●

Figure 6-2: ActiveX Viewer for In-band Connections

Prerequisites for Accessing Servers With In-band Connections

A 16-port CAT5 KVM user who needs to access any RDP server must have the following:

- The username and password of a valid account on the RDP server.
- Internet access and Microsoft Internet Explorer on a remote Windows client machine.

Prerequisites for Accessing Servers With KVM Connections

The following prerequisites must be met before you can access a KVM-connected server:

- Know the KVM Port(s) to which you have access (especially if direct access to a port is configured)
- Have the user name and password of a valid account on the connected server
- If you are connecting through the Web Manager, have the following:
  - A remote computer running a Windows operating system with Internet access and a supported browser installed
  - The IP address of the 16-port CAT5 KVM
- If you are making a local connection, have a direct connection made to the User 1 or User 2 ports of the KVM

Web Manager Login Screen

The following table list the sections that describe the three different possible views of the Web Manager login screen that can appear under various conditions.

Table 6-1: Web Manager Login Screen Options

Conditions	**Where Documented**
Direct logins to KVM ports not enabled: • You enter the 16-port CAT5 KVM's IP address in a browser to bring up the Web Manager login screen. • You can log on to the Web Manager and perform administration. • If you want to access a server connected to a KVM port after logging into the Web Manager, you can connect to the KVM port from the Connect to Server form.	"Login Screen: Direct Logins Not Enabled" on page 261
Direct logins to KVM ports enabled (option 1): • You enter the 16-port CAT5 KVM's IP address in a browser to bring up the Web Manager login screen. • You enter your username and password and the desired KVM port number on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first.	"Login Screen: Direct Logins Enabled, Only IP Address Entered" on page 263

Table 6-1: Web Manager Login Screen Options (Continued)

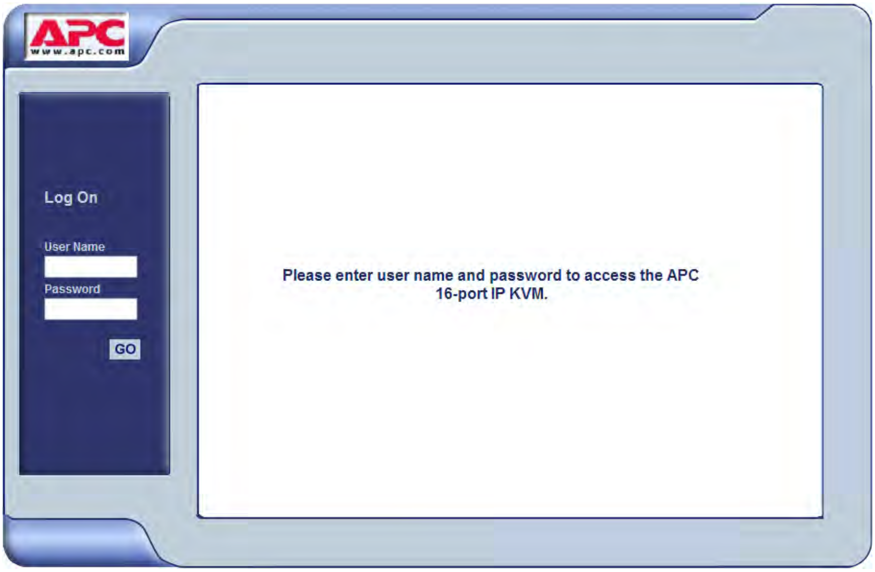
Conditions	Where Documented
Direct logins to KVM ports enabled (option 2): • You enter the 16-port CAT5 KVM's IP address along with the port name in a browser to bring up the Web Manager login screen. • The port field is already filled in when the Web Manager appears. • You save the URL that includes the port in a favorites file to save time when logging into the same port in the future. • You enter your username and password on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first, as in the previous row.	"Login Screen: Direct Logins Enabled, IP Address and Port Entered" on page 264

Note: The direct access method allows users to access servers that are connected to KVM ports only or servers that are connected to KVM ports and are available for in-band access as well. This method is particularly useful for users who may need direct KVM access to a server that has both KVM and in-band access enabled.

Login Screen: Direct Logins Not Enabled

The following screen shows an example of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the 16-port CAT5 KVM is entered in the browser.
- Direct logins to KVM ports is not enabled.



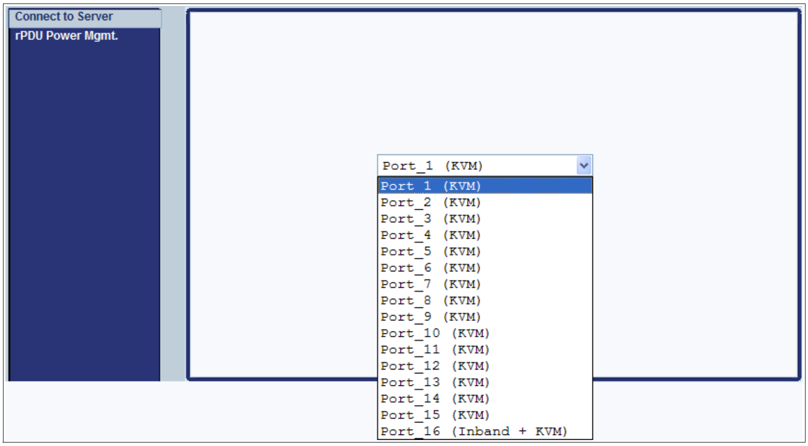
Please enter user name and password to access the APC 16-port IP KVM.

Figure 6-3: Web Manager Login Screen Without KVM Direct Logins Enabled

As shown in Figure 6-3, the Web Manager login screen displays two fields in the “Login” section: “username” and “password.” The product name appears in the “Welcome” line, and the model and the administrator-specified hostname are listed.

Connect to Server Drop-down List

With the connect to server drop-down list, you can select the in-band or KVM server you want to connect to.



```
Port_1 (KVM)
Port_1 (KVM)
Port_2 (KVM)
Port_3 (KVM)
Port_4 (KVM)
Port_5 (KVM)
Port_6 (KVM)
Port_7 (KVM)
Port_8 (KVM)
Port_9 (KVM)
Port_10 (KVM)
Port_11 (KVM)
Port_12 (KVM)
Port_13 (KVM)
Port_14 (KVM)
Port_15 (KVM)
Port_16 (Inband + KVM)
```

Figure 6-4: Connect To Server Drop-down List

The following sections can help you to identify whether a server has an in-band connection, KVM connection, or both and whether it is connected to a cascaded KVM device.

Servers and Connection Types in the Connect to Server Drop-down List

There are two levels of identifying servers in the Connect to Server drop-down list:

- Connection Type – The types of connections that can be made to each server is displayed in parenthesis at the end of each server entry in the list. An entry with “(KVM)” at the end of it can be accessed with a KVM connection only. An entry with “(Inband)” at the end of it can be accessed with an in-band connection only. An entry with “KVM + Inband”) can be accessed with both connection methods. See “Determining the Connection Type and its Supported Functionality” on page 30 for more detailed information.
- Server Name or Port Name/Number – The type of connection determines the type of name applied:

- Individual KVM ports are either labelled by the port number in the form Port_# or by an administrator-defined alias, which should describe the type of computer connected to the port or be the actual name of the connected server.
- Individual in-band connections are labelled by an administrator-defined server name, which should identify the type of computer being accessed or be the actual name of the server.

Note: A server that is configured for both in-band and KVM connections can have two different aliases configured: one for the KVM port and one for the in-band connection. In this case, the alias that appears in the Connect to Server drop-down list is the alias assigned to the KVM port.

Port Numbers of Cascaded KVM Devices in the Connect to Server Drop-down List

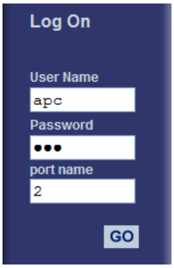
In the Connect to Server drop-down list on the Connect to Server form, a name and a number connected by a period (.) indicate the alias or name of the cascaded KVM unit followed by its physical port.

For example, in the port name kvm2.4, kvm2 is the name of the cascaded device, and 4 is the physical port on the device named kvm2.

Login Screen: Direct Logins Enabled, Only IP Address Entered

The following screen shows an example of the format of the Login portion of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the 16-port CAT5 KVM is entered in a browser.
- Direct logins to KVM ports is enabled.



Log On

User Name: apc

Password: •••

port name: 2

Login Screen: Direct Logins Enabled, IP Address and Port Entered

This section describes how the Web Manager login screen appears if the following two conditions are true:

- Direct logins to KVM ports is enabled,
- The IP address of the 16-port CAT5 KVM is entered along with a port ID (in the required format) in a browser

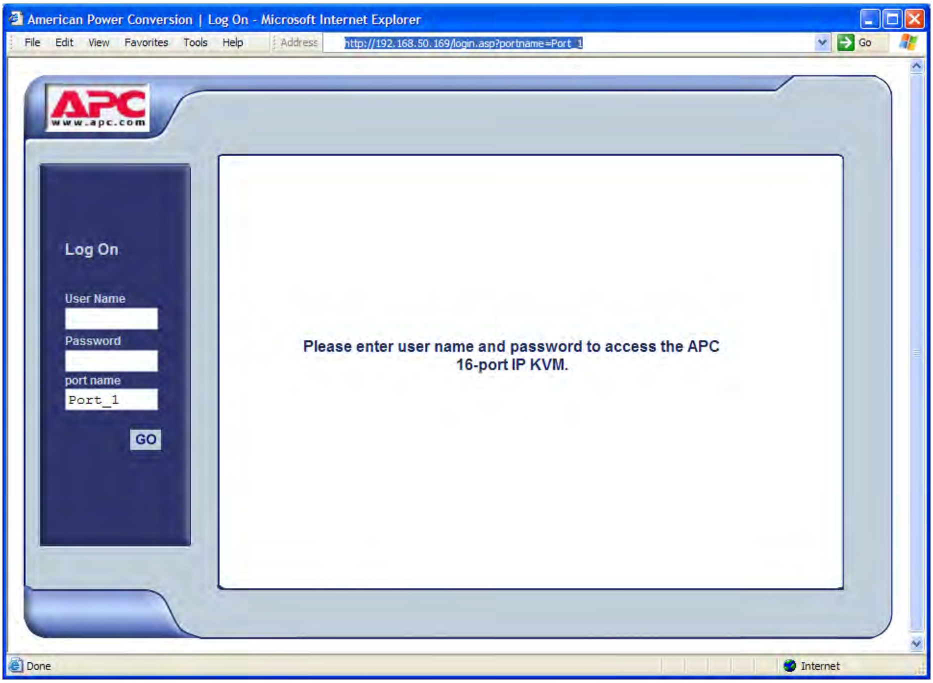
The required format is:

```
IP_address/login.asp?portname=portnumber
```

where *`IP_address`* is the IP address of the 16-port CAT5 KVM and *`portnumber`* is the portnumber or alias assigned to the KVM port.

Entering the port number along with the IP address makes it possible to connect directly to a KVM port without going to the Web Manager's Access page first. You can save the URL as a bookmark or in your browser's favorites list and go directly to the port login later without typing in the entire URL. The "port" field is filled in with the port number when the Web Manager login window appears.

The example in the following figure shows `http://192.168.46.169/login.asp?portname=Port_1` entered in the Address field of a Microsoft Internet Explorer browser. The login screen displays empty "username" and "password" fields and a port field filled with the name of the port from the URL, in this case "Port_1."



http://192.168.50.169/login.asp?portname=Port_1

Log On

User Name

Password

port name Port_1

GO

Please enter user name and password to access the APC 16-port IP KVM.

Figure 6-5: Example: Web Manager with Direct Logins Enabled, IP Address and Port Entered

Connecting to Servers Remotely Through the Web Manager

16-port CAT5 KVM administrators who are logging into the Web Manager to perform 16-port CAT5 KVM configuration can use any modern browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla, or Firefox).

See “Web Manager Login Screen” on page 259 for a description of the ways authorized users can connect to servers from the Web Manager.

See the following procedures for connecting to servers:

To Connect to a KVM Port Through the Web Manager Login Screen	Page 268
To Connect to Servers Through The Web Manager’s Connect To Server Form	Page 266

If needed, see one of the following login procedures.

To Log On to the Web Manager as Admin	Page 106
To Log Onto the 16-port IP KVM Web Manager as a Regular User	Page 248

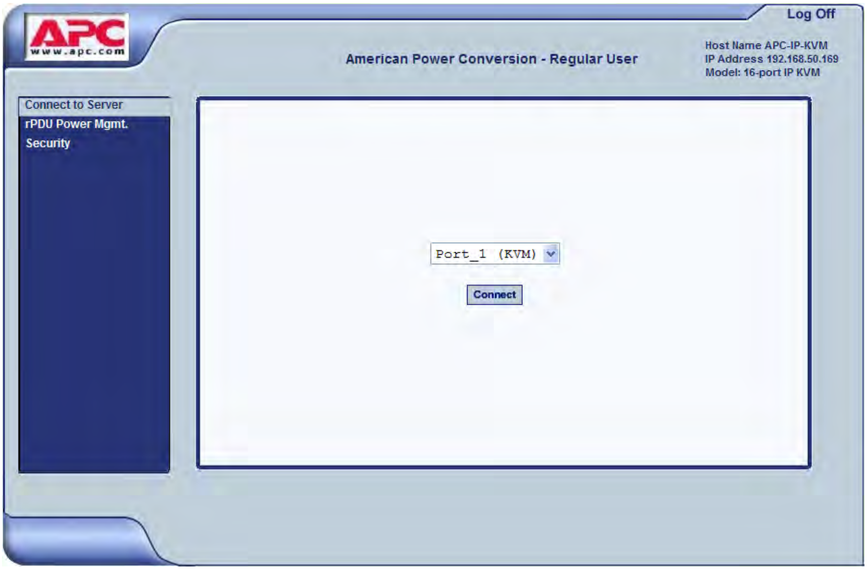
▼ *To Connect to Servers Through The Web Manager’s Connect To Server Form*

1. Log in to the 16-port CAT5 KVM using your username and password.

   See “To Log Onto the 16-port IP KVM Web Manager as a Regular User” on page 248 or “To Log On to the Web Manager as Admin” on page 106 for detailed instructions on logging in to the Web Manager.

2. From the left menu panel, select Connect to Server.

   The Port Connection form appears.



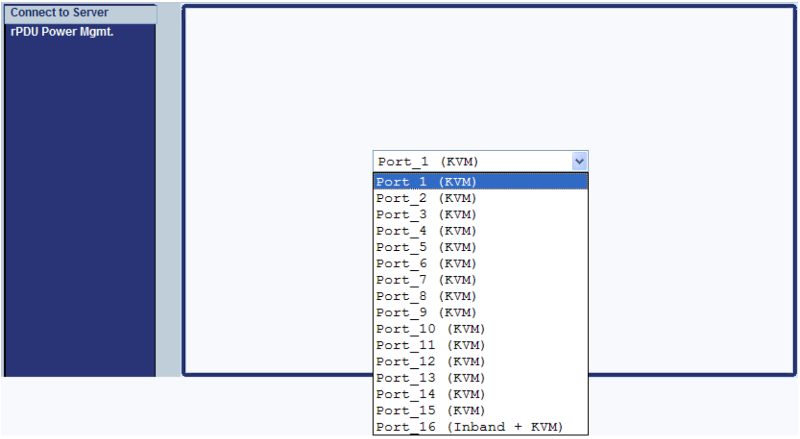
American Power Conversion - Regular User

Host Name APC-IP-KVM
IP Address 192.168.50.169
Model: 16-port IP KVM

Port_1 (KVM)

3. From the drop-down menu, select the server or port to which you want to connect.

   A list similar to the list in the following graphic appears.



Port_1 (KVM)

See “Determining the Connection Type and its Supported Functionality” on page 30 for a description of each type of connection method and what happens once connected.

4. Click on the Connect button.

The system may launch one or two browser windows: the Remote Viewer and the Access Window for KVM connections, or an ActiveX viewer for RDP connections. See “Server Connections: What You See” on page 255 for a description of each window.

Note: The first time the system invokes the Remote Viewer, it prompts you to accept a security certificate. Click Accept.

▼ *To Connect to a KVM Port Through the Web Manager Login Screen*

This procedure assumes that the 16-port CAT5 KVM administrator has enabled direct logins to KVM ports.

1. Enter the IP address of the 16-port CAT5 KVM alone or the IP address of the 16-port CAT5 KVM followed by the KVM port number (in the required format) in the address field of a browser.

The required format for entering a KVM port number in the URL is:

```
IP_address/login.asp?portname=portnumber
```

where *IP_address* is the IP address of the 16-port CAT5 KVM and *portnumber* is the portnumber or alias assigned to the KVM port.

Note: Check with the administrator who configured the basic network parameters on the 16-port CAT5 KVM, for help finding the IP address and the “apc” password, if needed. Also if needed, see an example of the proper format for entering the port number in “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 264.

- If DHCP is not enabled, use a fixed IP address assigned by the network administrator to the 16-port CAT5 KVM.
- If DHCP is enabled, enter the dynamically assigned IP address.

