

AlterPath KVM Manual

*A reference guide for users and systems administrators
of Cyclades AlterPath KVM*

Product Version 1.1.0
Document Revision 3



This document contains proprietary information of Cyclades and is not to be disclosed or used except in accordance with applicable contracts or agreements.

©Cyclades Corporation, 2004

We believe the information in this manual is accurate and reliable. However, we assume no responsibility, financial or otherwise, for any consequences of the use of this product or manual. This manual is published by Cyclades Corporation, which reserves the right to make improvements or changes in the products described in this manual as well as to revise this publication at any time and without notice to any person of such revision or change. All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

Cyclades AlterPath KVM, AlterPath KVM Terminator, and AlterPath KVM RP are registered trademarks of Cyclades Corporation.

Microsoft, Windows 95, 98, XP, ME, NT, and 2K are trademarks of Microsoft Corporation.

UNIX is a trademark of UNIX System Laboratories, Inc.

Linux is a registered trademark of Linus Torvalds.

For the latest manual revisions, please refer to Cyclades website on:

<http://www.cyclades.com/support/downloads.php>

All rights reserved. This document may not, in whole or part, be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form without the prior written consent of Cyclades Corporation, 41829 Albrae Street, Fremont, CA 94538, USA. Telephone (510) 771-6100. Fax (510) 771-6200. www.cyclades.com.

Table of Contents

Before You Begin

Audience	i
Document Organization	i
Typographical Conventions	ii
Naming Conventions	ii
Symbols	iii

Chapter 1: Introduction

Connectivity and Capacity	1-1
Product Components	1-2
KVM Terminator	1-3
Overview of AlterPath KVM	1-3
KVM Product Features	1-4
Cat-5-Based Cabling	1-4
Server-Based Authentication	1-4
Local User Authentication	1-5
User Access Lists Per Port	1-5
Cascading Support with Centralized Port Management	1-5
Flexibility and Scalability	1-5
On-Screen Display Capability	1-5
Mouse Support	1-5
Multi-User	1-6
Fan Monitoring	1-6
Event Logging Capabilities	1-6
The Linux Advantage	1-6
Rack Space Convenience	1-6
Setup Diagram	1-7

Chapter 2: KVM Installation

Product Installation Checklist	2-1
Port Connections	2-3
Rack Mounting the KVM	2-3
Installing AlterPath KVM	2-4
Booting Messages	2-6
Cascading AlterPath KVM	2-7
Connecting a Secondary KVM to a Primary KVM	2-8
Mouse Settings	2-8
Windows XP / Windows 2003	2-8
Windows 2000 / ME	2-9
Windows 95 / 98 / NT	2-9
Linux with Graphical Desktop	2-9
Safety Considerations When Rack Mounting	2-10
Activity LEDs on the KVM Ports	2-11
LED Functions	2-11
LED Status Definitions	2-12

Chapter 3: KVM OSD Configuration

OSD and Web Configuration	3-1
Configuring the KVM through the OSD	3-2
Basic Navigation Keys	3-2
Default Key Sequences	3-2
KVM User Interface Overview	3-4
Logging In	3-5
OSD Guidelines	3-5
Saving Your Configuration	3-5
KVM Main Menu	3-6
Configuration Menu	3-7
General Configuration: Windows Summary	3-8
Authentication Type	3-8
Syslog Facility	3-9
Escape Sequence	3-10

Sun Keyboard	3-10
Network Configuration	3-11
DHCP	3-11
IP Address	3-11
Netmask	3-12
Gateway	3-12
DNS Server	3-13
Domain	3-13
Hostname	3-14
Date/Time	3-14
Enabling the NTP Server	3-15
User Station Configuration	3-17
Idle Timeout	3-17
Screen Saver Time	3-18
Cycle Time	3-18
Keyboard Type	3-19
Power Management	3-20
Mouse/Keyboard Sync	3-21
Video Configuration	3-21
Switch Next	3-22
Switch Previous	3-22
Port Info	3-23
KVM Ports	3-23
Selecting a KVM Port to Configure	3-23
Activating a Port	3-24
Server Name	3-25
Power Outlet	3-26
Configuring a Server Connected to a Slave	3-26
Users and Groups	3-27
Configuring Users	3-28
Adding a User	3-28
Changing the User, Admin, or	
Root Password	3-30
Deleting a User	3-32

Table of Contents

Local Groups	3-33
Adding a Group	3-33
Adding a User to a Group	3-35
Deleting a User from a Group	3-36
Deleting a Group	3-38
User Access Lists Menu	3-39
Generic User	3-39
Adding a User to the User Access List	3-40
Edit User/Group	3-42
Deleting a User from the User Access List	3-44
Cascade Devices	3-45
Cascade Devices Menu	3-45
Adding a Secondary Device	3-45
Syslog	3-48
Save/Load Config	3-49
Saving Your Configuration	3-49
Loading Your Configuration	3-50
Saving your Configuration to an FTP Server	3-51
Loading Configuration from an FTP Server	3-53
System Info Menu	3-55
System Info Window	3-56
Reboot	3-57

Chapter 4: KVM Web Configuration

Overview	4-1
Types of Users	4-2
Root User	4-2
Admin User	4-2
Generic User	4-2
Changing the Password	4-3
Hierarchy of Permissions	4-3

Logging In	4-4
Direct Access to a Port	4-5
KVM Web Management Interface	4-6
Wizard Mode	4-6
Expert Mode	4-7
Button Functions	4-8
Saving Your Configuration	4-8
Configuring in Wizard Mode	4-9
Step 1: Network Settings	4-9
Step 2: Access	4-11
Step 3: System Log	4-14
Configuring in Expert Mode	4-15
Table of Menu and Forms	4-16
Access	4-18
Power Management	4-18
Power Management > Outlets Manager	4-19
Power Management > View IPDUs Info	4-21
Power Management > Users Manager	4-22
Power Management > Configuration	4-24
Power Management > Software Upgrade	4-25
Configuration	4-26
KVM	4-26
Default Key Sequences	4-27
Configuring the TCP Viewer Ports Address	4-31
Devices	4-32
Users & Groups	4-37
Security	4-41
Network	4-42
Network > Host Settings	4-43
Network > Syslog	4-45
Network > Services	4-46
Network > IP Filtering	4-47
Network > VPN	4-55

Table of Contents

Network > SNMP	4-59
Network > Host Table	4-63
Network > Static Routes	4-64
AUX Port	4-66
System	4-68
System > Date/Time	4-68
System > Boot	4-69
Information	4-71
General	4-71
Port Status	4-74
Management	4-74
Backup Configuration	4-75
Firmware Update	4-76
Microcode Update	4-77
Microcode Reset	4-78
Active Sessions	4-79
Reboot	4-80

Chapter 5: KVM Operation

Basic Navigation Keys	5-1
Default Key Sequences	5-2
Changing the Root Password	5-3
Logging In	5-4
Connecting to a Server	5-5
Using the Search Box	5-6
Successful / Unsuccessful Connection	5-6
Cycling Between Servers	5-7
Cycle by Server	5-7
Cycle by Key Sequence	5-8
Remote Operation	5-9
Operating through the Remote Unit (RP)	5-9
Finishing your Session	5-10
Method 1: Exiting through the Main Menu	5-10
Method 2: Exiting by using the	

escape sequence	5-10
Method 3: Exiting by Idle Timeout	5-11
OSD Screen Saver	5-11
Operating through the Remote Unit (RP)	5-11
Adjusting Screen Brightness and Contrast	5-12
Automatic (Video) Control Adjustment	5-12
Manual (Brightness/Contrast) Control	5-13
Sharing Server Connection	5-13
Synchronizing Your Keyboard and Mouse	5-15
Establishing a Power Control Session	5-16
Logging Events	5-16
KVM Web Operation	5-17
Connecting to a Server	5-17
Power Management	5-18
Access > Power management > Outlets Manager	5-18

Appendix A: <i>Technical Specifications</i>	
Appendix B: <i>KVM Remote Authentication</i>	
Glossary	

This page has been intentionally left blank.

Before You Begin

Welcome to the AlterPath KVM Manual! This manual is designed to help you install, configure, and operate your AlterPath KVM switch.

For simplicity, the document also refers to the Alterpath KVM unit as *KVM*.

Audience

This manual is intended for System administrators and regular users of the AlterPath KVM. At a minimum, the regular user must understand the basics of using a graphical user interface such as Microsoft Windows.

Document Organization

The document is organized as follows:

1: Introduction	Defines and explains the overall product features and uses of the KVM.
2: KVM Installation	Explains the procedure for installing and setting up the KVM.
3: KVM OSD Configuration	Explains the procedures for configuring the KVM switch, its devices, interfaces, connections, and users using the on-screen display (OSD).
4: KVM Web Configuration	Explains the procedures for configuring the KVM switch, its devices, interfaces, connections, and users using the web management interface.
5: KVM Operation	Presents the procedures for connecting to a port and other operations related to using the web user interface.
Appendix A:	Technical Specifications
Appendix B	KVM Remote Authentication

Glossary

This is a glossary of terms and acronyms used in the manual.

Typographical Conventions

Screen Labels

Words that appears on the screen are typed in **boldface**.

Examples: The **Configuration** window; the **Password** field.

Hypertext Links

With the exception of headings and the Table of Contents (which are already linked), all underlined words are hypertext links.

Screen Levels

Screen levels are indicated by the “greater than” symbol (>), starting from parent to child to grandchild and so forth.

Example: Main Menu > Configure > User Configuration

Important words

Certain words are *italicized* for emphasis.

Naming Conventions

Forms

The user input screens of the web management interface is referred to as *forms*.

Window

The KVM online-screen display (OSD) uses for its graphical user interface (GUI) similarly sized windows designed to provide users a means to enter commands to the system.