The Web Manager login screen appears. If you entered a KVM port ID in the URL, the “port field” is filled in with the port ID you entered.

2. If you entered a KVM port ID in the URL, save the URL as a bookmark or in your favorites list in the browser.

   For future connections to that port, you can click on the bookmark or item in favorites list to easily bring up the Web Manager login screen again with the port number filled in.

3. Enter your account name in “username” field and the account’s password in the “password” field.

4. If no port is listed in the “port” field, enter a port alias or number.

5. Press “Go.”

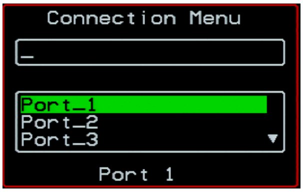
   If the Web Manager Access “Connect to Server” form appears, you are finished logging in.

6. For administrators, if a dialog box prompts you to verify whether you want to proceed by logging the other admin out or by cancelling your login attempt, click the appropriate radio button and then click Apply.

Note: Only one admin can be logged in at a time.

Connecting to Servers Locally Through the OSD

Administrators and authorized regular users who have local access to the 16-port CAT5 KVM can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are connected to KVM ports on the master 16-port CAT5 KVM or on any cascaded KVM device.



Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the 16-port CAT5 KVM. See “To Connect to the User 1 Management Port” on page 64 for instructions on connecting to the User 1 port, or see “To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM” on page 98 for instructions on connecting to the User 2 port.

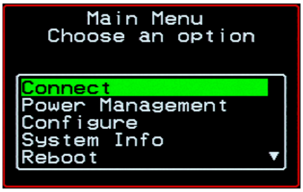
Connections made through the OSD are to physically connected devices only. Use the Web Manager to connect to a remote device. See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 266 for instructions.

Note: The OSD cannot be used to access in-band servers. See “Connecting to Servers Remotely Through the Web Manager” on page 266 for information and instructions on accessing in-band servers.

▼ *To Connect to Servers Through the OSD Connection Menu*

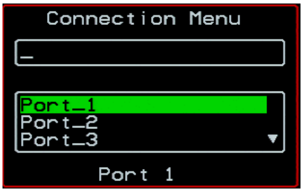
1. On the OSD Login window, enter your user name and password as provided to you by the 16-port CAT5 KVM administrator.

   The OSD Main Menu appears.



2. From the OSD Main Menu, select Connect.

   The Connection Menu appears.



3. To select the port you wish to connect to, do one of the following procedures:

   - Type the first letters of the port name in the quick search box until the desired port is highlighted in the port list box.

     This field is case-sensitive.

   - Select the desired port using the port list box.

4. Press Enter.

   Your monitor displays the work station of the connected server.

See Table 6-2, “Tasks Available While Connected to KVM Ports,” on page 272 for a complete lists of the tasks available while connected to KVM ports and references to the related instructions.

Controlling KVM Port Connections

Once connected to a server, you may want to perform one or more of the procedures listed in the following table.

Table 6-2: Tasks Available While Connected to KVM Ports

Task	Where Documented
Return to the OSD Connection menu after connecting to a port.	“To Return to the Connection Menu After Connecting to a Port” on page 275.
Access a port that is already in use by another user.	“Sharing KVM Port Connections” on page 281
Make direct connections to other servers without returning to the OSD Connection Menu.	• “To Initiate Cycle by Server” on page 276 • “To Connect to the Next Authorized Server from the Current Server” on page 277 • “To Connect to the Previous Authorized Server from the Current Server” on page 277
Reset your keyboard and mouse.	“To Reset the Keyboard and Mouse” on page 279
Adjust the color and brightness of the server window.	“To Adjust Screen Brightness and Contrast” on page 277
Power on, power off, or reboot the connected server.	“To Power On, Power Off, or Reboot the Connected Server” on page 280
View information about the currently selected port.	“To View Connected Port Information” on page 275

Hot Keys for KVM Connections

Predefined keyboard shortcuts (also called hot keys) allow you to perform common actions and launch management windows while connected through a KVM port.

The default hot keys are described in the following table. A plus (+) between two keys indicates that both keys must be pressed at once. When two keys are separated by a space, each key must be pressed separately. For example, “Ctrl+k p” means to press the Ctrl and “k” keys together followed by the “p” key, and “Ctrl Shift+i” means press the Ctrl key followed by the Shift and “i” keys pressed together.

Table 6-3: Default KVM Connection Keyboard Shortcuts

Key Combination	Action
Ctrl+k q	Quit. Closes the connection to the current KVM port and ends the KVM connection.
Ctrl+k p	Power management. Brings a power management menu with the options to turn on, off, or cycle the power for outlets to which the current server is connected.
Ctrl+k .	Next Port. Goes to the next authorized port.
Ctrl+k ,	Previous Port. Returns to the previous authorized port.
Ctrl+k v	Video. Brings up a menu that allows you to change between “Automatic control” (which compensates for the length of the cable running from the 16-port CAT5 KVM to the KVM Server Module that is connected to the server) and “Manual control” for adjusting screen brightness and contrast.
Ctrl+k s	Reset keyboard and mouse. Allows you to reset the keyboard and mouse if either of them stops responding.

The 16-port CAT5 KVM administrator may redefine the keyboard shortcuts, as described in “Redefining KVM Connection Hot Keys” on page 34. If the defaults shown in the previous table do not work, check with your 16-port CAT5 KVM administrator for the site-specified keys to use.

Hot Keys for Emulating Sun Keyboard Keys

The 16-port CAT5 KVM provides a default set of hot keys for use while connected to Sun servers. You can use the Sun hot keys to emulate keys that are present on Sun keyboards but are not present on Windows keyboards.

The hot keys are made up of an escape key followed by a function key. The default escape key is the Windows key, which is labeled with the Windows logo. The Windows key usually appears on the Windows keyboard between the `Ctrl` and `Alt` keys. The following table shows function keys and keys from the numeric keypad that emulate Sun equivalent keys when you enter them at the same time as the hot key. For example, to use the Sun `Find` key, you would press the Windows key at the same time you press the `F9` function key.

Table 6-4: Default Sun Key Emulation Hot Keys

	Win Key	Sun Key
Function Keys	F2	Again
	F3	Props
	F4	Undo
	F5	Front
	F6	Copy
	F7	Open
	F8	Paste
	F9	Find
	F10	Cut
	F11	Help
	F12	Mute

Table 6-4: Default Sun Key Emulation Hot Keys (Continued)

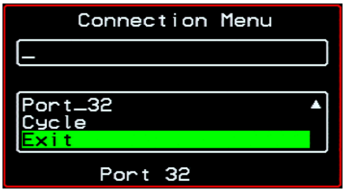
	Win Key	Sun Key
Numeric Keypad Keys	*	`Compose`
	+	`Vol +`
	-	`Vol -`

16-port CAT5 KVM administrators can change the default escape key portion of the Sun keyboard emulation hot keys from the Windows key to any of the following: `Ctrl`, `Shift`, or `Alt`. See “Redefining Sun Keyboard Equivalent Hot Keys” on page 34 for details and links to procedures.

▼ *To Return to the Connection Menu After Connecting to a Port*

1. Press Ctrl+k q to display the OSD Connect Menu.

The Connection Menu appears.



2. Do one of the following:

- To make a new server connection, select another port from the list.
- To return to the Main Menu, select Exit.
- To cycle through all servers, select Cycle.

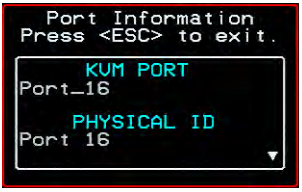
  The cycle option does not appear when you are connected through the Web Manager.

▼ *To View Connected Port Information*

1. Use the information keyboard shortcut.

The default is **Ctrl+k i**.

The following window appears.



Port Information
Press <ESC> to exit.

KVM PORT
Port_16

PHYSICAL ID
Port 16

2. Press Esc to exit the Port Information window and return to the connected server.

Cycling Between Servers

Cycle refers to the capability to connect to one or more authorized servers from the server to which you are currently connected. Through the OSD menus or by using a keyboard shortcut, you have immediate access to all configured and authorized servers.

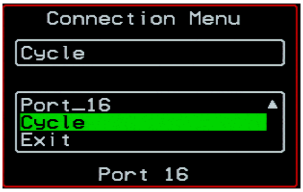
There are two types of cycle commands:

- Cycle by Server – View all authorized servers on a continuous basis until all servers have been exhausted and then start over again.
- Cycle by Key Sequence – View or access the server connected to the next or previous port in the Connection Menu list.

The servers are cycled in the order in which their ports are listed in the Server Connection form.

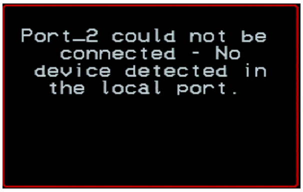
▼ To Initiate Cycle by Server

1. From the Connection Menu, choose Cycle.



2. Select Cycle at the bottom of the list.

The system initiates the cycle from the first authorized server, and the servers connected to all authorized ports appear for a few moments. If there is no device attached to the port associated with the next logical port, a message appears to indicate that there is no device connected.



```
Port_2 could not be
  connected - No
device detected in
 the local port.
```

3. To abort the process and close the session, press the escape sequence.

   The default is Ctrl+k q.

▼ To Connect to the Next Authorized Server from the Current Server

- Use the Next keyboard shortcut.

  The default is **Ctrl+k .**.

  The next authorized server appears. Repeat this step to move to the next server.

▼ To Connect to the Previous Authorized Server from the Current Server

- Use the Previous keyboard shortcut.

  The default is **Ctrl+k ,**.

  The previous authorized server appears. Repeat this step to move to the previous server.

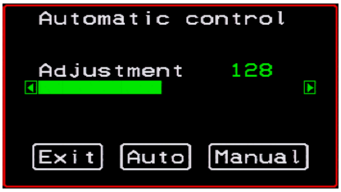
▼ To Adjust Screen Brightness and Contrast

1. Press the video control keyboard shortcut.

   The default is **Ctrl+k v**.

   Depending on which window was accessed last, one of the following windows appears.

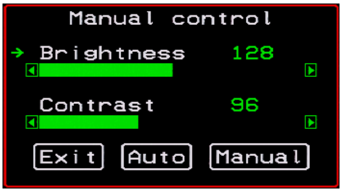
- Automatic Control



Automatic control

Adjustment 128

- Manual Control



Manual control

Brightness 128

Contrast 96

2. To switch to the Auto control window or the Manual control window select Auto or Manual respectively.

3. To adjust screen brightness and contrast on the Automatic Control window, select the right or left arrows to set the desired adjustment value.

   The Automatic Control window is used to compensate for cable length. For example, if you use a 500-foot cable, the setting might be 10 or 20. If a shorter cable such as 6 or 3 feet is used, a value of 128 or 150 is more appropriate. If this setting is not adjusted properly, the video quality may be poor.

4. To adjust screen brightness and contrast on the Manual control page, select the arrow keys to increase or decrease the contrast and brightness.

   The Manual Control window is used to control the levels of video brightness and contrast. The higher the value, the greater the brightness and contrast will be.

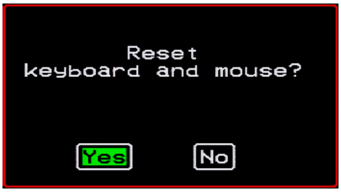
Resetting the Keyboard and Mouse

You can use the “Keyboard/Mouse Reset” hot key to bring up the “Reset keyboard and mouse?” screen if the keyboard and mouse is not working properly when accessing a server through a KVM port. This command is equivalent to unplugging and plugging in again the keyboard and mouse.

▼ To Reset the Keyboard and Mouse

1. Type the “Keyboard/Mouse Reset” hot key.

   The default is Ctrl-k s. The following confirmation window appears.



Reset
keyboard and mouse?

2. Select Yes to enable your keyboard and mouse again.

Note: See also the “Avoiding Conflicting Mouse Settings” on page 86.

Controlling Power of a KVM-connected Server

In order to control power of a server while connected to the server, the following conditions must be met:

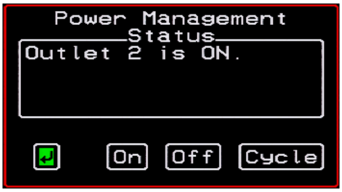
- The server must have at least one power cord plugged into an APC rPDU that is properly configured and connected to the AUX port.
- The power outlet(s) that the server is connected to must be configured to the port.
- If a regular user is accessing this device, the user must have the following permissions:
  - Full control (read, write, power) permission on the port,
  - Permission to control power on the rPDU outlet that the device is plugged into.

▼ To Power On, Power Off, or Reboot the Connected Server

1. While connected to a server, use the power management keyboard shortcut.

   The default is **Ctrl+k p**.

   A window similar to the following appears.



Outlet 2 is ON.

2. Select the configured outlet.
3. Do one of the following:
   - To turn the power on, select On.
   - To turn the power off, select Off.
   - To reboot, select Cycle.

Closing a KVM Connection

The ways you can close a KVM connection are listed below:

- For IP connections, select “Exit Viewer Client” from the Remote Viewer Shortcuts menu.
- Use a hot key sequence (Ctrl+k q) to bring up the Connection menu, then select the Exit option.
- Let the session time out.

▼ To Close a KVM Connection

Do one of the following steps.

1. To use the menu option from the Remote Viewer menu bar, go to Shortcuts and select “Exit Viewer Client.”

- OR-

2. To use the escape hot key, do the following steps.

a. Type the hot key escape sequence.

Ctrl+k q is the default.

The Connection menu appears.

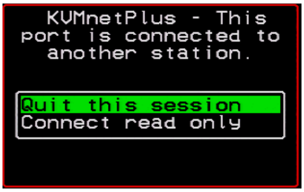
b. Type “e” in the text field to highlight the Exit option.

c. Click Enter.

Sharing KVM Port Connections

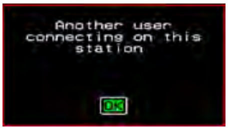
Two authorized users can connect simultaneously to a single KVM port.

When a user connects to a KVM port that is already in use, the software presents a menu to the connecting user. The options on the menu depend on the connecting user’s access permissions. The following figure shows two options that are always presented on the menu to the connecting user.

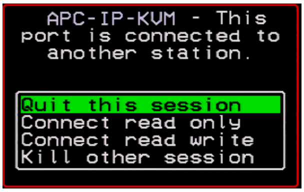


KVMnetPlus - This port is connected to another station.

The two menu options are described in the following table.

Quit this session	Ends the connection attempt and returns the user to the Connection Menu
Connect read only	Connects the user in read-only mode and sends this notice to the current user:  Another user connecting on this station

If the connecting user has either read-write, or full access permissions for the KVM port, additional menu options appear, as shown in the following figure.

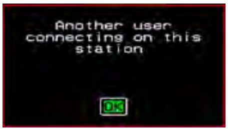


APC-IP-KVM - This port is connected to another station.

The two menu options are described in the following table.

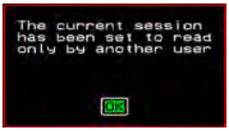
Connect read write

Connects the new user in read-write mode and sends this notice to the current user.



Another user connecting on this station

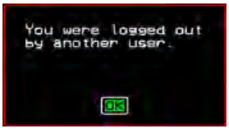
If the previous user is in read-write mode, that user’s mode is changed to read-only and the user sees the following notice:



The current session has been set to read only by another user

Kill other session

Kills the existing session and connects the new user in read-write mode. Sends the following notice to the current user and disconnects that user:



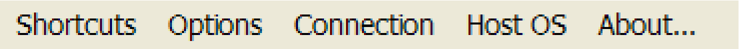
You were logged out by another user.

When the current user is in read only mode, the connecting user is always granted the highest level of access for which the connecting user is authorized.

If two users are connected to a KVM port, either user may choose at any time to change the access mode or disconnect from the session by issuing a hot key or Esc.

Remote Viewer Settings

You can configure the Remote Viewer settings from the top menu.



For a definition of the menu settings, refer to the tables below. A T1 connection is recommended for best performance when using the Remote Viewer.

Recommended Settings

The recommended Remote Viewer settings are listed in the following table. The connection you set must reflect your actual Internet connection method.

Menu	Select the following option(s):
Options	Auto Sync Mouse
Connection	T1 (preferred), No Encryption, High Color
Host OS	Auto/Other

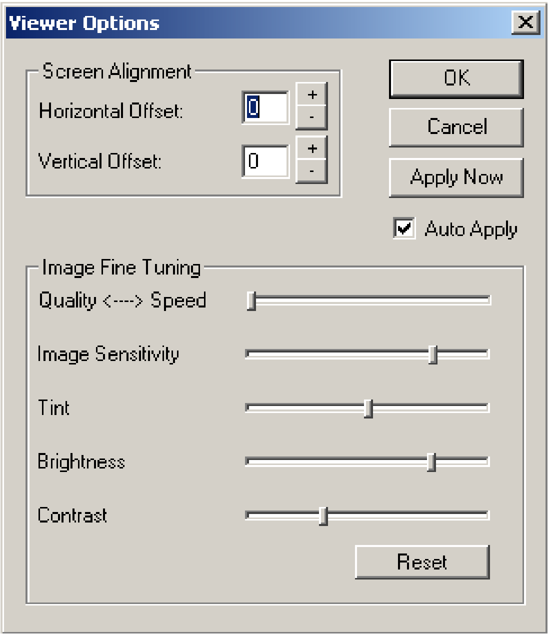
Options Menu

The following table describes the items in the Remote Viewer’s Options menu, which you can change as needed for your own requirements.

Menu Selection	Description
Force Screen Refresh	Refreshes the viewer.
Force Screen Auto Alignment	Switches to Auto Alignment mode, which may change the position of the viewer. (You can manually configure Screen Alignment by going to Options>Viewer Options>Screen Alignment.)
Toggle Full Screen	Switches the viewer’s display from window to full-screen mode or from full-screen to window mode.
Viewer Options	See Setting the Viewer Options
Show Frames/sec and Network bits/sec	Specify as needed.
Auto Sync Mouse	Make sure this is selected for APC 16-port CAT5 KVM compatibility
Show Startup Dialog	Causes a menu to appear when the viewer is launched.

Setting the Viewer Options

The Viewer Options window allows you to align or position the viewer window and to fine tune the image. The configuration for these settings may vary from one system to another.



Viewer Options

Screen Alignment

Horizontal Offset: 0

Vertical Offset: 0

☑ Auto Apply

Figure 6-6: Remote Viewer Options Screen

The following table defines the fields and menu items.

Table 6-5: Remote Viewer>Options>Viewer Options Menu

Field or Menu Item	Function
Horizontal Offset	The horizontal coordinate for positioning the Remote Viewer on the screen (default = 0).
Vertical Offset	The vertical coordinate for positioning the Remote Viewer on the screen (default = 0).
Quality <---->Speed	Move slider to the left to increase image quality; move slider to the right to increase the performance of the viewer.

Table 6-5: Remote Viewer>Options>Viewer Options Menu (Continued)

Field or Menu Item	Function
Image Sensitivity	Move slider to the right to increase the image sensitivity.
Tint	Move the slider in either direction to achieve the desired color. For a neutral (white) color, keep the slider in the middle.
Brightness	Move the slider to the right to increase screen brightness.
Contrast	Move the slider to the right to increase screen contrast.

Connection Menu

The following table describes the Connection menu options.

Menu Selection	Function
56K	For when your network connection method is a 56K modem
DSL	For when your network connection method is a DSL line
T1	Recommended connection type. For when your network connection method is a dedicated T1 line
Low BW LAN	For when you are connecting through a low bandwidth local area network
LAN	For when you are connecting through a standard speed local area network.
Auto	For setting the connection mode automatically
Encrypt Everything	For encrypting everything
Encrypt Keyboard and Mouse	For encrypting only keyboard and mouse input

Menu Selection	Function
Encryption Type	For either RC4 or Triple DES encryption
No Encryption	For no encryption
High Color	For high color resolution screens
Low Color	For low color resolution screens
Grey Scale	For grey scale screens
Low Grey Scale	For low resolution grey scale screens

Power Management

Administrators and authorized users can access Power Management windows, which allow you to check the status of the rPDUs connected to the AUX port from the Web Manager and the OSD. Any user who has administration privileges can turn on, turn off, or cycle (reboot) the outlets. See “Options for Managing Power” on page 39 for a detailed description of how authorized users can manage power. See “Setting Up and Configuring Power Management” on page 40 for a list of the administrative tasks involved in setting up power management.

The following section gives instructions on managing power through the OSD while connected locally to the 16-port CAT5 KVM.

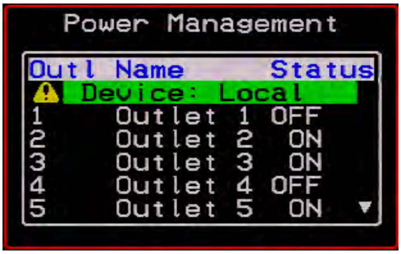
For instructions on how to manage power remotely through the Web Manager, see Table 5-1 on page 250 for a list the power management tasks available to regular users through the Web Manager and links to the associated procedures.

For instructions on managing power servers while connected to them through KVM ports, see “To Power On, Power Off, or Reboot the Connected Server” on page 280.

▼ *To Power On, Power Off, or Cycle Devices Plugged into rPDU Outlets*

1. Go to: Configure > Power Management.

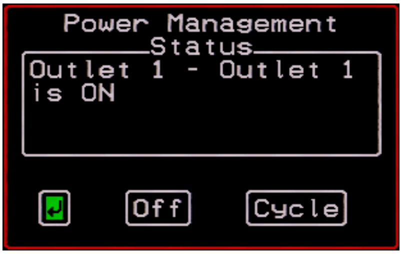
   The Outlet Status page appears with a list of all configured rPDUs. The status column displays whether the outlet is on or off.



```
         Power Management
Outl Name           Status
⚠ Device: Local
1        Outlet 1 OFF
2        Outlet 2  ON
3        Outlet 3  ON
4        Outlet 4 OFF
5        Outlet 5  ON    ▼
```

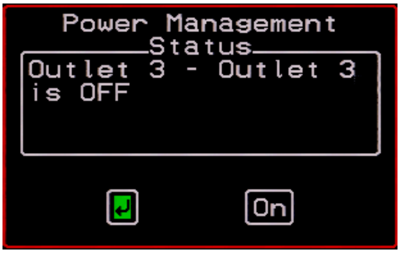
2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

   The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.



```
    Power Management
          Status
Outlet 1 - Outlet 1
is ON
```

The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is off displays only the On and Cycle option as in the following figure.



```
Power Management
Status
Outlet 3 - Outlet 3
is OFF
```

3. Use the arrow keys to select On, Off, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

Modem Connections

In addition to connecting to the 16-port CAT5 KVM through a regular Ethernet connection, you can also access the 16-port CAT5 KVM by dialing in through an installed external modem. Use PPP when dialing into any of the supported modems. Once the connection is made, all connections to the specified IP address are made through the PPP connection. For example, if you enter the specified IP address in a browser after making the PPP connection, the browser connects to the 16-port CAT5 KVM through the dialup connection. This way you can access the Web Manager through PPP even if the IP connection to the 16-port CAT5 KVM is not available.

The 16-port CAT5 KVM administrator performs the procedures to install and configure the modems. Contact your 16-port CAT5 KVM administrator for the phone numbers, user names, and passwords to use, and for questions about how the modems are configured.

Before anyone can use PPP to access the 16-port CAT5 KVM, the PPP connection must be configured by the user on the remote computer so the connection can be used for dialing in. Before configuring PPP, you need the following:

- A modem connected to the remote computer.
- The phone number of the line that is dedicated to the 16-port CAT5 KVM modem you want to access.
- If authentication is required for the modem, you need a user name and password for a user account on the 16-port CAT5 KVM.

The following table lists the related procedures and where they are documented.

Table 6-6: Tasks for Configuring and Making Dial Up Connections (User)

Configure a PPP Connection.	“To Configure a PPP Connection on a Remote Computer” on page 291
Connect Using PPP.	“To Make a PPP Connection From a Remote Computer” on page 292

▼ *To Configure a PPP Connection on a Remote Computer*

Perform this procedure on a remote computer with a modem to do the following:

- Create a PPP connection that anyone can use for dialing up the 16-port CAT5 KVM
- Optionally configure call back.

See the prerequisites listed in “Modem Connections” on page 290, if needed.

Note: The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems. You can use this procedure as an example.

1. From “My Computer,” go to “My Network Places.”
2. Under “Network Tasks,” click “View network connections.”
3. Under “Network Tasks,” select “Create a new connection.”

   The “New Connection Wizard” appears.
4. Click the “Next” button.
5. Click “Connect to the Internet” and click “Next>.”

   The “Getting Ready” form appears.
6. Click “Set up my connection manually” and click “Next>.”

   The “Internet Connection” form appears.
7. Click “Connect using a dial-up modem” and click “Next>.”

   The “Connection Name” form appears.

   Type a name for the connection to the 16-port CAT5 KVM in the “ISP Name” field and click “Next>.”

   The “Phone Number to Dial” form appears.
8. Type the phone number for the 16-port CAT5 KVM’s modem in the “Phone number” field and click “Next>.”

   The “Internet Account Information” form appears.

9. Type the user name for accessing the 16-port CAT5 KVM in the “User Name” field.
10. Type the password for accessing the 16-port CAT5 KVM in the “Password” and “Confirm Password” field and click “Next>.”
11. Click the “Finish” button.

    The “`Connect` *`connection_name”`* dialog appears.
12. Click the “Cancel” button.

    The name of the connection appears on the Network Connections” list.
13. To configure call back, do the following steps.
    a. Select the name of the connection from the Network Connections dialog box.
    b. Select “Dial Up Preferences” from the “Advanced” menu.

       The “Dial-up Preferences” dialog box appears.
    c. Click the “Callback” tab.
    d. Click “Always call me back at the number(s) below.”
    e. Highlight the name of the modem and click “Edit.”

       The “Call Me Back At” dialog box appears.
    f. Enter the phone number of your local modem in the “Phone number:” field, and click OK.

▼ *To Make a PPP Connection From a Remote Computer*

Perform this procedure on a remote computer that has a modem to initialize a dial up and optional call back session on the 16-port CAT5 KVM. This procedure assumes a PPP connection for dial up or call back has previously been created as described in “To Configure a PPP Connection on a Remote Computer” on page 291.

Note: The following steps work if you are on a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use these steps as an example.

1. From the Start menu, go to My Computer>My Network Places.
2. Under “Network Tasks,” click “View network connections.”
3. Double-click the name of the connection in the list.

   The “`Connect` *`connection_name”`* dialog appears.
4. Type the user name and password in the “User Name” and “Password” fields.
5. Click the “Dial” button

Chapter 7
On Screen Display

Administrators and regular users can use the OSD for troubleshooting when a direct connection method is required. However, most configuration and operations tasks are performed through the Web Manager, as described in Chapter 5 and Chapter 4.

Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the16-port IP KVM. See “To Connect to the User 1 Management Port” on page 64 for instructions on connecting to the User 1 port, or see “To Connect the APC CAT5/IP KVM Console Extender to the 16-port IP KVM” on page 98 for instructions on connecting to the User 2 port.

Once the connected monitor is turned on, the OSD login window appears.

See the following sections for more information on the OSD screens:

Navigating the OSD

In the OSD you can use keyboard sequences to navigate the windows and make menu selections. The following sections describe:

- Basic Navigation Keys
- Common Navigation Actions

Basic Navigation Keys

The following table displays a short list of keyboard controls to help you navigate the 16-port IP KVM on screen display. The OSD window must be selected and in an *active* state for these keys to work.

Table 7-1: Basic Navigation Keys

Key	Action
Tab	Changes between fields on the window
Up / Down	Scrolls within a menu
Left / Right	Selects a button in a button field
Backspace	Deletes the character left to the cursor
Page Up / Page Down	Pages within a menu
End	Moves to the end of a menu
Home	Moves to the top of a menu
Enter	Selects highlighted item / Commits changes
Esc	Returns to the previous main menu

Common Navigation Actions

Table 7-2 shows how to perform common actions used to go to windows, select items, and commit changes in the OSD.

Table 7-2: OSD Equivalents for Common Actions

Action	OSD Equivalent
Select OK	Tab to the OK button and press the Enter key on your keyboard.
Save changes	Tab to the Save button and press the Enter key.
Select an option	Tab to the option and press the Enter key.
Go to a specific window, as in: Go to Configure>Users and Groups."	Select the first option from the Main menu. On the next window that comes up select the next option from that menu. Do this until you get to the last option in the menu path.

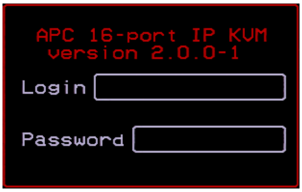
Logging On Through the OSD

In order to log on to the 16-port IP KVM through the OSD, you need to connect a keyboard, monitor, and mouse to the monitor, keyboard, mouse connectors, labelled User 1, on the 16-port IP KVM. See "To Connect to the User 1 Management Port" on page 64 for more information.

Optionally, you can connect to the OSD using an Console Extender, which you buy separately. See "Installing the APC CAT5/IP KVM Console Extender" on page 97 for instructions on installing the Console Extender. See "Controlling the OSD Through the APC CAT5/IP KVM Console Extender" on page 366 for instructions on using the Console Extender.

▼ *To Log In to the 16-port IP KVM Through the OSD*

1. Type your user name followed by your password.



2. Press <Enter>.

   The main menu of the 16-port IP KVM OSD appears. See the following section, “OSD Main Menu” on page 298 for a description of the OSD Main Menu items.

OSD Main Menu

The OSD Main Menu provides six menu selections as depicted in the following figure.

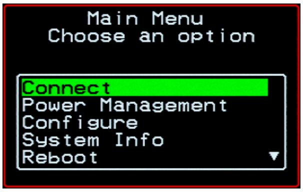


Figure 7-1:OSD Main Menu

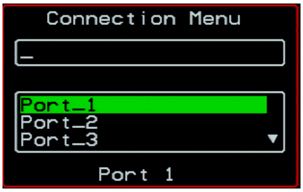
Table 7-5 gives a brief description of each menu item and lists where you can find more information.

Table 7-3: OSD Main Menu Items

Menu Selection	Select the menu item to:	Where Documented
Connect	View the Server Connection Menu and select the port to which you want to connect.	Page 299
Power Management	View status of all outlets on connected rPDUs and power on, power off, and cycle connected devices.	Page 300
Configure	View the Configuration Menu and perform 16-port IP KVM configuration.	Page 301
System Info	View the system information pertaining to the KVM version that you are using.	Page 363
Reboot	Reboot the 16-port IP KVM.	Page 364
Exit	Exit from the OSD and close the session.	N/A

Connection Menu

Administrators and authorized regular users can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are physically connected to KVM ports on the master 16-port IP KVM or on any cascaded KVM device.



See “To Connect to Servers Through the OSD Connection Menu” on page 270 for instructions on connecting to servers through the OSD.

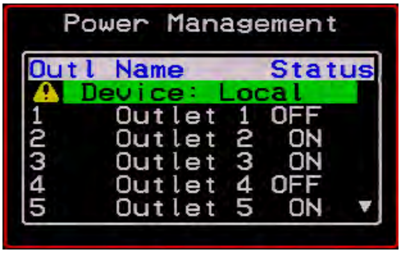
Power Management Menu

The Power Management windows allow you to check the status of the master APC rPDU connected to the AUX port in addition to all cascaded rPDUs. Any user who has administration privileges can turn on, turn off, and cycle (reboot) the outlets. See “Connecting APC rPDUs to the 16-port IP KVM” on page 95 for instructions on connecting rPDUs to the 16-port IP KVM.

▼ *To Power On, Power Off, or Cycle Devices Plugged into rPDU Outlets*

1. Go to: Configure > Power Management.

   The Outlet Status page appears with a list of all configured rPDUs. The status column displays whether the outlet is on or off.

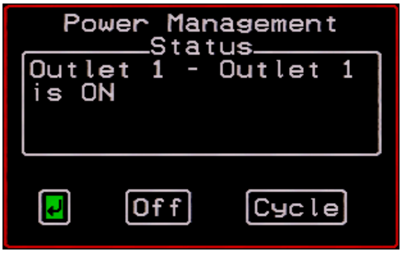


```
       Power Management

Outl Name          Status
⚠  Device: Local
1       Outlet 1  OFF
2       Outlet 2   ON
3       Outlet 3   ON
4       Outlet 4  OFF
5       Outlet 5   ON   ▼
```

2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

   The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.

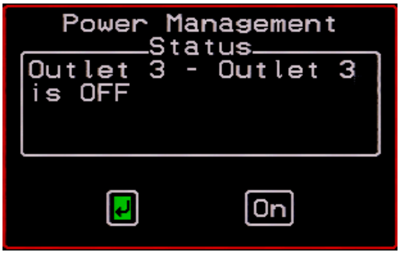


Power Management

Status

Outlet 1 - Outlet 1 is ON

The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is off displays only the On option as in the following figure.