Window Names

Some windows do not have titles or unique titles. While a name used to refer to a window may not appear on the window itself, the assigned name are designed to describe the purpose of the window, and to better distinguish every window.

KVM	Short name for the AlterPath KVM.
Select	To <i>select</i> is the same as to <i>click your mouse</i> .

Symbols

The manual uses three symbols to indicate the following:



This icon indicates a reference to another section, chapter, or document.



This icon indicates a note or comment.



This icon indicates a warning.

This page has been intentionally left blank.

Chapter 1

Introduction

Cyclades AlterPath™ KVM is a family of CAT5-based keyboard-video-mouse switches designed to provide you an easy and secure way to manage remote servers from a desktop unit. KVM provides you full access and control of GUI-based servers (*e.g.*, Windows NT or Windows Server 2003) through a dedicated channel or over the network.



*For simplicity, **AlterPath KVM** is also referred to in the manual as **KVM**.*

The flexibility of CAT5 cabling (supporting distances of up to 500 feet between the switch and the managed servers) enables KVM to use any data center's existing cabling infrastructure and provide for an easy installation.

The security features of KVM allow integration with existing security infrastructure such as RADIUS, TACACS+, LDAP, and Kerberos. Token-based strong authentication methods such as SecurID are also supported. As a backup, the KVM provides local authentication should any of the authentication servers fail.

The AlterPath KVM supports cascading, a feature which allows you to connect other KVM switches as secondary units connected to a primary KVM. Cascading allows data center managers to centralize port management and expand their coverage as the data center grows.

Connectivity and Capacity

KVM supports two concurrent users: one remote and one local.

Through cascading, AlterPath KVM allows you to control up to 1024 computers. For one primary AlterPath KVM 16, you can connect up to eight secondary KVM units; and for one AlterPath KVM32, up to 16 secondary KVM units. Two connections are used for each secondary-to-primary configuration to allow two simultaneous users. One CAT-5 cable between a primary port to a secondary USER 2 port and another CAT-5 cable between a primary port and a USER 1 port through a terminator.

Product Components

AlterPath KVM family comprises four product components:

- AlterPath KVM 16 - model that comes with 16 KVM ports.
- AlterPath KVM 32 - model that comes with 32 KVM ports.
- AlterPath KVM RP - allows a remote user to connect to the KVM.
- AlterPath KVM Terminator - interfaces the console keyboard, video and mouse to the KVM.



Figure 1.1 - AlterPath KVM: Front View



Figure 1.2 - AlterPath KVM 32: Back View



Figure 1.3 - AlterPath KVM Product Suite
(From bottom: KVM, front; KVM32, back; KVM RP; KVM Terminator.)

KVM Terminator

The AlterPath KVM terminator interfaces directly with the server through the video, mouse, and keyboard ports. It behaves as though it were a real keyboard, mouse, and monitor.

The KVM terminator comes in three models to support the following:

- PC mini DIN
- PC USB
- Sun USB

Overview of AlterPath KVM

The AlterPath KVM operates by using the keyboard, video, and mouse as the low-level access interfaces to the managed servers, which allows you to access server information that is otherwise inaccessible through in-band network interfaces.

For example, BIOS access, POST, and boot messages are inaccessible through in-band network management tools. In some cases, the in-band network interfaces are not available even after the system boot is completed (*e.g.*, after a Windows Safe Mode boot) which makes the KVM the only way to manage remote GUI-based servers.

The KVM offers advanced options to meet the most demanding user requirements. Cascading support, CAT5-based cabling for up to 500 feet of distance and integration with other server management devices such as the AlterPath PM IPDUs make the AlterPath™ KVM a powerful addition to any data center.

KVM Product Features

AlterPath KVM provides enterprise solutions that meet the needs of today's data center. The most notable features of AlterPath KVM are:

- CAT5-based cabling
- Server-Based Authentication
- Local User Authentication
- User Access List Per Port
- Cascading Support with Centralized Port Management
- Flexibility and Scalability
- Online Screen Display
- Mouse Support
- Multi-User
- Event Logging
- Fan Monitoring
- Rack Space Savings

Cat-5-Based Cabling

CAT-5-based cabling allows for a clean cabling setup and access to servers located far away from the AlterPath KVM switch. CAT-5 cabling allows you to use existing cabling infrastructure in the data center. Setup is quick and simple. The KVM supports distances up to 500 feet between the switch and the managed servers, which makes even the most remote server in the data center reachable by the AlterPath KVM.

Server-Based Authentication

The AlterPath KVM's support for existing security infrastructure and token-based strong authentication methods allows it to provide a high level of security and adapt to your current security policies and infrastructure.

For example, in large data centers with hundreds of KVM switches that support user authentication using locally-stored passwords, each time a new user is created or removed, the system administrator has to manually reconfigure each device. Security is compromised if he forgets or misconfigures any device. With server-based authentication, the administrator updates a single centralized database and all access devices consult that database using a server-based authentication method such as Radius or LDAP.

Local User Authentication

AlterPath KVM also supports local backup user authentication, allowing the system to fall back to local authentication mode in case your server-based authentication engine is unreachable. This ensures continuous, secured access to your servers even if the network or the authentication server is down.

User Access Lists Per Port

This feature allows you to define which users have access to which servers, which provides greater control and peace of mind.

Cascading Support with Centralized Port Management

You can have multiple AlterPath KVM switches cascaded to provide higher port density, yet they will behave as one single, larger, KVM switch. This means that you can configure the entire KVM switch chain from a single point (the primary unit). Once it is ready, the configuration is broadcasted to all the units in the chain, which simplifies the configuration process.

User authentication and access follows the same approach, which means you authenticate only once and choose the server you want to access from a single list, and the AlterPath KVM chain will automatically connect you to the proper server.

Flexibility and Scalability

Cascading support with centralized port management allows the AlterPath KVM to increase the number of managed servers without losing the initial investment, or the advantage of a centralized configuration and access interface. As the data center grows, managers and system administrators have greater control, and greater ability to expand their coverage.

On-Screen Display Capability

You can use the on-screen display to control your AlterPath KVM easily. From the OSD, you can perform tasks such as navigating through the servers, cycling servers, and more.

Mouse Support

AlterPath KVM supports the popular PS/2 mouse interface, as well as USB mouse and keyboard.

Multi-User

KVM supports two concurrent users; one local and one remote. The remote user may be placed up to 500 feet away from the KVM unit. The KVM RP enables the remote operator to select the local keyboard, video, and mouse console between a local station and a server from the AlterPath KVM.

Fan Monitoring

The KVM is designed with a circuit that senses and monitors the fan speed. If configured, when the fan stops, an alarm message is sent to the syslog server and the OSD screen.

Event Logging Capabilities

The AlterPath KVM provides event logging capabilities that allows your organization to audit its usage and identify who accessed which KVM ports at what time and date. This helps your organization track how server issues are being handled by system administrators and analyze problem-solving policies for future improvement.

The Linux Advantage

Instead of using proprietary software technologies, KVM leverages on Open Source software (Linux), which gives users the freedom to customize its operation, to modify or add features.

Rack Space Convenience

Available in 16 and 32-port models that fit in 1U of rack space, KVM helps maximize server availability with scalability and security. Using KVM for server management decreases network maintenance costs while increasing efficiency and productivity.

Setup Diagram

The diagram below shows a typical setup of the various KVM product components.

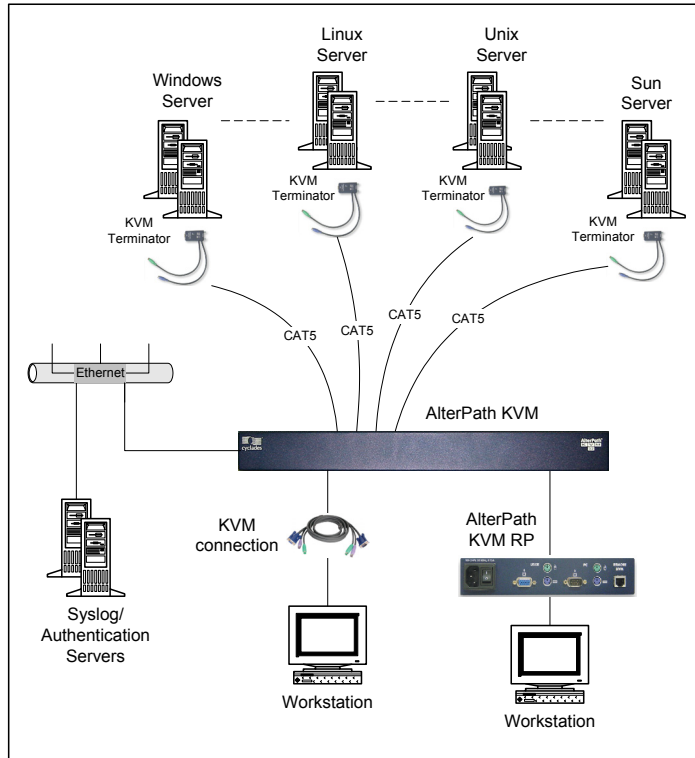


Figure 1.4 - AlterPath KVM Setup

This page has been intentionally left blank.

Chapter 2

KVM Installation

This section discusses the procedures and requirements for installing the AlterPath KVM, and is organized as follows:

- Product Installation Checklist
- Rack Mounting and Connecting the KVM Components
- Installing AlterPath KVM
- Cascading AlterPath KVM

Product Installation Checklist

While the quantity of the product components may vary based on your order, at a minimum, your AlterPath KVM package should contain the following items:

- 1 AlterPath KVM
- AlterPath KVM Terminators¹
- 1 RJ-45 straight-through cable
- 1 RJ-45 to DB-9F crossover adapter
- 1 power cable
- 1 mounting kit
- 1 Manual
- 1 Quick Start Guide

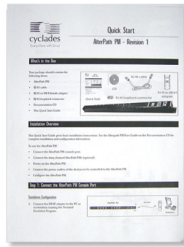
Your AlterPath KVM RP should contain the following items:

- 1 AlterPath KVM RP
- 1 RJ-45 straight-through cable
- 1 power cable
- 1 KVM cable
- 1 Quick Start Guide

1. This item is only included based on the customer's need.

2: AlterPath KVM Installation

The contents of a typical AlterPath KVM package is shown below:
(Power cord and mounting kit not shown.)



**Manual
& QuickStart Guide**



CD



RJ-45 cable



**RJ-45 to
DB-9F adapter**

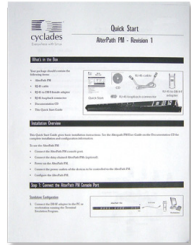


AlterPath™ KVM

KVM Terminator



The contents of a typical AlterPath KVM RP package is shown below:



**QuickStart
Guide**



RJ-45 cable



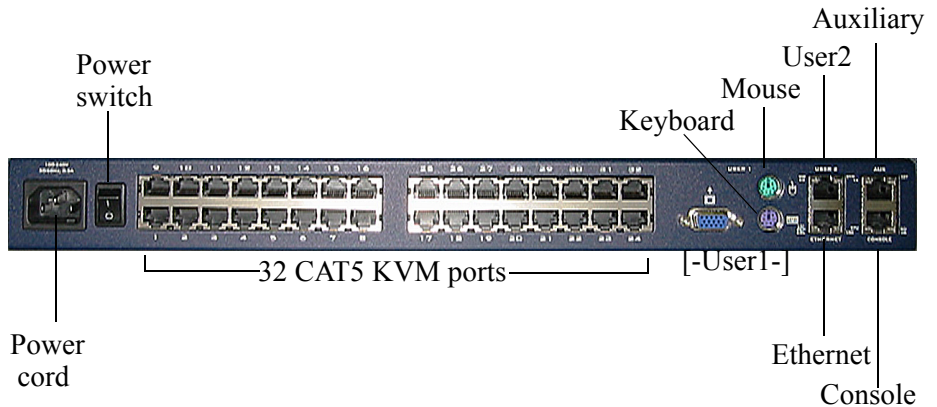
KVM cable



AlterPath™ RP

Port Connections

The diagram below shows the port connections located in the back of a KVM 32:



Rack Mounting the KVM

To rack-mount the KVM, perform the following steps:

1. Install the brackets onto the front corners of the box using a screw driver and the screws and bolts provided with the mounting kit.



2. Mount the KVM unit in a secure position.
Refer to the **Safety Considerations When Rack Mounting** section of this chapter to ensure safety.

Installing AlterPath KVM



While the KVM and its components are hot-pluggable, be aware that other non-Cyclades system components, such as the PS/2 keyboard and mouse ports on the server, may not respond properly when hot-plugged. When in doubt, power on your servers only after the KVM and its components are installed properly.

To install the AlterPath KVM, follow the procedure below:

1. Connect computers to the AlterPath KVM.
 - a. Select the appropriate KVM Terminator for the computer to be connected. Three Terminator types are available: PS/2, USB, and Sun.
 - b. Plug the selected Terminator to the matching Keyboard, Video and Mouse ports on the computer.



When connecting the terminator for the PC mini-DIN, you must first connect the mouse, then the video, then the keyboard, before connecting the RJ-45 straight-through CAT-5 cable.



Note the differences in cabling between the terminator types:

Terminator Type	Connection
PS/2, Sun-DIN	keyboard, video, mouse
Sun-USB, PC-USB	video, USB

- c. Repeat steps a and b for all computers to be connected.
 - d. Plug RJ-45 straight cables from each terminator to the CAT5 ports on the AlterPath KVM.
2. Connect a local user station to the AlterPath KVM.
 - a. Plug your station's Keyboard, Video and Mouse cables to the Keyboard, Video and Mouse **USER 1** connectors on your AlterPath KVM.
3. *Optional.* Connect the Remote Point Unit (RP) to the AlterPath KVM.
 - a. If you are not using an AlterPath KVM RP, skip this and proceed to step 4.
 - b. Make sure the AlterPath KVM, the AlterPath KVM RP, and all connected computers are powered down.

- c. Plug your Keyboard, Video and Mouse cables to the Keyboard, Video and Mouse User ports on your AlterPath KVM RP.
 - d. Plug your station's Keyboard, Video and Mouse cables to the Keyboard, Video and Mouse Local PC connectors on your AlterPath KVM RP.
 - e. Connect an RJ-45 straight cable from the REMOTE KVM port on the AlterPath KVM RP to the **USER 2** connector at the AlterPath KVM.
4. Power on your AlterPath KVM.
 - a. Connect the AC power cable of the AlterPath KVM to the power connector of the unit. Make sure the power switch is off.
 - b. Plug the other end of the cable to an AC wall power outlet.
 - c. Power on your AlterPath KVM by turning its power switch on.
 5. *Optional.* Power on your AlterPath KVM RP.



If you have a remote station connected to your AlterPath KVM RP, power will be driven from the Keyboard interface on your remote station, and thus you can skip this step.

- a. Connect the AC power cable of the AlterPath KVM RP to the power connector of the unit. Make sure the power switch is off.
 - b. Plug the other end of the cable to an AC wall power outlet.
 - c. Power on your AlterPath KVM RP by turning its power switch on.
6. Power on the connected computers and proceed to Chapter 3: AlterPath KVM Configuration.

Booting Messages

During the booting process, the system will display a succession of messages shown as follows:

```
Cyclades Corporation  
AlterPath-KUM Boot
```

```
Cyclades Corporation  
AlterPath-KUM Boot  
Loading RAMDISK.
```

```
Cyclades Corporation  
AlterPath-KUM Boot  
Running init.
```


Connecting a Secondary KVM to a Primary KVM

The procedure for connecting a secondary KVM to a primary KVM is as follows:

1. Ensure that all hardware (KVM switches and computers) to be connected are switched off.
2. Connect a CAT-5 cable from a primary KVM port to the **USER2** (for remote station) port of the secondary KVM.
3. Connect a KVM Terminator to the **USER1** (for local station) port of the secondary KVM.
4. Connect CAT5 cable from a primary KVM port to the KVM Terminator connected to the secondary KVM **USER1** port.
5. Repeat steps 1 through 4 for each secondary KVM to be connected to the primary KVM.



*In the KVM Expander, **User 1** is **User A**; **User 2** is **User B**.*

Mouse Settings

For optimal mouse performance, ensure that your mouse pointer acceleration and related enhancement features are disabled. This ensures that your mouse is synchronized with the server's mouse. To verify or configure your mouse settings, follow the procedure below:

Windows XP / Windows 2003

1. Go to: Settings > Control Panel > Mouse > Pointer Options
2. Disable *Enhance pointer precision*.
3. Set the motion speed to medium by positioning the slider right at the middle.
4. Go to: Settings > Control Panel > Display > Effects
5. Disable transition effects.

Windows 2000 / ME

1. Go to: Control Panel > Mouse > Pointer Options
2. Set the mouse pointer acceleration to **none**.
3. Set the motion speed to medium by positioning the slider right at the middle.
4. Go to: Control Panel > Display > Effect
5. Disable transition effects.

Windows 95 / 98 / NT

1. Go to: Control Panel > Mouse > Motion
2. Set the motion speed to the lowest setting.
3. Go to: Control Panel > Display > Effects
4. Disable window, menu, and list animation.

Linux with Graphical Desktop

1. Set mouse acceleration to: 1
2. Set threshold to: 1

You can also disable the mouse pointer acceleration setting by using the XSET command:

```
> xset m 0
```

Or reset the acceleration or threshold as follows:

```
> xset m 1 1
```

- OR -

```
> xset m 1 10
```

All servers work with any of the above settings, albeit each system may vary slightly.

Safety Considerations When Rack Mounting

When rack-mounting the KVM box, consider the following:

Operating Temperature

Cyclades's recommended operating temperature range for the KVM is: 50° to 112°F (10°C to 44°C).

Elevated operating ambient temperature

If you install the KVM in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Ensure that you install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Reduced air flow

Ensure that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Ensure that the equipment is mounted or loaded evenly to prevent a potentially hazardous condition.

Circuit loading

Ensure that the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Check the equipment nameplate ratings to address this concern.

Reliable Earthing

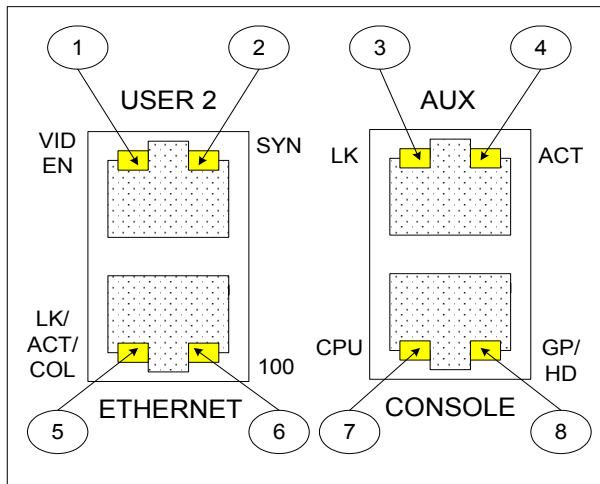
Maintain reliable earthing of rack mounted equipment by inspecting supply connections other than direct connections to the branch circuit such as power strips or extension cords.