Power Management

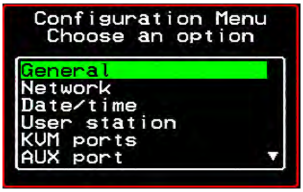
Status

Outlet 3 - Outlet 3 is OFF

3. Use the arrow keys to select On, Off, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

Configure Menu Overview

Selecting “Configure” from the OSD Main Menu brings up the Configuration Menu. The Configuration Menu provides a number of options, as shown in the following screen.



```
Configuration Menu
 Choose an option

General
Network
Date/time
User station
KVM ports
AUX port
```

Not all the options are visible. Table 7-4 gives a brief description of all the menu options and lists where you can find more information

Table 7-4: Configuration Menu Items

Menu Selection	Select the menu item to:	Where Documented
General	Configure authentication type for direct logins to KVM ports; syslog facility number; KVM connection hot key escape sequence, and Sun Keyboard emulation hot key escape sequence. **Note:** syslogging also requires configuration of the syslog server using the Syslog option, described later in this table.	“General Configuration Screens [OSD]” on page 305
Network	Configure DHCP or assign an IP address and configure other basic network parameters; configure SNMP, VPN, IP filtering, hosts, and static routes	“Network Configuration Menu Options [OSD]” on page 308
Date/Time	Enable/disable NTP or manually configure the system date and time.	“Date/time Configuration Screens” on page 332
User Station	Configure the Local User station’s idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current work station.	“User Station Screens” on page 333
KVM Ports	Activate KVM ports, assign aliases, and enable power management.	“KVM Ports Screens” on page 337

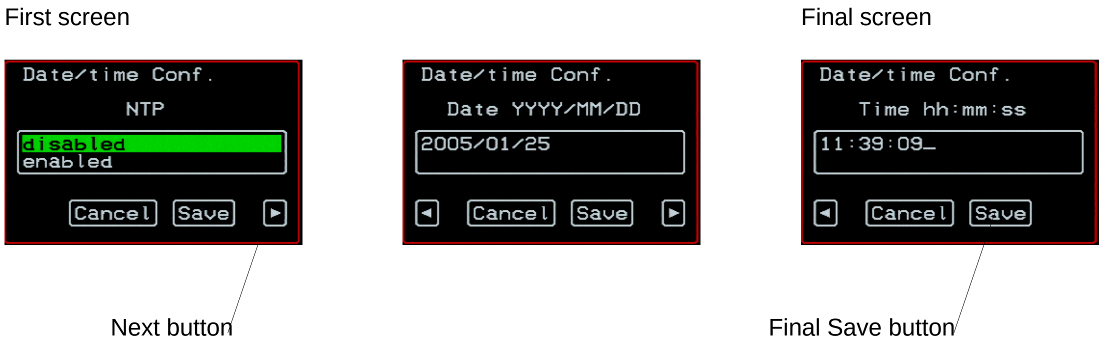
Table 7-4: Configuration Menu Items (Continued)

Menu Selection	Select the menu item to:	Where Documented
AUX Port	Configure the AUX port for PPP or power management.	"AUX Port Screens" on page 338
Users and Groups	Configure users and groups, user passwords, and KVM port access permissions.	"Users and Groups Screens" on page 344
Cascade Devices	Add, edit, or delete configurations of cascaded (slave) KVM units.	"Cascade Devices" on page 341
Syslog	Configure the IP address of the syslog server. **Note:** syslogging also requires assignment of a facility number using the General option, described earlier in this table.	"Syslog Screens" on page 351
Authentication	Configure an authentication method for logins to the 16-port IP KVM and authentication servers for 16-port IP KVM and KVM port logins.	"Authentication Screens" on page 352
Save/Load Config	Permanently save configuration changes, load a stored configuration or restore the configuration to factory default values.	"System Info Menu" on page 363
Exit	Exit from the menu.	N/A

Understanding OSD Configuration Screen Series

Selecting an option from the “Configure” menu usually brings you through a series of related screens, which you navigate through one at a time until you reach the final screen.

For example, if you select Date/Time, you are presented with a series of “Date/time Config.” screens starting with “NTP” and ending with “Time,” as shown in the following figure.



First screen

Date/time Conf.
NTP
disabled
enabled

Date/time Conf.
Date YYYY/MM/DD
2005/01/25

Final screen

Date/time Conf.
Time hh:mm:ss
11:39:09_

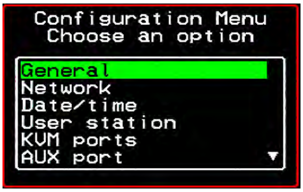
Figure 7-2: First, Middle, and Last Screens in Configuration Series

As illustrated, all the configuration screens except the final screen have a right arrow at the bottom right that you can select to go to the next screen. Clicking “Save” on any one of the screens saves the changes made to that point. You can wait until you get to the final screen in a series before saving changes. Clicking “Save” on the final screen saves any change you have made and takes you back to the Configuration menu.

See “Navigating the OSD” on page 296, if needed, for instructions on how to use the Tab key and other keys to move around the screens in the OSD.

General Configuration Screens [OSD]

You can select the General option on the OSD Configuration Menu to configure several general features of the 16-port IP KVM, which are introduced under “General” on page 302.



Selecting Configure>General from the OSD Main Menu brings up the Authentication type screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-5 gives a brief description of the sequence of General configuration screens.

Table 7-5: General Configuration Screens [OSD]

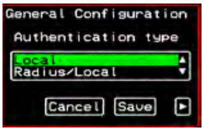
Screen	Description
Authentication Type  General Configuration Authentication type Local Radius/Local Cancel Save	The authentication type applies to *direct KVM port logins from the 16-port IP KVM login screen*: None, Local, Radius, TacacsPlus, Kerberos, LDAP, RadiusDownLocal, TacplusDownLocal, KerberosDownLocal, LdapDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal, and Windows NT/2K/2K3. Direct logins to KVM ports must also be enabled. (See “Direct Access” on page 307.) You also must ensure that an authentication server is specified for the type of method you select. See “Authentication Screens” on page 352.

Table 7-5: General Configuration Screens [OSD] (Continued)

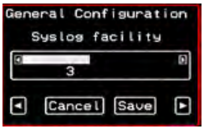
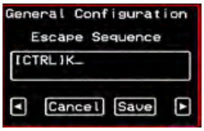
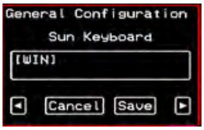
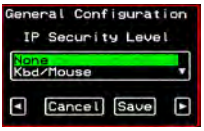
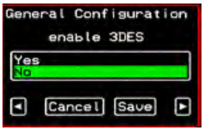
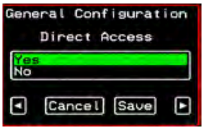
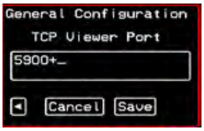
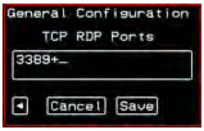
Screen	Description
Syslog Facility  General Configuration Syslog facility 3 Cancel Save	The syslog facility number that is used by the administrator of the syslog server to identify messages generated by devices connected to the KVM ports. Obtain the facility number to use for the 16-port IP KVM from the syslog server's administrator. Values are from 0 through 7. See "Syslog Servers" on page 46 for examples of using facility numbers as needed. In addition, the IP address of the syslog server must be configured, as described under "Syslog Screens" on page 351.
Escape Sequence  General Configuration Escape Sequence [CTRL]K_ Cancel Save	The escape sequence for Remote Viewer hot keys [Default: `Ctrl+k`, shown as `[CTRL]K` in the screen]. See "Redefining KVM Connection Hot Keys" on page 34 for more details.
Sun Keyboard  General Configuration Sun Keyboard [WIN] Cancel Save	The escape key for Sun hot keys. Default = the Windows [WIN] key, which is the key with the Windows logo on it. Other options are: [CTRL], [SHIFT], and [ALT]. See "Redefining Sun Keyboard Equivalent Hot Keys" on page 34 for more details.
IP Security Level  General Configuration IP Security Level None Kbd/Mouse Cancel Save	The level of encryption: "None," "encrypt keyboard and mouse data," or "encrypt data from the keyboard, video, and mouse."
3DES  General Configuration enable 3DES Yes No Cancel Save	Disables or enables 3DES encryption.

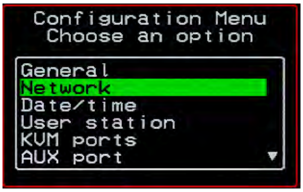
Table 7-5: General Configuration Screens [OSD] (Continued)

Screen	Description
Direct Access  General Configuration Direct Access Yes No 	Enables or disables direct access to KVM ports from the Web Manager login screen.
TCP Port Viewer  General Configuration TCP Viewer Port 5900+_ 	Allows you to assign an alternate TCP Port number or numbers for the Remote Viewer to use [Default, 5900+]. Use the plus sign (+) to increment the port number by 1 for each additional Remote Viewer. For example: 5903+ means that the first Remote Viewer uses port 5903 and the second uses port 5904. Use the hyphen (-) to indicate a range of addresses, for example, 5903-5907. Use the comma (,) to separate two TCP port addresses, for example, 5901,5903. Combine commas and hyphens, as desired, for example: 1901,5903-5905,5907. **Note:** Do not use reserved port numbers 1 through 1024.
TCP RDP Ports  General Configuration TCP RDP Ports 3389+_ 	Specify the TCP ports or a range of TCP ports to be used for RDP (in-band) server connections. You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the 16-port IP KVM. For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”. You can request valid TCP ports from your network administrator.

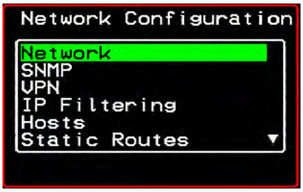
Note: The Save button on every screen saves configuration changes into the configuration files. To permanently save the configuration changes, you must select Save/Load Conf. from the Configuration Menu.

Network Configuration Menu Options [OSD]

You can select the Network option on the OSD Main Menu to configure network-related services for the 16-port IP KVM.



Selecting Network under Configuration brings up the Network Configuration Menu. The Network Configuration Menu provides a number of options, as shown in the following screen.



Not all the options are visible. The following diagram lists the names of all the configuration options accessed from the Configure>Network menu.

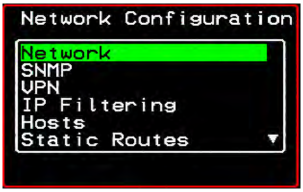
Configure

- Network
  - Network
  - SNMP
  - VPN
  - IP Filtering
  - Hosts
  - Static Routes
  - Exit

The configuration screen series for each of the options under Configure>Network are listed and described in the following sections:

Network Configuration Screens [OSD]

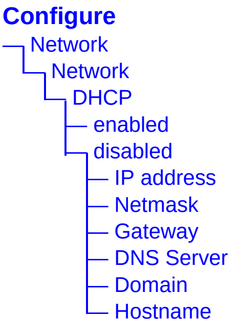
You can select the Network option from the Network Configuration menu to configure DHCP or configure a fixed IP address and other basic network parameters.



Network Configuration

Network
SNMP
VPN
IP Filtering
Hosts
Static Routes ▼

The following diagram lists the names of the configuration screens accessed under Configure>Network>Network.



Selecting Configure>Network>Network from the OSD Main Menu brings up the DHCP screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-6 gives a description of all the related configuration screens.

Table 7-6: Network Configuration Screens [OSD]

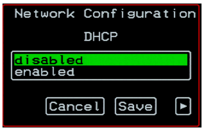
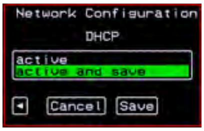
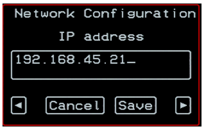
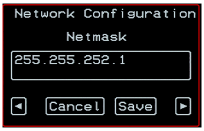
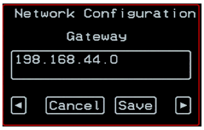
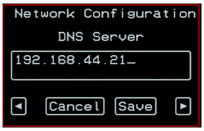
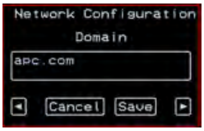
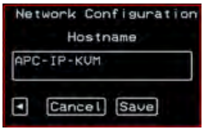
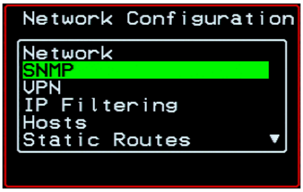
Screen	Description
DHCP  Network Configuration DHCP disabled enabled Cancel Save ►	Enable or disable DHCP. When you select “enabled,” the screen shown in the following figure appears.  Network Configuration DHCP active active and save ◄ Cancel Save “active” saves the changes to the configuration files. “active and save” overwrites the backup configuration files and makes the changes permanent. Either choice brings you back to the Network Configuration menu. When “disabled” is selected, the IP address, Netmask, Gateway, DNS Server, Domain, and Hostname forms appear in the sequence shown in the following rows.
IP Address  Network Configuration IP address 192.168.45.21_ ◄ Cancel Save ►	The IP address of the 16-port IP KVM.
Netmask  Network Configuration Netmask 255.255.252.1 ◄ Cancel Save ►	The netmask for the subnet (if applicable) in the form *NNN.NNN.NNN.N* (for example: `255.255.252.0`).

Table 7-6: Network Configuration Screens [OSD] (Continued)

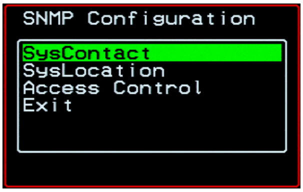
Screen	Description
Gateway  Network Configuration Gateway 198.168.44.0 	The IP address for the gateway (if applicable).
DNS Server  Network Configuration DNS Server 192.168.44.21_ 	The IP address for the DNS server.
Domain  Network Configuration Domain apc.com 	The domain name.
Hostname  Network Configuration Hostname APC-IP-KVM 	The hostname for the 16-port IP KVM.

SNMP Configuration Screens [OSD]

You can select the SNMP option from the Network Configuration menu to configure SNMP.



Selecting SNMP under Configuration>Network brings up the SNMP Configuration Menu. The SNMP Configuration Menu provides a number of options, as shown in the following screen.



The following diagram lists the names of all the configuration screen series accessed from the Configuure>Network>SNMP Configuration menu.

The following diagram lists the names of the configuration screens accessed under Configure>Network>SNMP.

Configure

- Network
  - SNMP
    - SysContact
    - SysLocation
    - Access Control
      - SNMPv1/2
        - Add | Edit
          - Community
          - Source
          - OID
          - Permission
            - Read-Only
            - Read-Write
        - Delete
        - Exit
      - SNMPv3
        - Add | Edit
          - User Name
          - Password
          - OID
          - Permission
            - Read-Only
            - Read-Write
        - Delete
        - Exit
      - Exit
    - Exit

Table 7-7 gives a brief description of all the SNMP configuration screens.

Table 7-7: SNMP Configuration Screens [OSD]

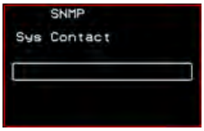
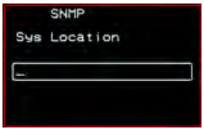
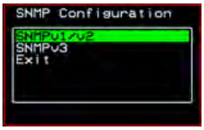
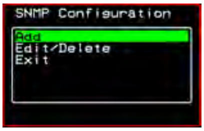
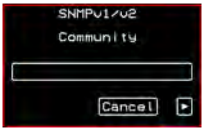
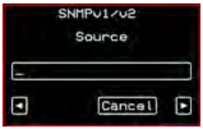
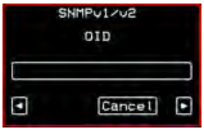
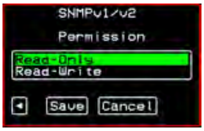
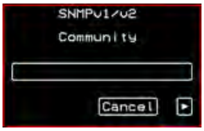
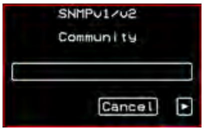
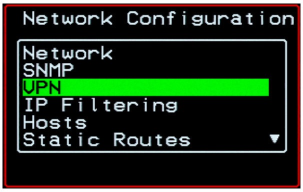
Screen	Description
SysContact  	The email address for the 16-port IP KVM administrator, for example: `kvm_admin@apc.com`.
SysLocation  	The physical location of the 16-port IP KVM.
Access Control  	Choices are SNMP v1/2 or SNMP v3.
SNMP Configuration  	Appears when either SNMP v1/2 or SNMP v3 is selected. Choices are “Add,” “Edit/Delete,” or “Exit.”
SNMPv1/v2 Community  	The community name is sent in every SNMP communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under “Permission”: either read only or read write. The most common community is “public” and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the 16-port IP KVM.

Table 7-7: SNMP Configuration Screens [OSD] (Continued)

Screen	Description
SNMPv1/v2 Source  	The source IP address or range of IP addresses.
SNMPv1/v2 or v3 OID  	Object Identifier. Each managed object has a unique identifier.
SNMPv1/v2 or v3 Permission  SNMPv1/v2 Permission Read-Only Read-Write Save Cancel	Choices are “Read-Only” and “Read-Write.” Read Only - Read-only access to the entire MIB (Management Information Base) except for SNMP configuration objects. Read/Write - Read-write access to the entire MIB except for SNMP configuration objects.
SNMPv3 User Name  	User Name.
SNMPv3 Password  	Password.

VPN Configuration Screens [OSD]

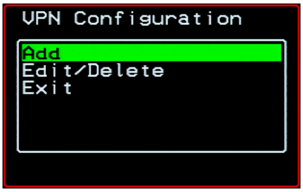
You can select the VPN option from the Network Configuration menu to configure VPN.