Activity LEDs on the KVM Ports

The KVM unit comes with LEDs positioned on each side of the following ports:

- User 2
- Aux
- Ethernet
- Console

The LEDs are designed to monitor the interface connections as described in the succeeding LED tables. The diagram below shows the position of the LEDs as they appear on the back of the KVM/net switch:



LED Functions

The LED numbers in the tables below correspond to the bubbled numbers in the previous diagram.

LED No.	Function
1 and 2	Monitor KVM CAT5 video output interface.
3 and 4	Monitor async interface.
5 and 6	Monitor Ethernet RJ-45 connector signals.
7	Monitors CPU control.
8	Monitors HD control.

LED Status Definitions

<i>LED No.</i>	<i>Label</i>	<i>Color</i>	<i>Status</i>
1	VID EN	Off	Video disabled.
1	VID EN	Green	Video enabled pass through
1	VID EN	Orange	Video enabled internal blank screen generated.
2	SYN	Off	No input channel signal.
2	SYN	Green	Input channel signal level detected and synchronized.
2	SYN	Orange	Input channel signal level detected but NOT synchronized.
3	LK	Orange	DTR active.
4	ACT	Green	RX or TX activity.
5	LK/ACT/COL	Green	Link/Activity.
5	LK/ACT/COL	Orange	Collision.
6	100	Green	Speed 100.
6	100	Off/Orange	Speed 10.
7	CPU	Green	CPU control active.
8	GP/HD	Green	Inactive
8	GP/HD	Orange	Active

Chapter 3

KVM OSD Configuration

This chapter discusses the procedures and requirements for configuring the AlterPath KVM through the on-screen display (OSD), and is organized as follows:

- Configuring the KVM through the OSD
 - Basic Navigation Keys
 - Default Key Sequences
 - KVM User Interface Overview
 - Procedure for using each menu selection
 - Saving your configuration
 - Web Management Interface
- Configuring through the WMI
 - Logging In
 - Running and Saving your Configuration
 - General Configuration
 - Syslog and SNMP
 - KVM General
 - KVM Slaves
 - KVM Servers
 - KVM Users
 - Microcontroller Firmware Upgrade
 - Users and Groups

OSD and Web Configuration

There are two types of graphical interface that you can use to configure the AlterPath KVM:

- On Screen Display (OSD)
- Web Management Interface (WMI)

Configuring the KVM through the OSD

Basic Navigation Keys

A short list of keyboard controls to help you navigate through the KVM on screen display is as follows:

<i>Key</i>	<i>Action</i>
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 / Commit changes

For the keys to work, make sure that your window is selected so that it is in the *active* state.

Default Key Sequences

A *key sequence* (also known as *escape sequence*) is a sequence of special characters used to send a command to a device or program, in this case the KVM application. Typically, an escape sequence begins with an escape character, but this is not universally true.

In KVM, the default key sequence (Ctrl-K, Q) for closing a window (without saving any changes made) while connected to a port is also called *escape sequence*.

Aside from the navigation keys listed above, you can use the following default key sequences to perform a specific action:

<i>Key Sequence</i>	<i>Action</i>
<Ctrl-K>, and then <Q>	Quit command - closes the port session and takes you back to the KVM Main Menu.
<Ctrl-K>, and then <P>	Port command - initiates a power control session.
<Scroll Lock> twice, and then <L>	RP Switch to Local command - switches the Alter-Path KVM RP video display to the local computer.

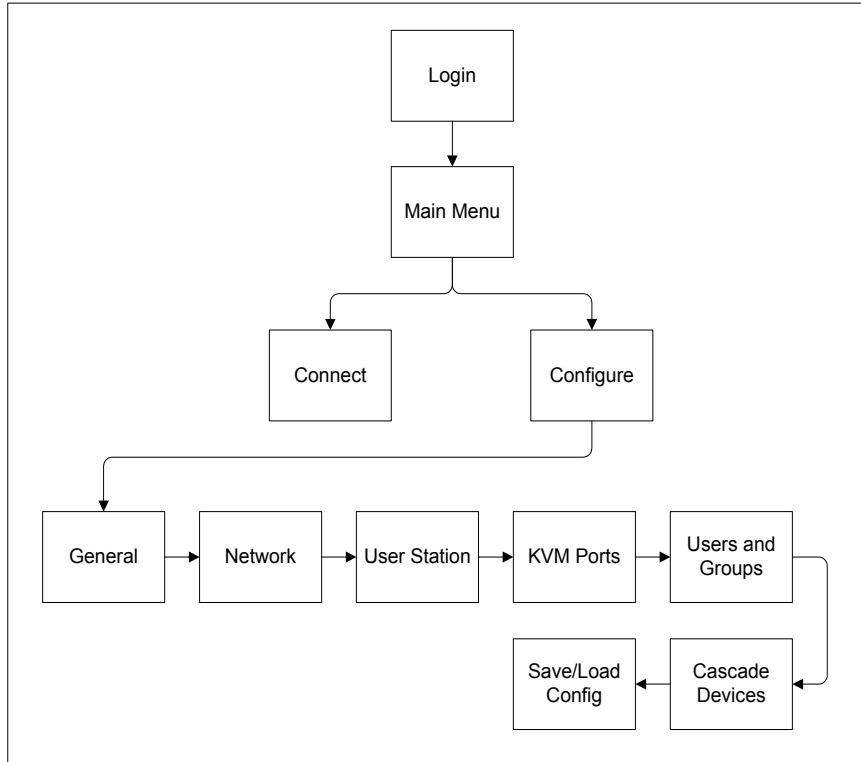
<i>Key Sequence</i>	<i>Action</i>
<Scroll Lock> twice, and then <R>	RP Switch to Remote command - switches the Alter-Path KVM RP video display to the remote computer.
<Scroll Lock> twice, and then 	RP Beep On/Off - switches the beeper on or off when switching between devices (local-remote).
<Ctrl-K>, and then <. >	Next Port command - switches from the currently connected port to your next authorized port.
<Ctrl-K>, and then <, >	Previous Port command - switches from the current port to the previous port.
<Ctrl-K>, and then <V>	Video command - controls screen brightness and contrast.
<Ctrl-K>, and then <S>	Keyboard & Mouse Synchronization command - resets the keyboard and mouse synchronization if either of these becomes unavailable after adding a new server to the KVM.

With the exception of the RP Switch commands, you can change or modify the key sequences in the User Configuration (Main Menu > Configure > User Configuration). See User Configuration section.

KVM User Interface Overview

The KVM user interface is composed of windows, each of which has a specific function, allowing you to interface with the KVM to perform all your KVM configuration and management tasks.

The diagram below presents the organizational structure of the user interface:



A Word About the Window Names

Not all names used to refer to windows appear in the actual windows. Because some windows do not have distinguishable names, the document assigns names to these windows to best describe their function. Consequently, these window names are not boldfaced. Some examples are: Main Menu, Server Name Entry window, Access List - Port Selection window.

Logging In

1. To log in, type in the default Login name, **admin** (lower case) followed by the password, **cyclades** (lower case) in the respective fields.



2. Tab to the **OK** button and press <Enter>. The system should bring up the KVM main menu.

OSD Guidelines

The succeeding procedures in this chapter assume that you are already logged in. For security, Cyclades recommends that you change your password as soon as convenient.

Saving Your Configuration

You do not need to click on the Save button if you are not finished with configuring a set of parameters for a given Configuration menu selection. However, if you are done with a configuration, just tab to the Save button to complete your configuration.

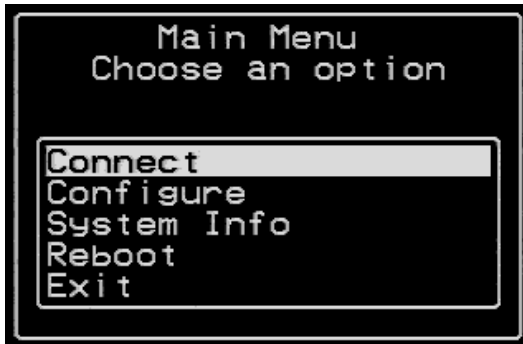
Press <Esc> to return to the last main menu.

KVM Main Menu

The KVM Main Menu provides three selections:

<i>Menu Selection</i>	<i>Select the menu item to:</i>
Connect	View the Server Connection Menu. From this menu, you can select the port to which you wish to connect, or invoke the Cycle function to view the ports.
Configure	View the Configuration Menu.
System Info	View the system information pertaining to the KVM version that you are using.
Reboot	Reboot the KVM switch.
Exit	Close the KVM OSD session.

The actual menu as viewed from the OSD:



*The **Connect** selection is discussed in more detail in Chapter 4: KVM Operation.*

Before a user can connect to a port, you (as KVM system administrator) must first configure the necessary port and user access requirements.

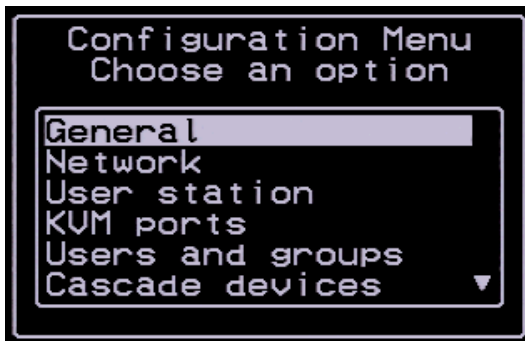
To start configuration, select **Configure** from the Main Menu.

Configuration Menu

The **Configuration Menu** provides the following selections:

<i>Menu Selection</i>	<i>Select the menu item to:</i>
General	Configure authentication type, authentication servers, syslog facility, IP Security, 3DES, Access Type and more.
Network	Configure DHCP and/or IP address,
User Station	Configure the work station's idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current workstation.
KVM Ports	Activate ports, name servers, and configure power outlets.
Users and Groups	Configure local users and groups, set up user passwords, and update the User Access List.
Cascade Devices	Add, edit or delete devices in connection with cascading.
Save/Load Config	Save or load configuration, and restore configuration to factory default values.
Exit	Exit from the OSD and close the session.

The actual menu as viewed from the OSD:



General Configuration: Windows Summary

The function of each General Configuration window is as follows:

<i>Menu Selection</i>	<i>Select the menu item to:</i>
Authentication Type	Assign the authentication type. (Select from: None, Local, Radius, TacacsPlus, Kerberos, LDAP, and Windows NT/2K/2K3.)
Syslog Facility	Define the number which the target syslog server will use as a message identifier. Values are from 0 through 7.
Escape Sequence	Configure the escape sequence (default is ^K).
Sun Keyboard	Enable your keyboard to simulate the Sun keyboard.

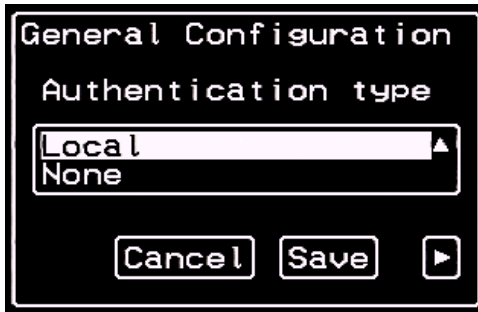


*The **Save** button in every window saves your configuration into the running configuration. To save the configuration to Flash, you must select Save from the Configuration Menu.*

General Configuration: Authentication Type

(Configure > General > Authentication Type)

The Authentication Type window allows you to select the authentication service to authenticate a KVM user. It is the first window in the General Configuration menu.



1. From the **Authentication Type** window, select the authentication service.
2. Tab to the next button to configure the Syslog Facility.



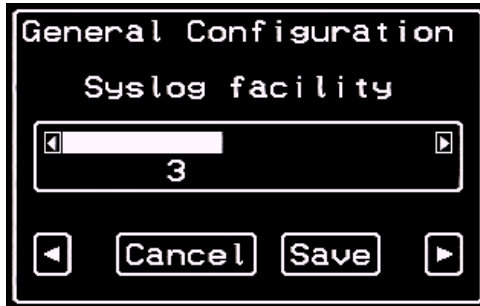
The type of dialog windows that appears depend on the type of authentication that you define in the Authentication Type window.

Syslog Facility

(Configure > General > Authentication Type > Syslog Facility)

The Syslog Facility defines the number which the target syslog server will use as a message identifier. Values are from 0 through 7.

1. To configure, go to: General Configuration > Authentication Type > Syslog Facility:



2. From the Syslog Facility window, select the right or low arrow key inside the box to select the value (0 through 7) of the target syslog server.
3. Tab to the forward button to configure the **Escape Sequence**.

Syslog Facility Values

The Syslog Facility values (0 through 7) correspond to the log levels defined in Linux <linux/kernel.h> as follows:

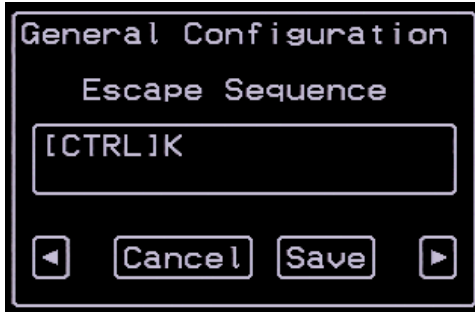
```
#define KERN_EMERG    "<0>" /* system is unusable          */
#define KERN_ALERT    "<1>" /* action must be taken immediately */
#define KERN_CRIT     "<2>" /* critical conditions             */
#define KERN_ERR      "<3>" /* error conditions                */
#define KERN_WARNING  "<4>" /* warning conditions              */
#define KERN_NOTICE   "<5>" /* normal but significant condition */
#define KERN_INFO     "<6>" /* informational                   */
#define KERN_DEBUG    "<7>" /* debug-level messages            */
```

When a number is selected, all messages of that level and below are logged.

Escape Sequence

(Configure > General > Authentication Type > Syslog Facility > Escape Sequence.)

The Escape Sequence defines the key sequence for the escape function when operating from the OSD.

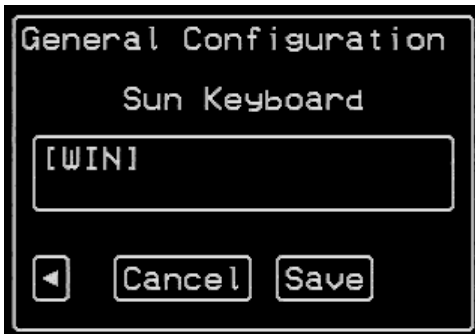


1. From the Escape Sequence window, enter the key sequence for the escape function, or to change the default escape sequence (Ctrl-K).
2. Tab to the forward button to configure the Sun Keyboard.

Sun Keyboard

(Configure > General > Authentication Type > Syslog Facility > Escape Sequence > Sun Keyboard)

The Sun Keyboard window allows you to configure and simulate a Sun keyboard for the KVM.



1. From the Sun Keyboard window, enter the keyboard type that you are using (default: WIN).
2. Tab to the forward button to configure the IP Security.

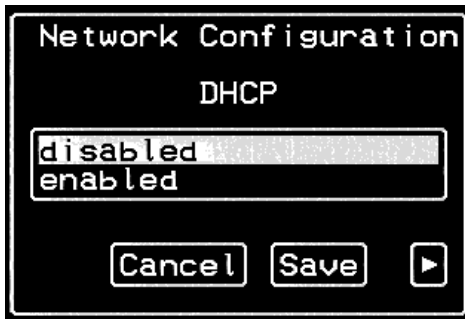
Network Configuration

The Network Configuration screens allow you to configure the KVM switch network settings. If you are not using a DHCP server, it will provide additional screens to enable you to configure such network parameters as the IP address, netmask, gateway, and more.

DHCP

(Configure > Network > DHCP)

The DHCP window allows you to enable or disable the DHCP server.

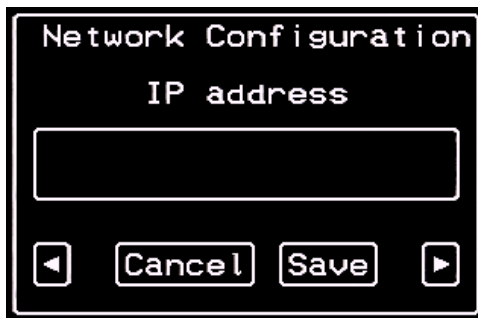


1. From the DHCP dialog window, select from: Disabled, Active, or Save.
2. Tab to the next button and press <Enter> to configure the **IP address**.

IP Address

(Configure > Network > DHCP > IP Address)

If DHCP is disabled, continue on to the IP Address window and the rest of the Network Configuration windows.

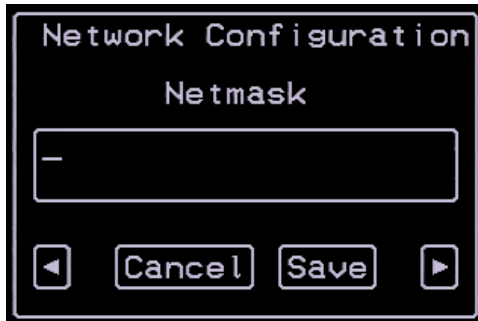


1. From the IP Address window, enter the IP address for the KVM.
2. Tab to the next button and press <Enter> to configure the **Netmask**.

3: KVM OSD Configuration

Netmask

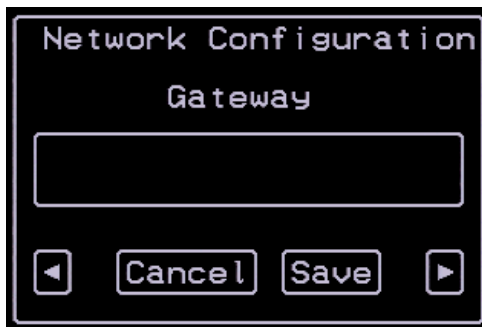
(Configure > Network > DHCP > IP Address > Netmask)

A screenshot of a terminal window titled "Network Configuration" with the subtitle "Netmask". It features a large rectangular input field containing a single hyphen character. Below the input field are four buttons: a left-pointing arrow, a button labeled "Cancel", a button labeled "Save", and a right-pointing arrow.

1. From the Netmask window, enter the Netmask address.
2. Tab to the next button and press <Enter> to configure the **Gateway**.

Gateway

(Configure > Network > DHCP > IP Address > Netmask > Gateway)

A screenshot of a terminal window titled "Network Configuration" with the subtitle "Gateway". It features a large rectangular input field that is currently empty. Below the input field are four buttons: a left-pointing arrow, a button labeled "Cancel", a button labeled "Save", and a right-pointing arrow.

1. From the Gateway window, enter the Gateway address.
2. Tab to the next button and press <Enter> to configure the **DNS Server**.

DNS Server

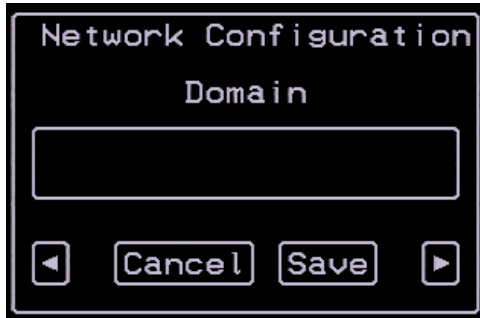
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server)



1. From the DNS Server window, enter the server address.
2. Tab to the next button and press <Enter> to configure the **Domain** name.