Network Configuration

Network
SNMP
VPN
IP Filtering
Hosts
Static Routes ▼

Selecting VPN under Configuration>Network brings up the VPN Configuration Menu. The VPN Configuration Menu provides the options shown in the following screen.

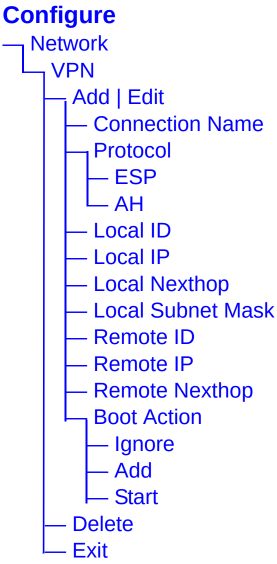


VPN Configuration

Add
Edit/Delete
Exit

You can use these options to add a VPN connection or to edit or delete a previously configured VPN connection. See “VPN” on page 205 for details.

The following diagram lists the names of the configuration screens accessed from the Add and Edit/Delete options on the Configuure>Network>VPN Configuration menu.



- **Configure**
  - Network
    - VPN
      - Add | Edit
        - Connection Name
        - Protocol
          - ESP
          - AH
        - Local ID
        - Local IP
        - Local Nexthop
        - Local Subnet Mask
        - Remote ID
        - Remote IP
        - Remote Nexthop
        - Boot Action
          - Ignore
          - Add
          - Start
      - Delete
      - Exit

Table 7-8 gives a brief description of the VPN configuration screens series under Add and Edit.

Table 7-8: VPN Configuration Screens [OSD]

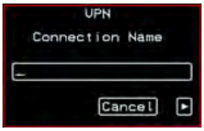
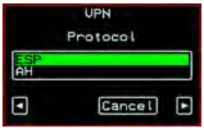
Screen	Description
Connection Name  	Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN”
Protocol  	The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header)

Table 7-8: VPN Configuration Screens [OSD] (Continued)

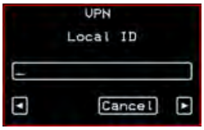
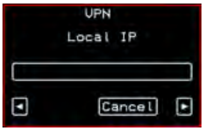
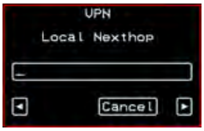
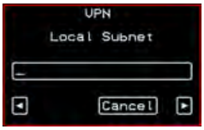
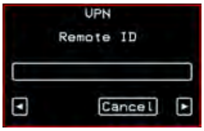
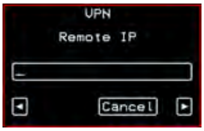
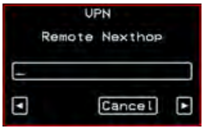
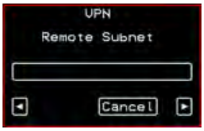
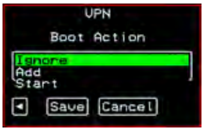
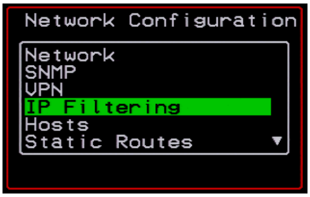
Screen	Description
Local ID  	The hostname of the 16-port IP KVM, referred to as the “local” host.
Local IP  	The IP address of the 16-port IP KVM.
Local NextHop  	The router through which the 16-port IP KVM sends packets to the host on the other side.
Local Subnet Mask  	The netmask of the subnetwork where the 16-port IP KVM resides, if applicable.
Remote ID  	The hostname of the remote host or security gateway
Remote IP  	The IP address of the remote host or security gateway.

Table 7-8: VPN Configuration Screens [OSD] (Continued)

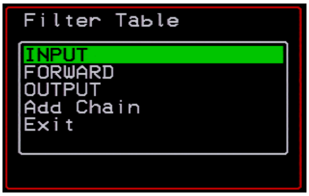
Screen	Description
Remote Nexthop 	The IP address of the router through which the host on the other side sends packets to the 16-port IP KVM.
Remote Subnet Mask 	The netmask of the subnetwork where the remote host or security gateway resides, if applicable.
Boot Action  VPN Boot Action Ignore Add Start Save Cancel	Choices are “Ignore,” “Add,” and “Start.” “Ignore” means that VPN connection is ignored. “Add” means to wait for connections at startup. “Start” means to make the connection

IP FIltering Configuration Screens

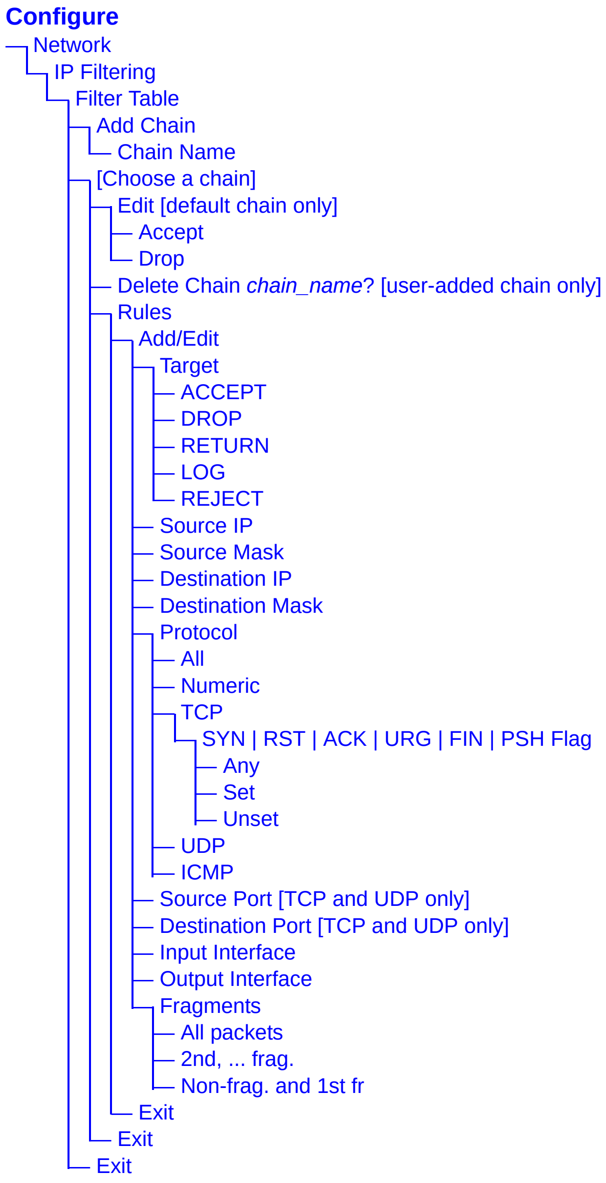
You can select the IP Filtering option from the Network Configuration menu to configure the 16-port IP KVM to filter packets like a firewall.



Selecting IP Filtering under Configuration>Network brings up the “Filter Table.” The “Filter Table” lists the default chains along with any administratively configured chains, the “Add Chain,” and the “Exit” options, as shown in the following screen.



You can use this menu to create chains and set up rules for the new chains or you can edit or delete a previously configured chain. The following diagram lists the names of the configuration screens accessed under Configure> Network>IP Filtering.



Configure

- Network
  - IP Filtering
    - Filter Table
      - Add Chain
        - Chain Name
      - [Choose a chain]
        - Edit [default chain only]
          - Accept
          - Drop
        - Delete Chain *chain_name*? [user-added chain only]
        - Rules
          - Add/Edit
            - Target
              - ACCEPT
              - DROP
              - RETURN
              - LOG
              - REJECT
            - Source IP
            - Source Mask
            - Destination IP
            - Destination Mask
            - Protocol
              - All
              - Numeric
              - TCP
                - SYN | RST | ACK | URG | FIN | PSH Flag
                  - Any
                  - Set
                  - Unset
              - UDP
              - ICMP
            - Source Port [TCP and UDP only]
            - Destination Port [TCP and UDP only]
            - Input Interface
            - Output Interface
            - Fragments
              - All packets
              - 2nd, ... frag.
              - Non-frag. and 1st fr
          - Exit
        - Exit
      - Exit

The following table shows the IP filtering screens.

Table 7-9: IP Filtering Configuration Screens [OSD]

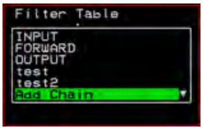
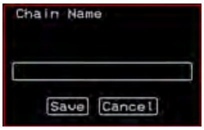
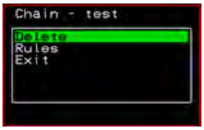
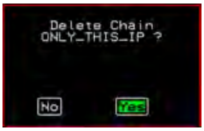
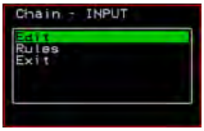
Screen	Description
Filter Table  Filter Table INPUT FORWARD OUTPUT test test2 Add Chain	Lists the default chains along with any administratively configured chains, the “Add Chain,” and the “Exit” options.
Chain Name  	Only appears when “Add Chain” is selected. Entering the name of the chain adds the new chain’s name to the “Filter Table,” where you need to select the name of the new chain and define rules for the chain.
Chain - *chain_name*  	Appears when a user-added chain is selected from the “Filter Table.” The choices are “Delete,” “Rules,” “Exit.”
Delete Chain *chain_name?*  	Appears when a user-added chain is selected and the Delete option is chosen from the “Chain - *chain_name*” menu.A
Chain - *CHAIN_NAME*  	Appears when a default chain is selected from the “Filter Table.” The choices are “Edit,” “Rules,” and “Exit.”

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

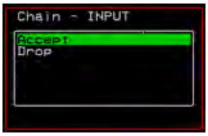
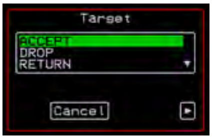
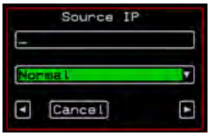
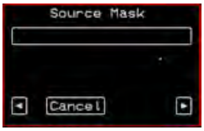
Screen	Description
Edit 	Appears when a default chain is selected and the Edit option is chosen from the Chain - *Chain_name* menu. Choices are “Accept” or “Drop.”
	The following screens define the rules for packet filtering. The packet is filtered for the characteristics defined in the rule, for example, a specific IP header, input and output interfaces, TCP flags or protocol. The target action is performed on all packets that have the characteristic. If “Inverted” is selected for a characteristic, the target action is performed on all packets that do not have the characteristic.
Target 	Appears when a user-added chain is selected. Choices specify the target action to take when a packet’s characteristics match the rule, or, if “Inverted” is selected, if the packets do not match the rule. Choices are: “ACCEPT,” “DROP,” “RETURN,” “LOG,” and “REJECT.”
Source IP 	The IP address of the source of an input packet.
Source Mask 	The netmask of the subnetwork where an input packet originates.

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

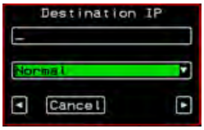
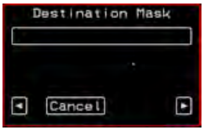
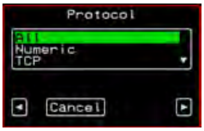
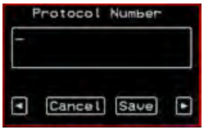
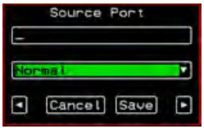
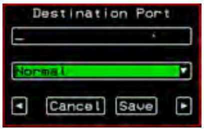
Screen	Description
Destination IP 	The IP address of an output packet's destination.
Destination Mask 	The netmask of the subnet to which an output packet is going.
Protocol 	Choices are "All," "Numeric," "TCP," "UDP," "ICMP."
Protocol Number 	Appears only if "Numeric" is selected from the "Protocol" menu.
Source Port 	Appears only if "TCP" or "UDP are selected from the "Protocol" menu. The source port number.
Destination Port 	Appears only if "TCP" or "UDP are selected from the "Protocol" menu. The destination port number.

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

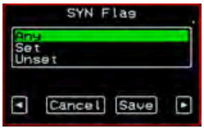
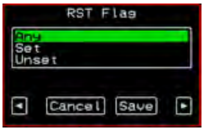
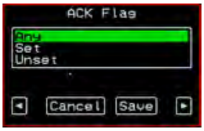
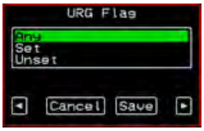
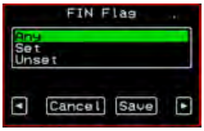
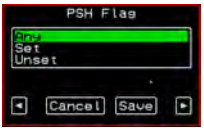
Screen	Description
SYN Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
RST Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
ACK Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
URG Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
FIN Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
PSH Flag  	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

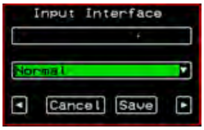
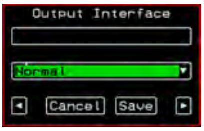
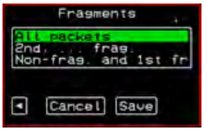
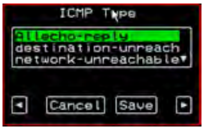
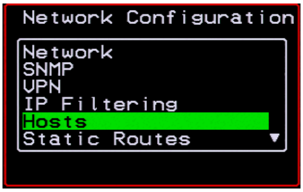
Screen	Description
Input Interface  	Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP are selected from the “Protocol” menu.
Output Interface  	Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP are selected from the “Protocol” menu.
Fragments  Fragments All packets 2nd, ... frag. Non-frag. and 1st fr Cancel Save	Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP are selected from the “Protocol” menu.

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

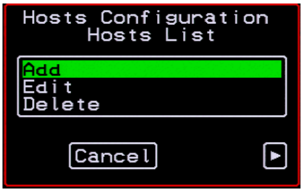
Screen	Description
ICMP Type  ICMP Type all echo-reply destination-unreach network-unreachable Cancel Save	Appears only if ICMP is selected from the “Protocol” menu. Choices are: • all • echo-reply • destination-unreachable • network-unreachable • host-unreachable • port-unreachable • fragmentation needed • source-route-failed • network-unknown • host-unknown • network-prohibited • host-prohibited

Hosts Configuration Screens [OSD]

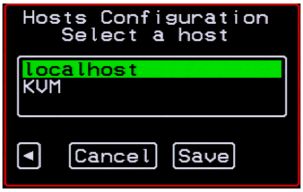
You can select the Hosts option from the Network Configuration menu to configure hosts.



Selecting Hosts under Configuration>Network brings up the “Hosts List” action menu, as shown in the following screen.



You can select the options on this menu to add, edit, or delete host entries. Selecting “Edit” or “Delete Entry” brings up the following “Select a host” screen.



The following diagram lists the names of the configuration screens accessed under Configure>Network>Hosts.

Configure

- Network
  - Hosts
    - Add | Edit
      - Select a host [Edit only]
      - IP
      - Name
      - Alias
    - Delete
      - Select a host

The following table shows the screens for the Add and Edit options.

Table 7-10: Hosts Configuration Screens [OSD]

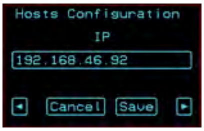
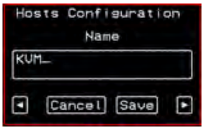
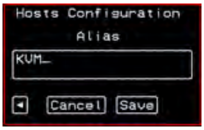
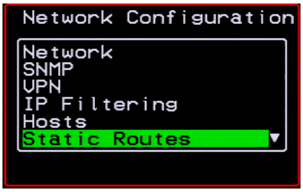
Screen	Description
IP  192.168.46.92	IP address of the host

Table 7-10: Hosts Configuration Screens [OSD]

Screen	Description
Name  	Hostname of the host
Alias  	Optional alias of the host

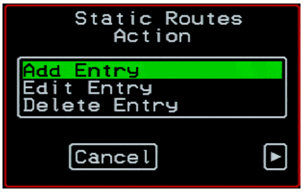
Static Routes Configuration Screens

You can select the Static Routes option from the Network Configuration menu to configure static routes.



If judiciously used, static routes can sometimes reduce routing problems and routing traffic overhead. If injudiciously used, when a network fails, static routes can block packets that would otherwise be able to find alternate routes around the point of failure if dynamic-routing were in effect.

Selecting Static Routes under Configuration>Network brings up the Static Routes Action Menu, as shown in the following screen.



The following diagram lists the names of the configuration screens accessed under Configure>Network>Static Routes.

Configure

- Network
  - Static Routes
    - Add | Edit Entry
      - Select a route [Edit option only]
      - Host or Net Route [Select host | net | default]
        - Target [host and net options only]
        - Netmask [net option only]
        - Gateway or Device
          - Gateway (gw)
            - Gateway
            - Metric
          - Network Device (dev)
            - Device
            - Metric
    - Delete Entry
      - Select a route

The following table shows the static routes screens that appear when you select one of the menu options.

Table 7-11: Static Routes Screens [OSD]

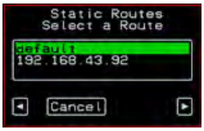
Screen	Description
Select a route  Static Routes Select a Route default 192.168.43.92 Cancel	Appears only when the Edit and Delete options are selected. Choices are “default” and any previously configured static routes.

Table 7-11: Static Routes Screens [OSD] (Continued)

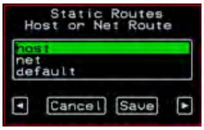
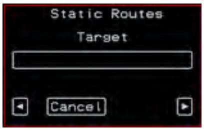
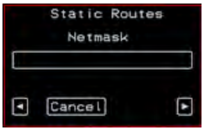
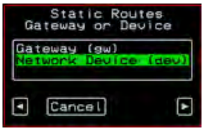
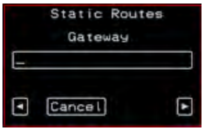
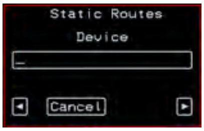
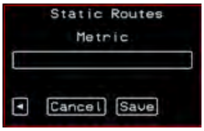
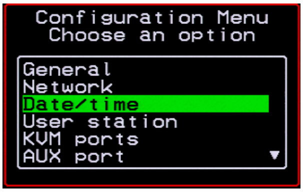
Screen	Description
Host or Net Route  Static Routes Host or Net Route host net default Cancel Save	Types of routes: "host," "net," or "default." **Note:** A default route is used to direct packets that are addressed to networks not listed in the routing table.
Target  	IP address for the target host or network.
Netmask  	Appears only when "net" is selected from the "Host or Net Route" screen. Netmask for the destination.
Gateway or Device  Static Routes Gateway or Device Gateway (gw) Network Device (dev) Cancel	Two options are: "Gateway (gw)" or "Network Device (dev)."
Gateway  	Appears only when "Gateway (gw)" is selected from the "Gateway or Device" menu. Default Gateway address.
Device  	Appears only when "Network Device" is selected from the "Gateway or Device" menu. Device address (such as `eth0`).

Table 7-11: Static Routes Screens [OSD] (Continued)

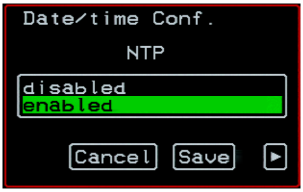
Screen	Description
Metric 	The number of hops to the destination.

Date/time Configuration Screens

You can select the Date/time option from the OSD Configuration menu to either configure an NTP server or manually set the date and time.



Selecting Date/time under Configuration>Network brings up the NTP menu, as shown in the following screen.

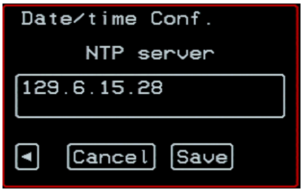


The following diagram lists the names of the configuration options accessed from the Configure>Date/time menu.

Configure

- Date/time
  - NTP
    - enabled
      - NTP server
    - disabled
  - Date/time conf.
    - Date
    - Time

If NTP is enabled, the following screen appears for entering the IP address of the NTP server.

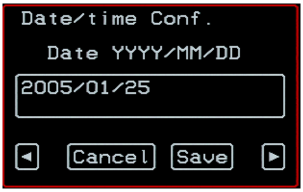


Date/time Conf.

NTP server

129.6.15.28

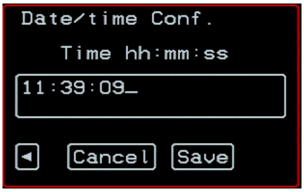
If NTP is disabled, the following series of two screens appears to allow you to enter the date and time manually.



Date/time Conf.

Date YYYY/MM/DD

2005/01/25



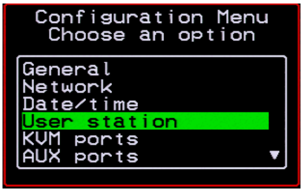
Date/time Conf.

Time hh:mm:ss

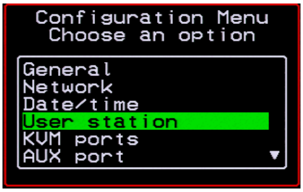
11:39:09_

User Station Screens

You can select the User Station option from the OSD Configuration menu to redefine the parameters that apply to a local user session (when a user is accessing the OSD through the User 1 or User 2 port).



Configuration Menu
Choose an option



Configuration Menu
Choose an option

The changes apply only to the currently accessed local station. For example, if an administrator configures these settings while connected to the User 2 port, these settings will be changed for all users who log on to the User 2 port, but the USer 1 port setting will remain unchanged.

The following diagram lists the configuration screens accessed through the Configure>User station option. All the screens that appear after the “Keyboard type” screen are for optionally redefining the command key portion of the KVM connection hot keys: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Configuration,” “Switch Next,” “Switch Previous,” and “Port Info.” See “Redefining Keyboard Shortcuts (Hot Keys)” on page 34 for details, if needed.

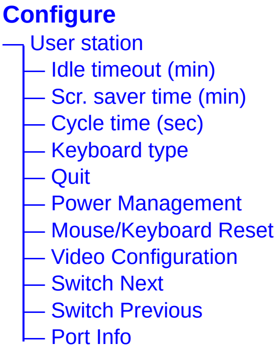


Figure 7-3: User Station Configuration Screens

The following table shows the user station configuration screens.

Table 7-12: User Station Configuration Screens

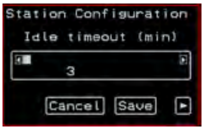
Screen	Description
Idle timeout  Station Configuration Idle timeout (min) 3 	The period of inactivity before the user is logged out from the OSD. The default is 3 minutes.

Table 7-12: User Station Configuration Screens (Continued)

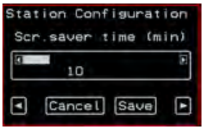
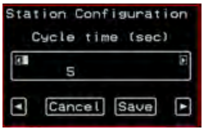
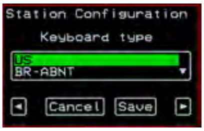
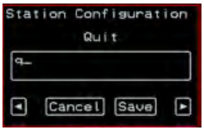
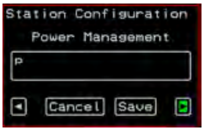
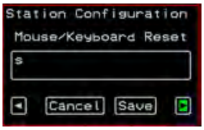
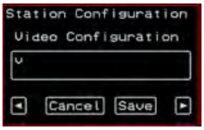
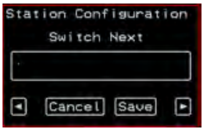
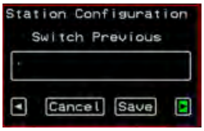
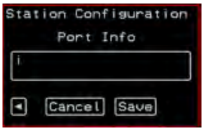
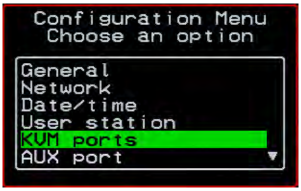
Screen	Description
Scr. saver timeout  Station Configuration Scr.saver time (min) 10 	The period of inactivity before the screen saver starts. The default is 10 minutes.
Cycling  Station Configuration Cycle time (sec) 5 	The number of seconds each server is viewed while the user is cycling from one port to another. Default = 5 seconds. See “To Initiate Cycle by Server” on page 276 for instructions on how to cycle through the servers.
Keyboard Type  Station Configuration Keyboard type US BR-ABNT 	The type of keyboard connected to the User 1 or User 2 management port of the 16-port IP KVM. • US [Default] • BR-ABNT • BR-ABNT2 • Japanese • German • Italian • French • Spanish
Quit  Station Configuration Quit q 	Redefine the command key for the KVM connection quit hot key.
Power Management  Station Configuration Power Management P 	Redefine the command key portion of the KVM connection power management hot key.

Table 7-12: User Station Configuration Screens (Continued)

Screen	Description
Mouse/Keyboard  Station Configuration Mouse/Keyboard Reset s 	Redefine the command key portion of the KVM connection mouse/keyboard reset hot key.
Video  Station Configuration Video Configuration v 	Redefine the command key portion of the KVM connection video brightness and contrast hot key.
Switch Next  Station Configuration Switch Next . 	Redefine the command key portion of the KVM connection switch next hot key.
Switch Previous  Station Configuration Switch Previous , 	Redefine the command key portion of the KVM connection switch previous hot key.
Port Info  Station Configuration Port Info i 	Redefine the command key portion of the KVM connection port info hot key.

KVM Ports Screens

You can select the KVM Ports option on the OSD Configuration Menu to configure KVM ports.



Configuration Menu
Choose an option

General
Network
Date/time
User station
KVM ports
AUX port

The following diagram lists the configuration screens accessed through the Configure>KVM ports option.

Configure

- KVM ports [Select a port]
  - Active
  - Server name
  - Power outlet

Figure 7-4:KVM Ports Configuration Screens

The following table shows the KVM port configuration screens.

Table 7-13:KVM Port Configuration Screens

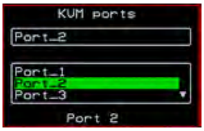
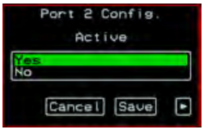
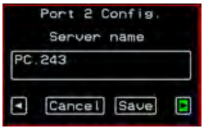
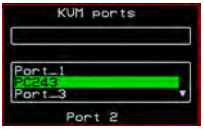
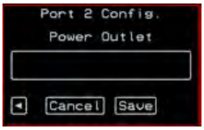
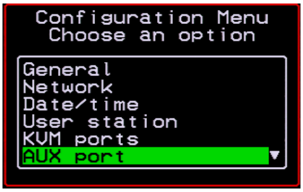
Screen	Description
KVM ports  KVM ports Port_2 Port_1 Port_2 Port_3 Port 2	Lists all KVM ports by their default names or administratively defined aliases.
Active  Port 2 Config. Active Yes No Cancel Save	Choices are “Yes” and “No” to activate or deactivate the selected KVM port.

Table 7-13:KVM Port Configuration Screens (Continued)

Screen	Description
Server name  PC.243 	Allows you to assign a descriptive alias, such as the name of the server to which the selected KVM port is connected. Only alpha-numeric characters, hyphens (-), and underscores (_) are accepted. The new alias replaces the default port name in the list of ports as shown here:  Port_1 PC243 Port_3
Power Outlet  	Allows you to enter one or more numbers that identify power outlet or outlets into which the server that is connected to this KVM port is plugged.

AUX Port Screens

You can select the AUX Port option on the OSD Configuration Menu to configure the AUX port.



The following diagram lists the configuration screens accessed through the Configure>AUX port option.

Configure

- AUX port [Select a port]
  - Active
  - Server name
  - Power outlet

Figure 7-5:AUX Port Configuration Screens

The following table shows the AUX port configuration screens.

Table 7-14:KVM Port Configuration Screens

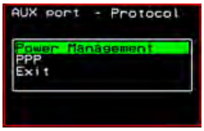
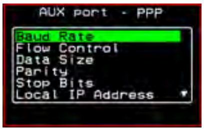
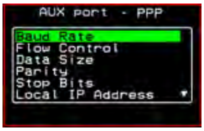
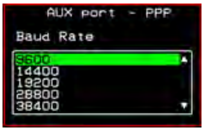
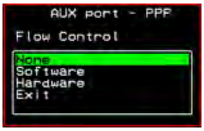
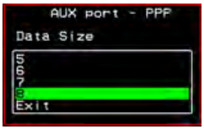
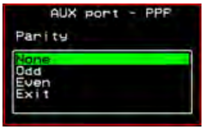
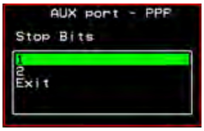
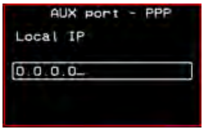
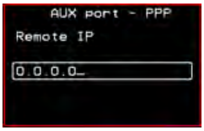
Screen	Description
AUX port - Protocol  	Choices are "Power Management" and "PPP." If you select Power Management, a confirmation screen appears. If you select PPP, the following connection configuration menu appears:  AUX port - PPP Baud Rate Flow Control Data Size Parity Stop Bits Local IP Address
AUX port - PPP  AUX port - PPP Baud Rate Flow Control Data Size Parity Stop Bits Local IP Address	Appears when PPP is selected from the AUX port - Protocol screen. Allows you to configure the connection settings for any PPP connection being made through an external modem connected to the AUX port.
AUX port - PPP Baud Rate  AUX port - PPP Baud Rate 9600 14400 19200 28800 38400	The port speed.
AUX port - PPP Flow Control  AUX port - PPP Flow Control None Software Hardware Exit	Gateway or interface address used for the route.

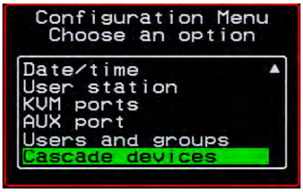
Table 7-14:KVM Port Configuration Screens (Continued)

Screen	Description
AUX port - PPP Data Size  AUX port - PPP Data Size 5 6 7 8 Exit	The number of data bits.
AUX port - PPP Parity  AUX port - PPP Parity None Odd Even Exit	None, even, or odd.
AUX port - PPP Stop Bits  AUX port - PPP Stop Bits 1 2 Exit	The number of stop bits.
AUX port - PPP Local IP  AUX port - PPP Local IP 0.0.0.0_	
AUX port - PPP Remote IP  AUX port - PPP Remote IP 0.0.0.0_	

Cascade Devices

You can select the Cascade Devices option on the OSD Configuration Menu to perform the following tasks:

- Add a secondary KVM unit to be cascaded from the master 16-port IP KVM.
- Edit the configuration of a cascaded device.
- Delete the configuration of a cascaded device.



The Cascade Devices option of the Configuration Menu allows you to configure a secondary KVM unit to be cascaded to the 16-port IP KVM to increase the number of supportable ports. The secondary device may be a 16-port IP KVM or a 16-port CAT5 KVM. The following diagram lists the configuration screens accessed through the Configure>AUX port option.

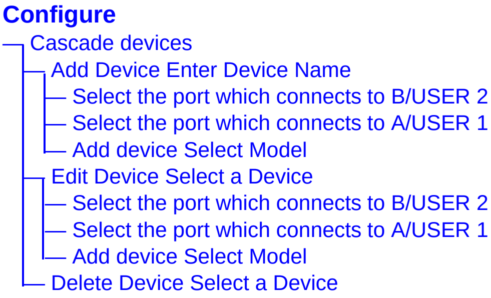

Configure
Cascade devices
Add Device Enter Device Name
Select the port which connects to B/USER 2
Select the port which connects to A/USER 1
Add device Select Model
Edit Device Select a Device
Select the port which connects to B/USER 2
Select the port which connects to A/USER 1
Add device Select Model
Delete Device Select a Device

Figure 7-6: Cascade Devices Configuration Screens

The following table shows the Cascade Devices configuration screens.

Table 7-15: Cascade Devices Configuration Screens

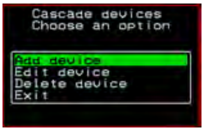
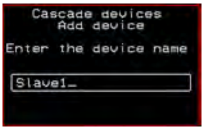
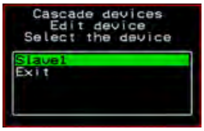
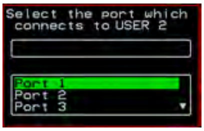
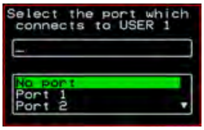
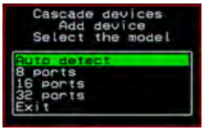
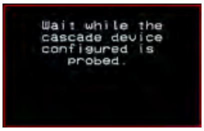
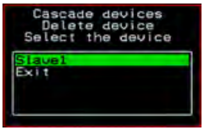
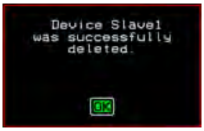
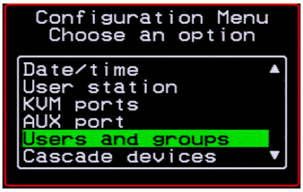
Screen	Description
Cascade device Choose an option  Cascade devices Choose an option Add device Edit device Delete device Exit	Options include Add device, Edit device, and Delete device.
Cascade Device Add DeviceEnter the device name  Cascade devices Add device Enter the device name Slave1_	Appears when Add device is selected from the “Cascade device Choose an option” screen. Enter the name of the new cascaded KVM unit.
Cascade Device Edit DeviceSelect the device  Cascade devices Edit device Select the device Slave1 Exit	Appears when Edit device is selected from the “Cascade device Choose an option” screen. Select the name of a previously added cascaded KVM unit.
Select the port which connects to B/USER 2  Select the port which connects to USER 2 Port 1 Port 2 Port 3	Enter the port number of the master 16-port IP KVM that is connected to the User 2 port of the secondary KVM device. **Note:** See “Connecting Cascaded KVM Units to the Primary 16-port IP KVM” on page 95 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master 16-port IP KVM.