Domain

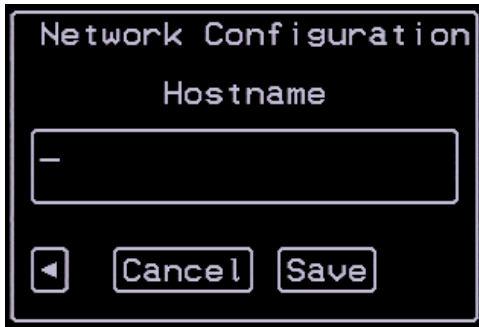
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server > Domain Name)



1. From the Domain window, enter the domain name.
2. Tab to the next button and press <Enter> to configure the **Hostname**.

Hostname

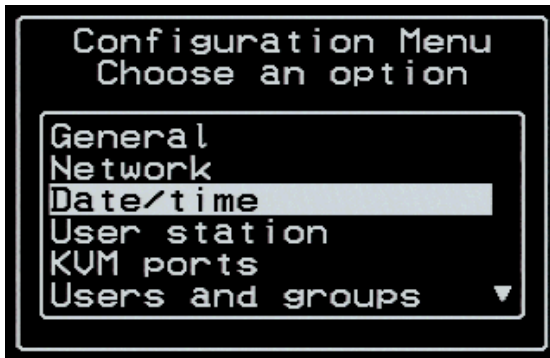
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server > Domain Name > Hostname).



1. From the Hostname window, type in the hostname.
2. Tab to the **Save** button and press <Enter> to complete Network configuration.

Date/Time

(Configure > Date/Time)



The Date/Time window allows you to enable or disable the NTP server. If disabled, more windows will be provided to allow you to enter the system date and time manually.

Enabling the NTP Server

(Configure > Date/Time > NTP)



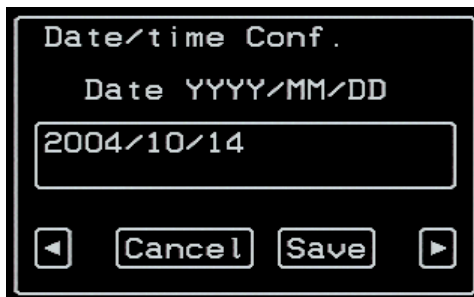
1. From the NTP window, select **enabled** and press <Enter>. The system displays the NTP Server window:



2. Tab to the **Save** button and press <Enter> to complete the procedure.

Entering the Date and Time Manually

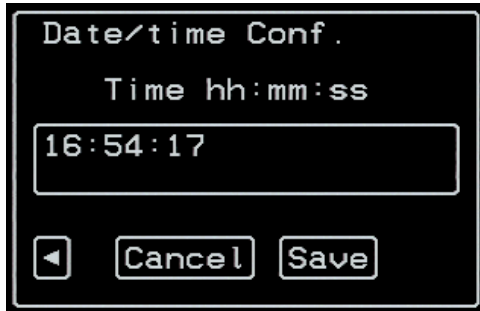
1. From the NTP window, select **disabled** and press <Enter>. The system displays the Date entry window:



2. From the resulting window, type in the date (follow the given format).
3. Tab to the next button and press <Enter>.

3: KVM OSD Configuration

The system displays the Time entry window:



4. From the resulting window, type in the time (follow the given format).
5. Tab to the Save button and press <Enter> to complete the procedure.

User Station Configuration

The User Station option allows you to configure the following user station parameters:

- Idle Timeout
- Cycle Time
- Keyboard Type

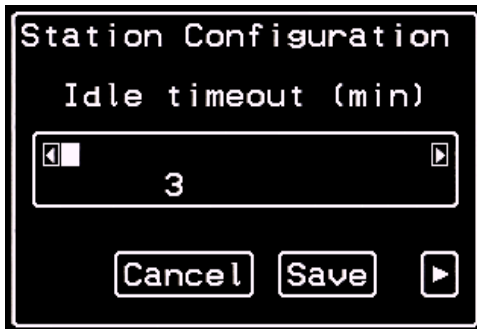
The keyboard escape sequences for the following commands

- Quit
- Power Management
- Mouse/Keyboard Sync
- Video Configuration
- Switch Next
- Switch Previous

Lastly, it allows you to view the Port Information for a selected port.

Idle Timeout

(Configure > User Station > Idle Timeout)

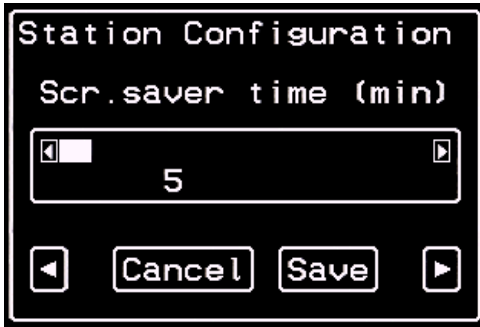


1. From the Idle Timeout window, click on the forward or back button to select the length of time (0 through 60 minutes) before the system times out after a period of inactivity.
2. Tab to the next button and press <Enter> to configure the **Screen Saver Time**.

Screen Saver Time

(Configure > User Station > Idle Timeout > Screen Saver Time)

The screen saver is designed to protect your screen even after the screen times out, by activating the screen saver mode after a period of inactivity. 1

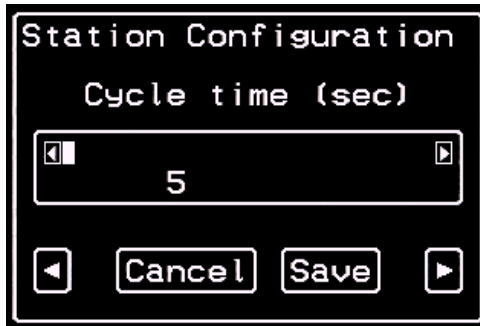


1. From the Screen Saver Time window, click on the forward or back button to select the length of time (0 through 60 minutes) before the system activates the screen saver after a period of inactivity.
2. Tab to the next button and press <Enter> to configure the **Cycle Time**.

Cycle Time

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time)

The Cycle Time window allows you to set the time interval for cycling from one port to another.



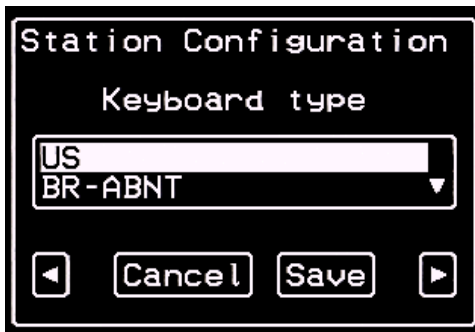
1. From the Cycle Time window, click on the forward or back button to select the cycle time (0 through 60 seconds; default value is 3 seconds) for cycling between ports.
2. Tab to the next button and press <Enter> to configure the **Keyboard Type**.

Keyboard Type

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type)

The keyboard type defines the keyboard layout connected to the **USER 1** port of the KVM box. The types of keyboard to choose from are:

- US
- BR-ABNT
- BR-ABNT2
- Japanese
- German
- Italian
- French
- Spanish

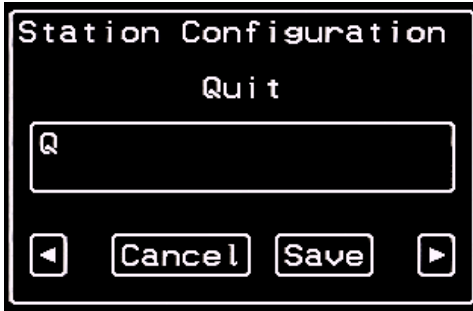


3: KVM OSD Configuration

Quit

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit)

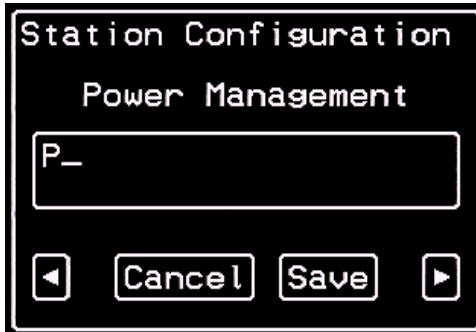
The Quit window allows you to define (or change the default value of) the key sequence for the quit command.



Power Management

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management)

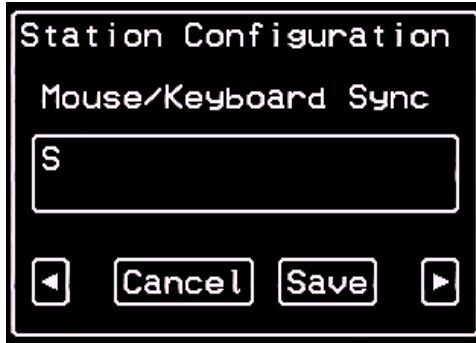
The Power Management screen defines the key sequence for the "Power Management" command. The default key sequence (^KP) displays an OSD menu which allows you to switch ON or OFF the remote server.



Mouse/Keyboard Sync

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management > Mouse/Keyboard Sync)

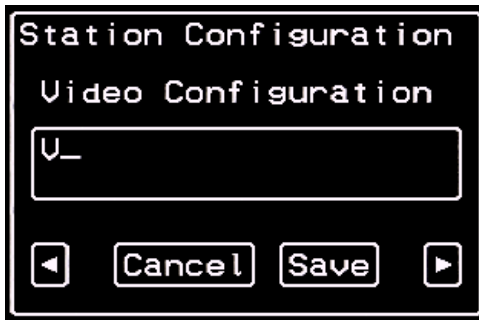
The Mouse/Keyboard Sync defines the key sequence for the mouse and keyboard synchronization command.



Video Configuration

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management > Mouse/Keyboard Sync > Video Configuration)

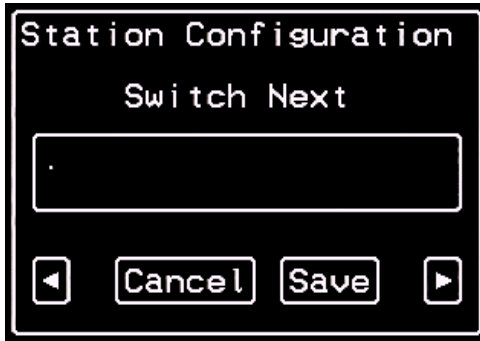
The Video Configuration window defines the key sequence for displaying the video configuration command.



Switch Next

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management > Mouse/Keyboard Sync > Video Configuration > Switch Next)

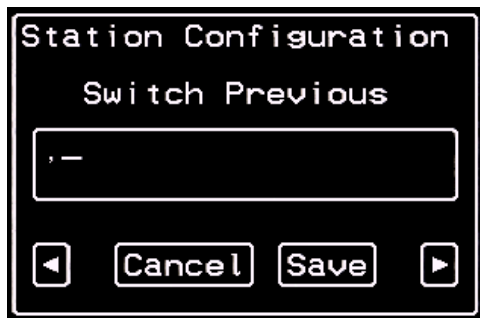
The Switch Next window allows you to define or change the default key sequence for the switch next command. This command allows the user to switch to the next port or server while using the OSD.



Switch Previous

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management > Mouse/Keyboard Sync > Video Configuration > Switch Next > Switch Previous)

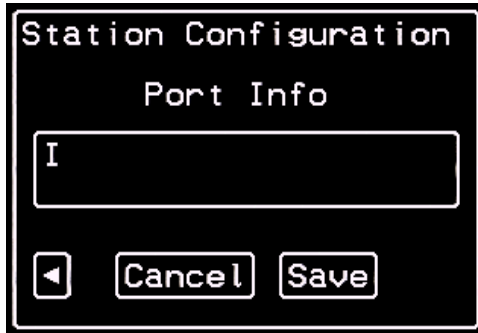
The Switch Previous window allows you to define or change the default key sequence for the switch previous command. This command allows the user to switch to the previous port or server while using the OSD.



Port Info

(Configure > User Station > Idle Timeout > Screen Saver Time > Cycle Time > Keyboard Type > Quit > Power Management > Mouse/Keyboard Sync > Video Configuration > Switch Next > Switch Previous > Port Info)

The Port Info window allows you to define or change the default key sequence for the command to view port information while using the OSD.

**KVM Ports**

The KVM Ports option allows you to configure the KVM ports as follows:

- Enable or disable a port.
- Name a server.
- Define the power outlets to be used.

Selecting a KVM Port to Configure

(Configure > KVM Ports)

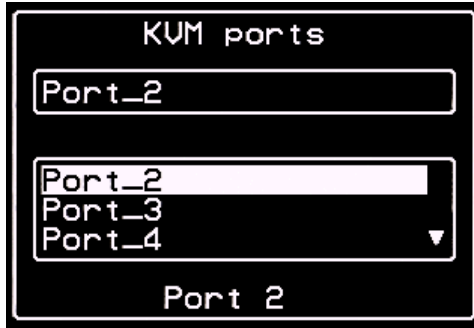
The KVM Ports (or port selection window) allows you to select from the scrollable list the port you wish to configure.

The input field at the top of the window is a search box which functions exactly the same as the port connection (**Connect**) window. Simply enter the first letters of the KVM port name and, if a match is found, the system will locate the port from the list.

3: KVM OSD Configuration

To select a KVM Port:

1. Go to the KVM Ports window:



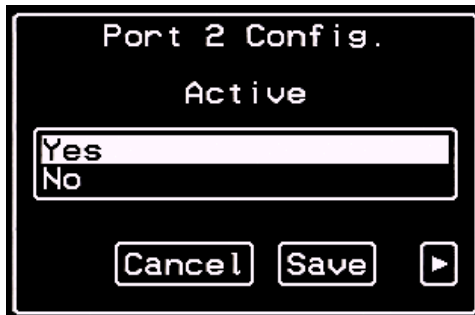
2. From the resulting window, enter or select the port you wish to configure
3. Press <Enter>.



*All subsequent procedures in the KVM Ports section assume that you have already selected a port using the **KVM Ports** window.*

Activating a Port

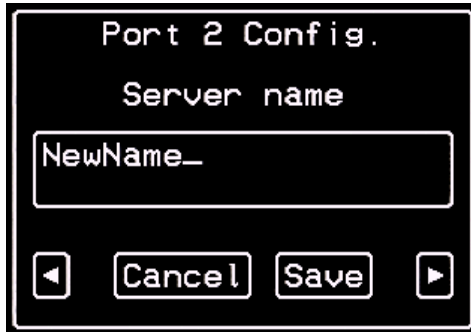
(Configure > KVM Ports > Active)



1. From the **Active** window, select **Yes** or **No** to activate or disable the currently selected port.
2. Tab to the next button to configure the **Server Name**.

Server Name

(Configure > KVM Ports > Active > Server Name)

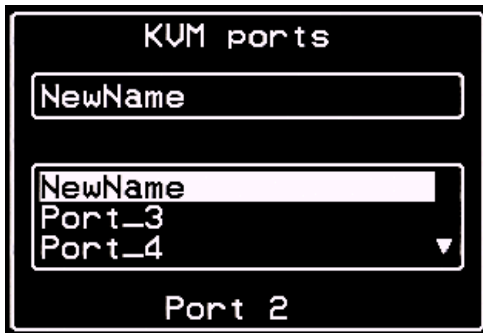


1. From the **Server Name** window, type in the server name of the currently selected port.
2. Tab to the next button to configure the **KVM Ports**.

- OR -

To verify the new server name, tab to the **Save** button and press <Enter>.

The system displays the KVM Ports selection window:

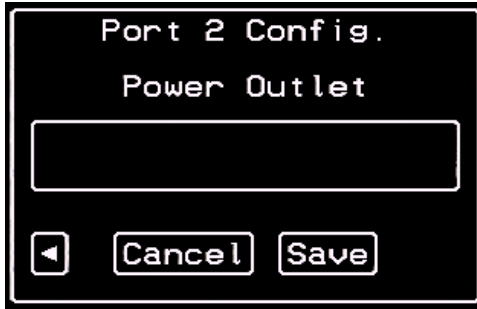


3. Type in the server name in the search box, as necessary.


Power Outlet

(KVM Ports > Active > Server Name > Power Outlet)

The Power Outlet window allows you to assign the AlterPath PM outlet number(s) that powers the current port.



1. Enter the AlterPath PM outlet number that powers the selected computer, otherwise leave the field box blank. If you are using two outlets, use a space to separate the second outlet (e.g., 4 16).
2. Tab to the **Save** button and press <Enter> to complete the procedure.

 *To complete the configuration required to establish a power control session, you need to configure the AUX serial port of your KVM unit for the power management profile. You can do this through the web interface using the following procedure:*

1. Log on to the AlterPath KVM through the web interface as shown in Chapter 5: KVM Operation.
2. From the menu to the left of the Configuration screen, select Serial Ports.
You will see the screen for configuring the ttyS1 port, which is the AUX serial port of your KVM.
3. Select AlterPath PM Profile.
4. Save the configuration, making sure that you select serial ports configuration.

Configuring a Server Connected to a Slave

When configuring a server that is connected to a slave KVM, follow the same procedure described for configuring servers. You choose a server that is connected to a slaved KVM. In response, the system will bring you the Physical Port window, with the currently configured physical port selected

(for example, kvm16.4). You can also define, if any, the AlterPath PM outlet that powers the computer connected to the port of the slave KVM.



To enable power management in a cascading environment, you must connect the AlterPath PM units to the Master AlterPath KVM's AUX port. Connecting AlterPath PM units to the AUX port on Slave KVM units is not supported.

Users and Groups

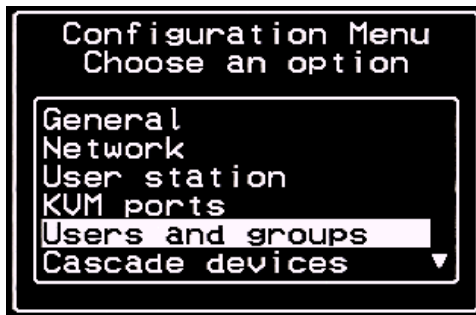
The Users and Groups option of the Configuration Menu allows you to configure the following:

- Add or delete local users
- Set or reset passwords
- Add or delete local groups
- Configure or edit the User Access List
- Configure or edit the access permissions of the Generic User



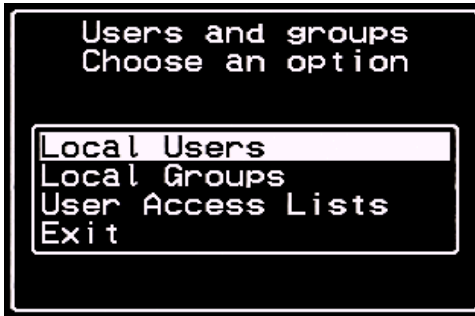
*To understand how the hierarchy of permissions work when creating user permissions between groups and the generic user, refer to **Hierarchy of Permissions, Chapter 4: KVM Web Configuration.***

The Users and Groups option of the Configuration Menu:



Configuring Users

To configure local users, go to: Configure > Users and Groups > Local Users:



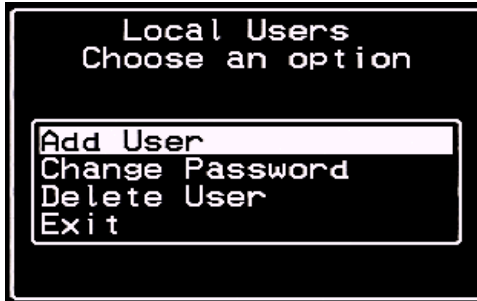
Tab to **Local Users** and press <Enter> to configure the Local Users.