Table 7-15: Cascade Devices Configuration Screens (Continued)

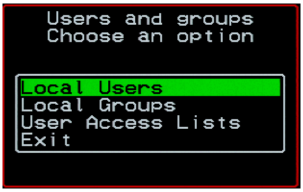
Screen	Description
Select the port which connects to A/USER 1  Select the port which connects to USER 1 _ No port Port 1 Port 2	Enter the secondary KVM port that is connected to the User 1 port of the primary 16-port IP KVM.
Cascade device Add device Select Model  Cascade devices Add device Select the model Auto detect 8 ports 16 ports 32 ports Exit	Select the number of ports on the cascaded KVM unit or select Auto detect and press <Enter>. Selecting Auto detect automatically detects the number of ports on the cascaded KVM unit. The unit must be already connected in order for the auto detect option to work. During auto detection, the following message appears.  Wait while the cascade device configured is probed.
Cascade Devices Delete device Selete the device  Cascade devices Delete device Select the device Slave1 Exit	Appears when Delete device is selected from the "Cascade device Choose an option" screen. The following confirmation screen appears once a cascaded device is selected.  Device Slave1 was successfully deleted. OK

Users and Groups Screens

You can choose the “Users and groups” option from the OSD Configuration menu to configure users, groups, and KVM port permissions.



When you select “Users and Groups,” the “Choose an option” screen appears, as shown in the following screen example. The “Local Users” option is for configuring users; the “Local Groups’ option is for configuring groups, and the “User Access Lists” option is for configuring users’ and groups’ access to KVM ports.



The following diagram lists the configuration screens accessed through the Configure>Users and Groups options:

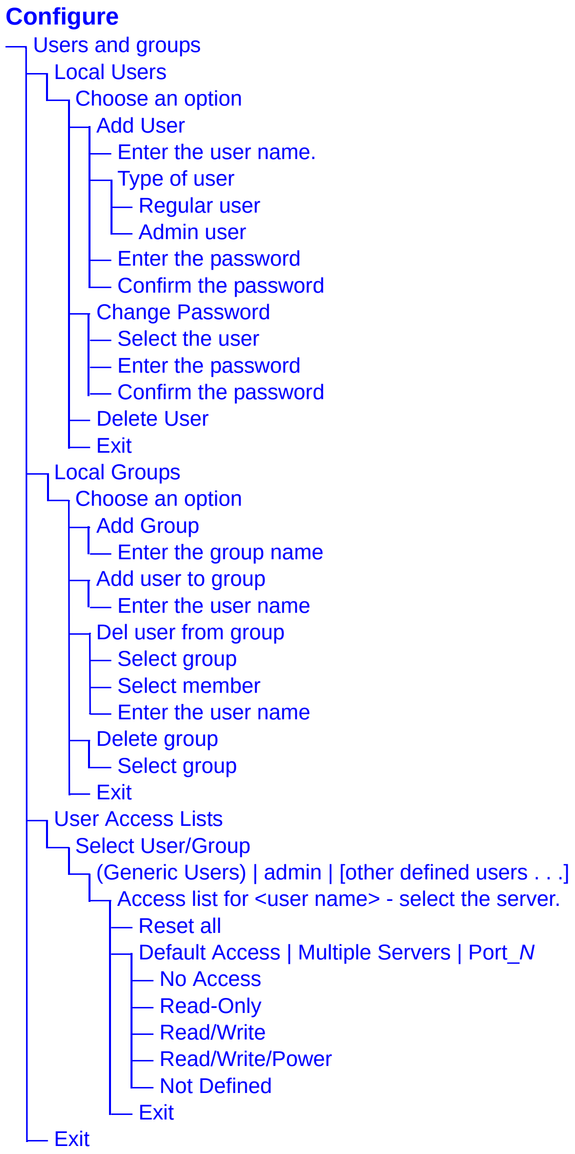


Figure 7-7: Users and Groups Configuration Screens

The following table shows the configuration screens that appear when the “Local Users” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-16: Local Users Configuration Screens

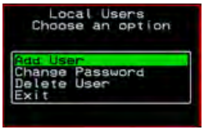
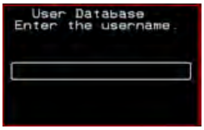
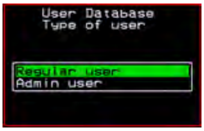
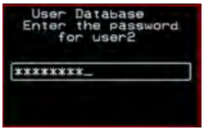
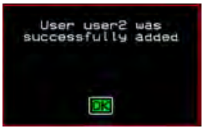
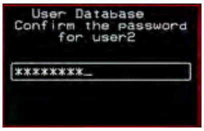
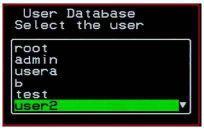
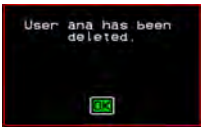
Screen	Description
Choose an option  Local Users Choose an option Add User Change Password Delete User Exit	Options are: “Add User,” “Change Password,” “Delete User,” or “Exit.”
User Database Enter the user name  User Database Enter the username.	Appears only when “Add User” is selected.
Type of user  User Database Type of user Regular user Admin user	Appears only when “Add User” is selected.
Enter the password  User Database Enter the password for user2 ********_	Appears only when “Add User” or “Change Password” are selected. **Note:** Passwords are case sensitive. When the password is successfully confirmed, the following dialog box appears.  User user2 was successfully added OK
Confirm the password  User Database Confirm the password for user2 ********_	

Table 7-16: Local Users Configuration Screens (Continued)

Screen	Description
Select the user  User Database Select the user root admin usera b test user2	Appears only when “Change Password” or “Delete User” are selected. When “Delete User” and then a user name are selected, a confirmation screen like the following appears:  User ana has been deleted. OK

The following table shows the configuration screens that appear when the “Local Groups” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-17: Local Groups Configuration Screens

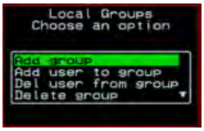
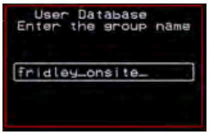
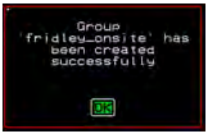
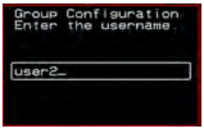
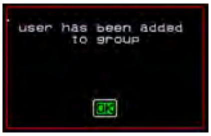
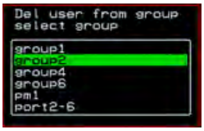
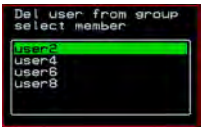
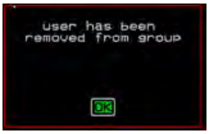
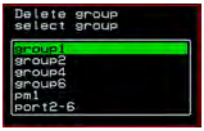
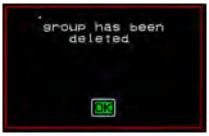
Screen	Description
Choose an option  Local Groups Choose an option Add group Add user to group Del user from group Delete group	Options are “Add group,” “Add user to group,” “Del. user from group,” “Delete group,” and Exit
Enter the group name  User Database Enter the group name fridley_onsite_	When “Add group” is selected. After the group name is entered, a confirmation screen like the following appears.  Group 'fridley_onsite' has been created successfully OK

Table 7-17: Local Groups Configuration Screens (Continued)

Screen	Description
Enter the user name  Group Configuration Enter the username user2_	When “Add user” or “Add user to group” are selected. To add multiple users, use a comma to separate each user name. When the user is successfully added, the following confirmation screen appears.  user has been added to group
Delete user from group select group  Del user from group select group 	When “Del user from group” is selected.
Select member  Del user from group select member 	When “Del user from group” and a user name are selected, the user is removed from the group, and the following confirmation screen appears:  user has been removed from group
Delete group select group  Delete group select group 	When “Delete group” and a group name are selected, the following confirmation screen appears.  group has been deleted

You can use the User Access Lists menu to view and change KVM port access permissions for the Default User and all administratively configured users and groups. See “Prerequisites for Accessing Servers With KVM Connections” on page 258 for details.

The following table shows the configuration screens related to setting KVM port access permissions when the “User Access List” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-18: User Access List KVM Port Permissions Configuration Screens

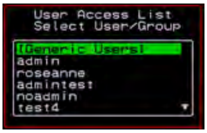
Screen	Description
Select User/Group  User Access List Select User/Group [Generic Users] admin roseanne admintest noadmin test4	“[Generic Users],” “admin,” and any administratively defined users and groups are listed, along with the “Exit” option. The Generic Users’ permissions apply to all users except for “apc” and any users in the “admin” group. By default, the Generic Users’ default permission is “No Access,” and no KVM port permissions are defined. Therefore, by default, any regular users that may be added cannot access any KVM ports. The 16-port IP KVM administrator can configure access to KVM ports for added regular users by: • By selecting “[Generic Users]” and modifying the permissions - OR - • By configuring specific permissions for one or more individual users or groups (by selecting a single port or the “Multiple Servers” option)

Table 7-18: User Access List KVM Port Permissions Configuration Screens

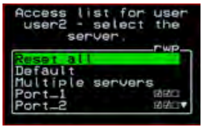
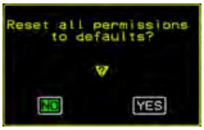
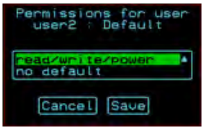
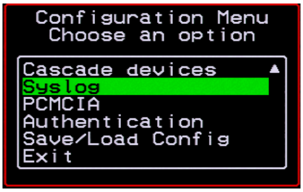
Screen	Description
Access list for user name - select the server  Access list for user user2 - select the server. rwp Reset all Default Multiple servers Port_1 ☑☑□ Port_2 ☑☑□ ▼	The access list includes the “Reset all,” “Default,” “Multiple Servers,” and “Exit” options along with each individual KVM ports. The “Default” option defines access permissions for all KVM ports, which apply unless the user has specific access permissions for any KVM ports. For a new user, because “Default Access,” is not defined, and also because no permissions are specified for that user’s access to any specific port, the Generic Users’ permissions apply. A series of three checkboxes appear to the right of each entry that has specific permissions (as defined in the following row). If a3 port has “No Access” defined, the checkboxes are empty. The headings for the checkboxes are: `rwp` for read, write, and power, and the boxes are checked appropriately when any of these permissions are defined. For example, in the screen to the left, the `r` and `w` boxes are checked next to “Port_1” and “Port_2,” which indicates that the user has read-write access to these ports. If “Reset all” is selected, the following confirmation screen appears.  Reset all permissions to defaults?

Table 7-18: User Access List KVM Port Permissions Configuration Screens

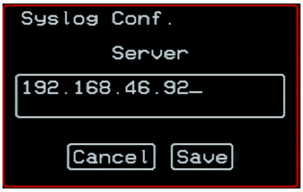
Screen	Description
Permissions for *`user name`* **:***`port_number`* **or for** *`user name`* **: followed by another Access list option, such as "Default" or "Multiple Servers"**  Permissions for user user2 : Default read/write/power no default Cancel Save	The permissions from this menu can be configured to be "Default" permissions for all ports, applied to Multiple Servers, or applied to a selected port. Permissions menu options are "No Access," Read-Only," "Read Write," "Read/Write/Power." When "Default" is selected from the previous menu, the "Not Defined" menu option also appears. When any of the other options

Syslog Screens

You can select the Syslog option on the OSD Configuration Menu to specify the IP address for a syslog server.



Selecting the Configure>Syslog option brings up a Server screen for entering the IP address of a syslog server.



Syslog Conf.

Server

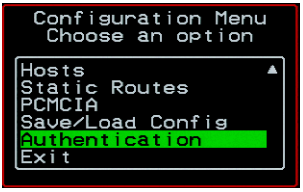
192.168.46.92_

Figure 7-8: Syslog Configuration Server Screen

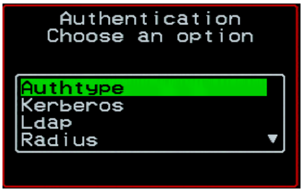
To complete the configuration of system logging, you must specify a facility number as shown in "Syslog Facility" on page 306.

Authentication Screens

You can select the Authentication option on the OSD Configuration Menu to configure an authentication type (AuthType) for logins to the 16-port IP KVM and to configure authentication servers for any type of logins: to the 16-port IP KVM or to KVM ports. See “Authentication” on page 42 for details about authentication on the 16-port IP KVM.



The Authentication menu appears as shown in the following figure.



Not all options are visible.

The following diagram lists the Authentication screens.

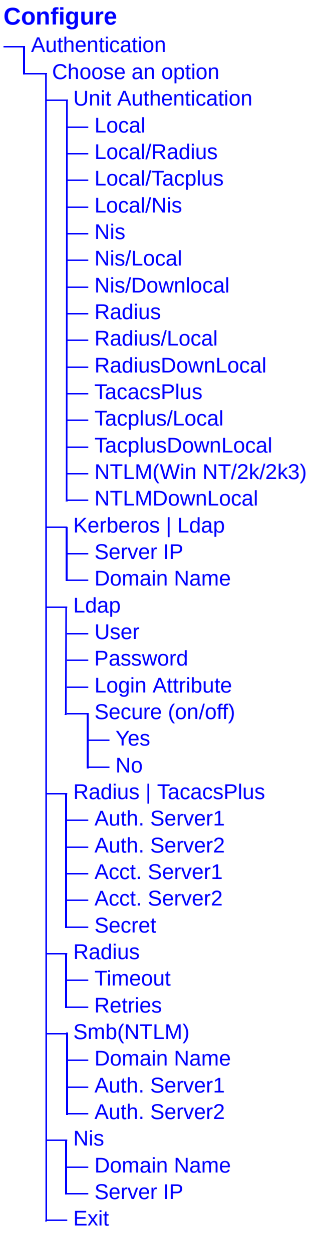
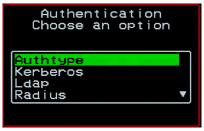
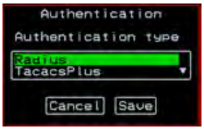


Figure 7-9: Authentication Options and Screens

The following tables show the screens that appear when the “Authentication” option is selected from the Configure menu in the OSD. The first table shows the screen for choosing a 16-port IP KVM login authentication method.

Table 7-19:Authentication Configuration Screens for 16-port IP KVM Logins

Screen	Description
Choose an option  Authentication Choose an option Authtype Kerberos Ldap Radius	Choose either “Unit authentication” to select an Authentication method for 16-port IP KVM logins, or choose one of the Authentication methods listed on this screen to configure an authentication server: Kerberos, Ldap, Radius, TacacsPlus, Smb(NTLM), or Nis.
Authentication type  Authentication Authentication type Radius TacacsPlus Cancel Save	Authentication method options for 16-port IP KVM logins. Default = “Local.” Other authorization type options are: Local/ Radius, Local/Tacplus, Local/Nis, Nis, Nis/Local, Nis/ Downlocal, Radius, Radium/Local, RadiusDownLocal, TacacsPlus, Tacplus/Local, TacplusDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal

The following table shows the common screens that appear when Kerberos or Ldap are selected to configure an authentication server.

Table 7-20:Common Configuration Screens for Kerberos and LDAP Authentication Servers

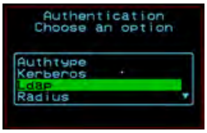
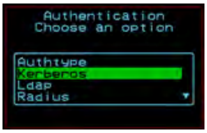
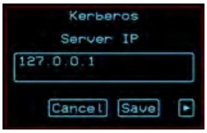
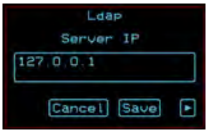
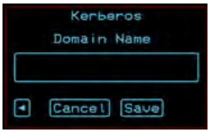
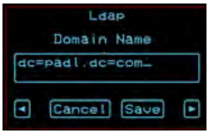
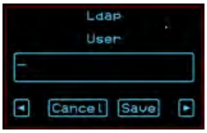
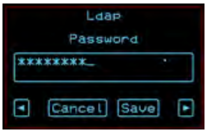
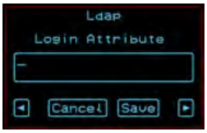
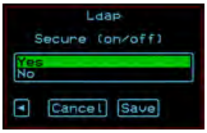
Screen	Description
Ldap  Authentication Choose an option Authtype Kerberos Ldap Radius	Choose Ldap to configure an LDAP authentication server.
Kerberos  Authentication Choose an option Authtype Kerberos Ldap Radius	Choose Kerberos to configure a Kerberos authentication server.

Table 7-20: Common Configuration Screens for Kerberos and LDAP Authentication Servers (Continued)

Screen	Description
Server IP  Kerberos Server IP 127.0.0.1  Ldap Server IP 127.0.0.1 	IP address of the Kerberos or LDAP server.
Domain Name  Kerberos Domain Name  Ldap Domain Name dc=padl.dc=com 	Domain name.

The following table shows the unique screens for configuring an LDAP server that appear in addition to the screens shown in Table 7-20, “Common Configuration Screens for Kerberos and LDAP Authentication Servers,” on page 7-354.The following table shows the configuration screens for the

Table 7-21: Unique LDAP Authentication Server Configuration Screens

Screen	Description
User  	The LDAP user name.
Password  ********_	The LDAP password.
Login Attribute  	The login attribute.
Secure (on/off)  [✓ Yes] No	Choices are “Yes” or “No.”

Radius and TACACS+ authentication servers.The following table shows the

Table 7-22: Configuration Screens for the Radius or TACACS+ Authentication Servers

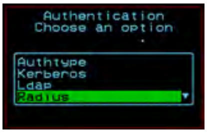
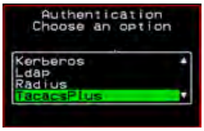
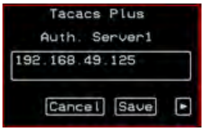
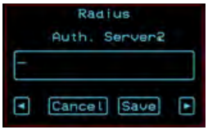
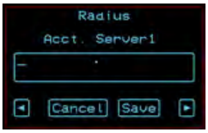
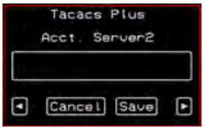
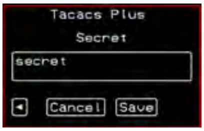
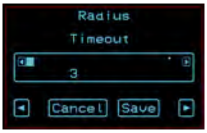
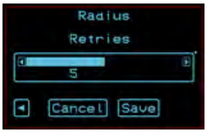
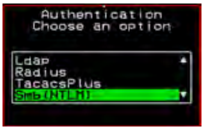
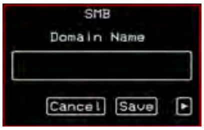
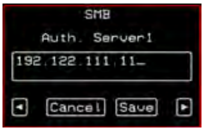
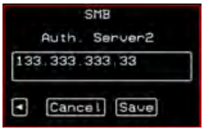
Screen		Description
Radius  Authentication Choose an option Authtype Kerberos Ldap Radius	**TacacsPlus**  Authentication Choose an option Kerberos Ldap Radius TacacsPlus	Choose Radius or TacacsPlus to configure a Radius or TACACS+ authentication server.
Auth. Server1  192.168.49.125	**Auth. Server2**  	IP addresses of one or two authentication servers. The second server is optional.
Acct. Server1 and Acct. Server2  	 	IP addresses of one or two optional accounting servers.
Secret  secret		Shared secret.
Timeout  3		Appears only when Radius is selected. Timeout in seconds. The default is 3.

Table 7-22: Configuration Screens for the Radius or TACACS+ Authentication Servers (Continued)

Screen	Description
Retries  5	Appears only when Radius is selected. Number of retries. The default is 5.

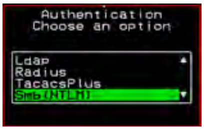
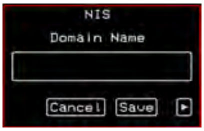
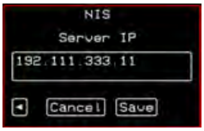
Screens for configuring a Smb (NTLM) authentication server.

Table 7-23: Smb (NTLM) Configuration Screens

Screen	Description
Smb(NTLM)  Authentication Choose an option Ldap Radius TacacsPlus Smb(NTLM)	Choose Smb(NTLM) to configure an SMB (NTLM) authentication server.
Domain Name  	The domain name.
Auth. Server1 and Auth. Server2  192.122.111.11_  133.333.333.33	IP addresses for one or two SMB (NTLM) authentication servers. The second server IP is optional.

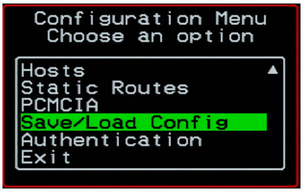
The following table shows the screens for configuring a NIS authentication server.

Table 7-24:NIS Configuration Screens

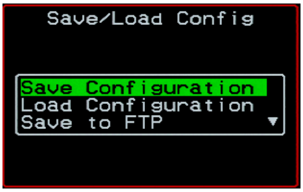
NIS  Authentication Choose an option Ldap Radius TacacsPlus Smb(NTLM)	Choose the NIS authentication server
Domain Name  NIS Domain Name Cancel Save	Enter the Domain Name
Server IP  NIS Server IP 192.111.333.11 Cancel Save	IP address of the NIS server.

Save/Load Configuration Screens

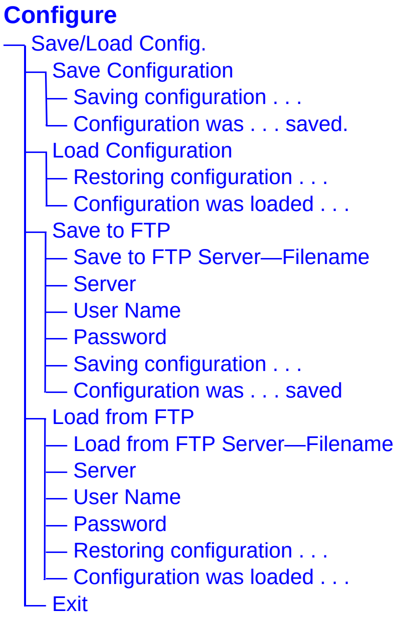
You can use the Save/Load Config option on the OSD Configuration Menu to save any configuration changes you have made since the last save into a backup directory or onto an FTP server. You can also restore configuration file changes from a backup directory or FTP server to overwrite any configuration changes that were made since the last save.



The Save/Load Config screen appears as shown in the following figure. Not all options are visible.



The following diagram lists the Save/Load Configuration screens.



- **Configure**
  - Save/Load Config.
    - Save Configuration
      - Saving configuration . . .
      - Configuration was . . . saved.
    - Load Configuration
      - Restoring configuration . . .
      - Configuration was loaded . . .
    - Save to FTP
      - Save to FTP Server—Filename
      - Server
      - User Name
      - Password
      - Saving configuration . . .
      - Configuration was . . . saved
    - Load from FTP
      - Load from FTP Server—Filename
      - Server
      - User Name
      - Password
      - Restoring configuration . . .
      - Configuration was loaded . . .
    - Exit

Figure 7-10: Save/Load Config Configuration Screens

The following table shows the screens that appear when the “Save/Load Configuration” option is selected from the Configure menu in the OSD.

Table 7-25: Save/Load Configuration Screens

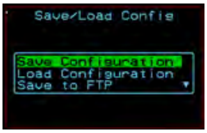
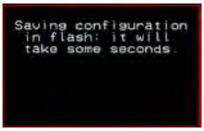
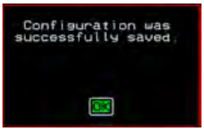
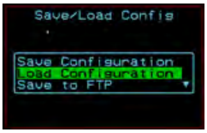
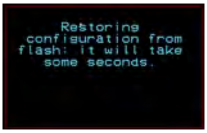
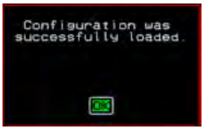
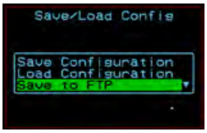
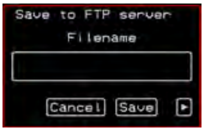
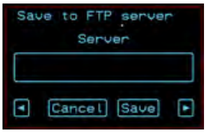
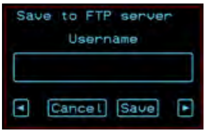
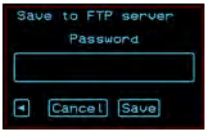
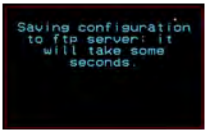
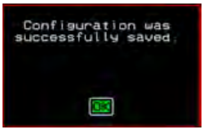
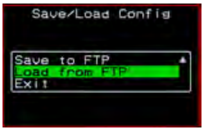
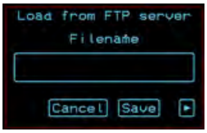
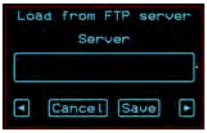
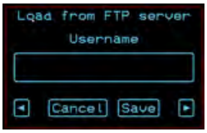
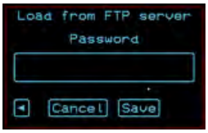
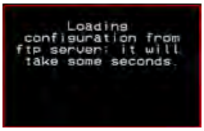
Screen	Description
Save Configuration  Save/Load Config Save Configuration Load Configuration Save to FTP	When “Save Configuration” is selected, the following two screens appear.  Saving configuration in flash: it will take some seconds.  Configuration was successfully saved.

Table 7-25: Save/Load Configuration Screens (Continued)

Screen	Description
Load Configuration  Save/Load Config Save Configuration Load Configuration Save to FTP	When "Load Configuration" is selected, the following two screens appear.  Restoring configuration from flash: it will take some seconds.  Configuration was successfully loaded.
Save to FTP  Save/Load Config Save Configuration Load Configuration Save to FTP	When "Save to FTP" is selected, the following five screens appear for you to enter the "Filename," FTP "Server" name, FTP Login "User Name" and "Password." The last screens confirm the save to FTP succeeded.      Saving configuration to ftp server: it will take some seconds.  Configuration was successfully saved.
Load from FTP  	When "Load from FTP" is selected, the following four screens appear for you to enter the "Filename," FTP "Server" name, FTP Login "User Name" and "Password."      Loading configuration from ftp server: it will take some seconds.

System Info Menu

System Information window provides administrators detailed system information. The following table offers an example of the type of information you may see on the System Info window.

Table 7-26: System Information Example

Information Type	Example
Board	16-port IP KVM Server ports: 16 User stations: 2 ID: B7DA3C0A000011
Version	Firmware: 2.0 Orig. Boot: 2.0.7 Alt. Boot: no code SYS FPGA: 0x43 MUX FPGA: 0x5b
Memory	RAM: 128 Mbytes Flash: 16 Mbytes RAM usage: 17% RAMDISK usage: 100%
CPU	Clock: 48 MHz
Time	Mon Jul 19 2005 12:35:12 PDT up 10 min
User1 connection	Int. uC, V1.0.4

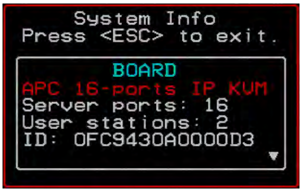
Table 7-26: System Information Example (Continued)

Information Type	Example
User2 connection	Console Extender main V1.0.4 Console Extender local V1.0.4

To Access System Information

1. On the Main Menu, select System Info.

   The System Info window appears.



```
System Info
Press <ESC> to exit.
BOARD
APC 16-ports IP KVM
Server ports: 16
User stations: 2
ID: 0FC9430A0000D3
```

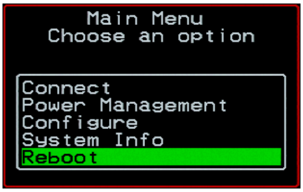
2. Use the up and down arrow keys to view the information.
3. To exit, press the escape key.

Reboot

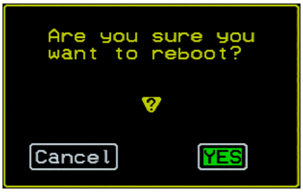
You can reboot the 16-port IP KVM from the Main Menu of the OSD. This is particularly useful when operating through the Console Extender.

To reboot the 16-port IP KVM

1. Select Reboot from the Main Menu.



The following message appears.



Are you sure you want to reboot?

2. Select Yes to reboot the 16-port IP KVM.

Controlling the OSD Through the APC CAT5/IP KVM Console Extender

While using the Console Extender, an administrator has full access to the OSD menus, so all local administration tasks can be performed in an office or at any other location up to 500 feet away from the 16-port IP KVM. In addition, you do not need a dedicated monitor, keyboard, and mouse to use the Console Extender; the Console Extender box allows you to use the monitor, keyboard, and mouse of your regular work station and use keyboard shortcuts to toggle between the view at your local work station and the view of the 16-port IP KVM.

See “Installing the APC CAT5/IP KVM Console Extender” on page 97 for details on how to install an Console Extender. No configuration is required to begin using the Console Extender.

▼ *To Use to the APC CAT5/IP KVM Console Extender to Access the 16-port IP KVM*

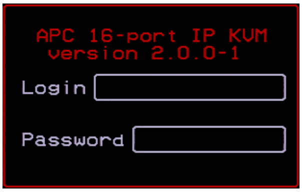
1. Connect the Console Extender to the 16-port IP KVM using a CAT5 cable up to 500 feet long.

   See “Installing the APC CAT5/IP KVM Console Extender” on page 97 for detailed instructions and diagrams on how to connect the Console Extender to the 16-port IP KVM and to your local work station.

2. Power on the Console Extender.

3. Press the Select Local-Remote button on the front of the Console Extender unit to switch the local video display from your local work station to the 16-port IP KVM OSD.

   The OSD login screen appears.



APC 16-port IP KVM
version 2.0.0-1

4. Type your user name followed by your password and press Enter.

The main menu of the 16-port IP KVM OSD appears. See “OSD Main Menu” on page 298 for a description of the OSD Main Menu items.

5. Depending on your access privilege, perform one or more of the following actions:

   - If logged in as administrator, perform configuration tasks as described in “Configure Menu Overview” on page 301, “System Info Menu” on page 363, and “Reboot” on page 364.
   - If desired, connect to devices that are physically connected to the 16-port IP KVM.

     See “Connection Menu” on page 299 for instructions.
   - If desired, power manage devices that are plugged into a configured APC rPDU.

     See “Power Management Menu” on page 300 for instructions.

▼ *To Switch the APC CAT5/IP KVM Console Extender Video Display from the OSD to the Local Computer*

Do one of the following:

- Press the following keyboard shortcut:

  Scroll Lock Scroll Lock L
- Press the Select Local-Remote button on the Console Extender front.

  The green LED labelled Remote turns off, and the green LED labelled Local lights on.

  By default the Console Extender is set to beep when the monitor display switches from local to remote. See “To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations” on page 368 for instructions on turning the beep on or off.

▼ *To Switch the APC CAT5/IP KVM Console Extender Video Display from the Local Computer to the OSD*

Do one of the following:

- Press the following keyboard shortcut:

  Scroll Lock Scroll Lock R

- Press the Select Local-Remote button on the Console Extender front.

  The green LED labelled Local turns off, and the green LED labelled Remote lights on.

  By default the Console Extender is set to beep when the monitor display switches from local to remote. See "To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations" on page 368 for instructions on turning the beep on or off.

▼ *To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations*

- Press the following keyboard shortcut:

  Scroll Lock Scroll Lock B

Glossary

3DES

Tripple Data Encryption Standard, an encrypting algorithm (cipher) that processes each data block three times, using a unique key each time. 3DES is much more difficult to break than straight DES. Because it is the most secure of the DES combinations, 3DES is also slower in performance.

authentication

The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.

basic in/out system (BIOS)

Chips on the motherboard of a computer contain read onlymemory 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

A measurement of processor speed made by the Linux kernel when it boots, to calibrate an internal busy-loop.

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).

bootp

Bootstrap Protocol. A TCP/IP protocol allowing a BOOTP server node to allocate IP addresses to diskless work stations at startup.

CAT5

Category 5. A cabling standard for use on networks at speeds up to 100 Mbits including FDDI and 100base-T. The 5 refers to the number of turns per inch with which the cable is constructed.

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.

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.

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.

escape sequence A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.

An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one capability, and thus need some way to tell data from commands.

Ethernet A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.

Flash Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.

flow control A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.

Hot-Swap Ability to remove and add hardware to a computer system without powering off the system.

IP address

A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals. Each address has a network number, an optional sub network number and a host number. The first two numbers are used for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.

IP packet filtering

This is a set of facilities in network equipment that allows the filtering of data packets based on source/destination addresses, protocol, TCP port number and other parameters. Packet filtering is one of the main functions of a firewall.

IPsec

Short for *IP Security Protocol*, IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as access and trustwothiness control. IPsec provides similar services as SSL, but it works on a network layer. Through IPsec you can create encrypted tunnels (VPN) or encrypt traffic between two hosts.

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. 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.

KVM

Keyboard, video and mouse interface to a server.

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.

network mask

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 (for example, 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.

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.

OSD

On-Screen Display.

packet

A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.

parity

In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.

The following lists the available parity parameters and their meanings:

Odd – Parity bit set so that there is an odd number of 1 bits

Even – Parity bit set so that there is an even number of 1 bits

None – Parity bit is ignored, value is indeterminate

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.

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.

RC4

Rivest Cipher four, an encryption method using variable length secret key streams. RC4 is an alternate to DES and is approximately ten times as fast as DES; however, it is less secure.

SMTP

Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.

SNMP

Short for *Simple Network Management Protocol*, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

(Source: Webopedia)

SNMP Traps

Notifications or Event Reports are occurrences of Events in a Managed system, sent to a list of managers configured to receive Events for that managed system. These Event Reports are called Traps in SNMP. The Traps provide the value of one or more instances of management information.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

The Trap Definition vary with the SNMP Version (which defines the messaging format), but the information contained in these are essentially identical. The major difference between the two message formats is in identifying the events.

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.

Stop Bit

A bit which signals the end of a unit of transmission on a serial line.A stop bit may be transmitted after the end of each byte or character.

Subnet Mask

A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.

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, used by Cisco Systems.

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.

TFTP

Trivial File Transfer Protocol. A simple network application based on User Datagram Protocol (UDP). It is used to transfer files from one computer to another.

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.

VPN

Virtual Private Networking allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.

Watchdog timer

Mechanism to detect hardware and operating system failures.

Index