Adding a User

(Configuration > Users and Groups > Local Users > Add User)

To Add a User follow the steps below:

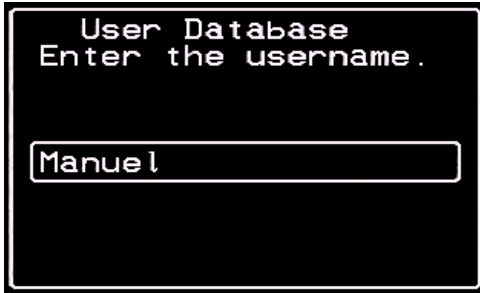
1. With **Add User** highlighted from the Local Users Menu, press <Enter>.



The system displays the Enter the Username window as shown:



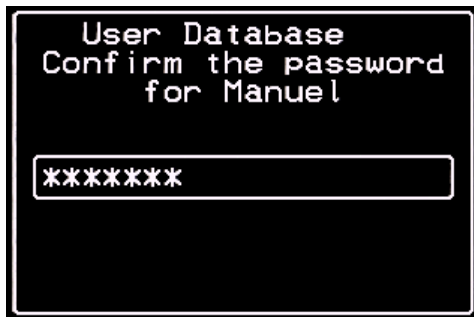
2. From the resulting window, type in the username (this field is case-sensitive) in the input box as shown by the following example:



3. Press <Enter> when done.
The system displays the **Enter the Password** window as shown:



4. From the resulting window, type in the user's password (this field is also case-sensitive) and then press <Enter>.
The system displays the Confirm the Password window as shown:



5. From the resulting window, re-enter the password to confirm and then press <Enter>.

The system displays the following message:



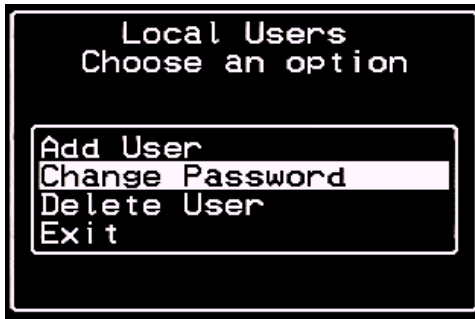
6. Click on **OK** to complete the procedure.

Changing the User, Admin, or Root Password

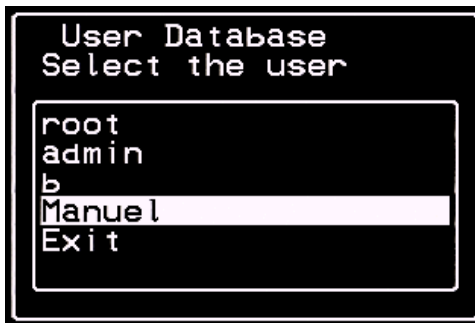
(Configure > Users and Groups > Local Users > Change Password)

To change the a user's password, follow the steps below:

1. From the Local User Menu, select **Change Password** and press <Enter>.

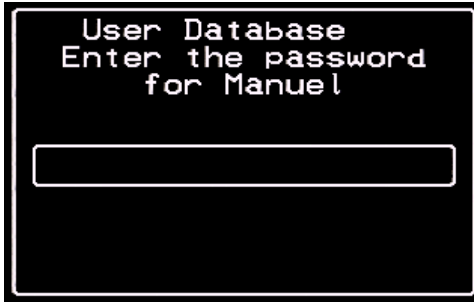


The system displays the **Select the User** window.



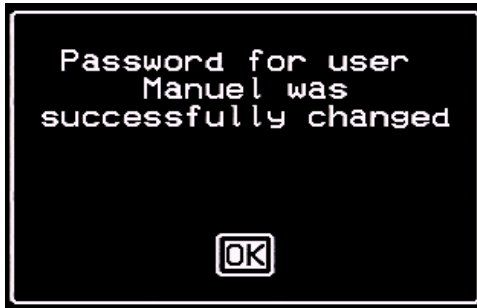
2. From the resulting window, select the user whose password you want to change, and then press <Enter>.

The system displays the **Enter the Password** window:



3. Enter the new password and then press <Enter>. The system displays a password confirmation window.
4. Re-enter the password to confirm the new password and then press <Enter>.

The system displays the following message:



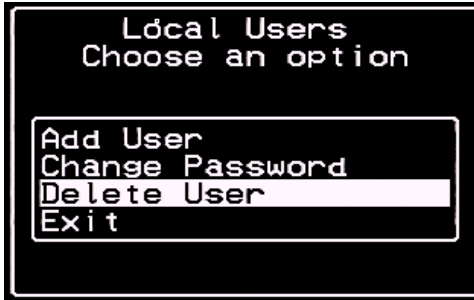
5. Select **OK** to complete the procedure.

Deleting a User

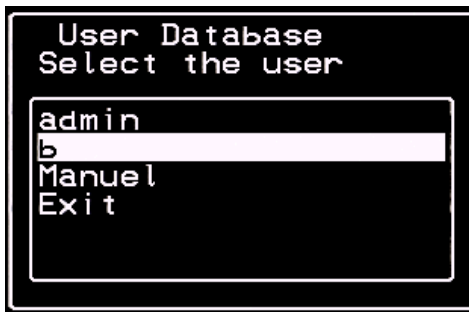
(Configure > Users and Groups > Local Users > Delete User)

To delete a user, follow the steps below:

1. From the Local Users Menu, select Delete User and press <Enter>.



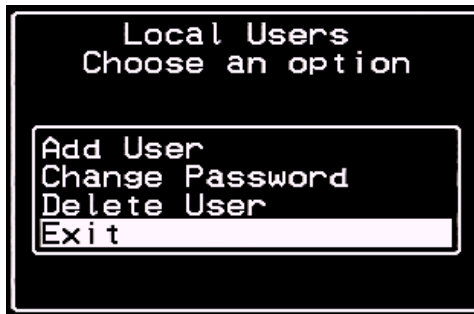
The system displays the **Select the User** window as shown:



2. From the resulting window, select the user that you wish to delete and then press <Enter>.

The system will display a message to confirm your deletion.

3. From the Select the User window, tab to the Exit line and press <Enter>.

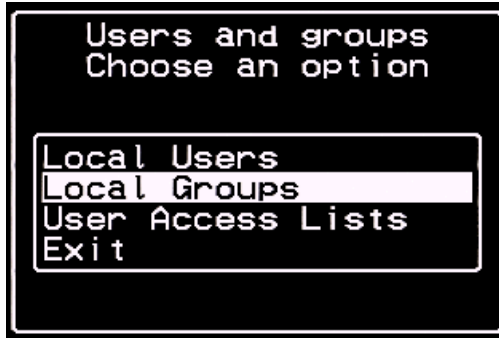


Local Groups

The Local Groups option allows you to perform the following:

- Add a new group
- Add a user to a group
- Delete a user from a group
- Delete a group

Users and Groups Menu:

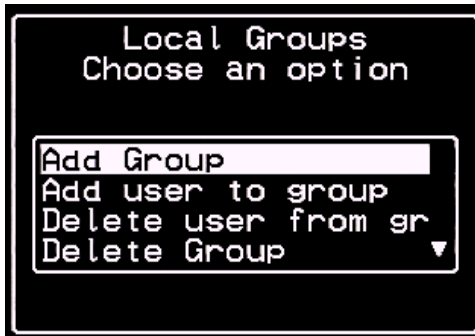


Adding a Group

(Configure > User and Groups > Local Groups > Add Group)

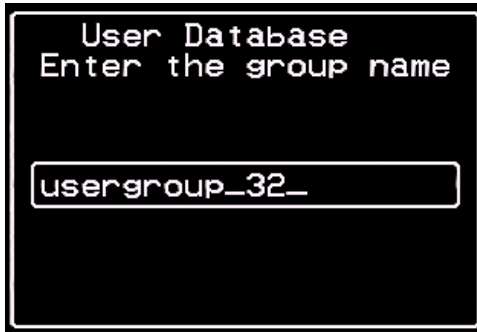
To add a user group, follow the steps below:

1. From the Local Groups Menu, select Add Group and press <Enter>.



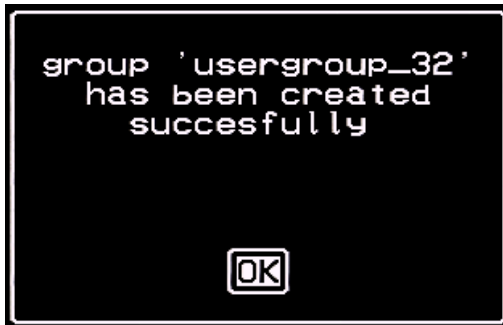
3: KVM OSD Configuration

The system displays the Enter the Group Name window as shown:



2. From the resulting window, type in the group name you wish to add and then press <Enter>.

The system displays the following message:



3. Click on OK to complete the procedure.

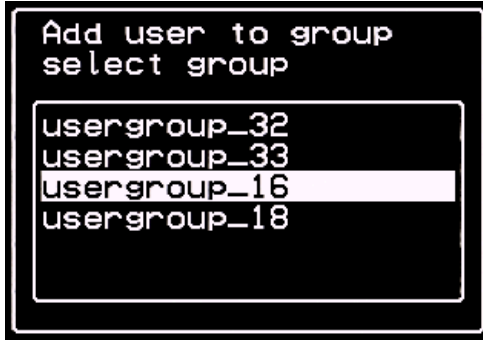
Adding a User to a Group

(Configure > User and Groups > Local Groups > Add User to Group)

To add a user group, follow the steps below:

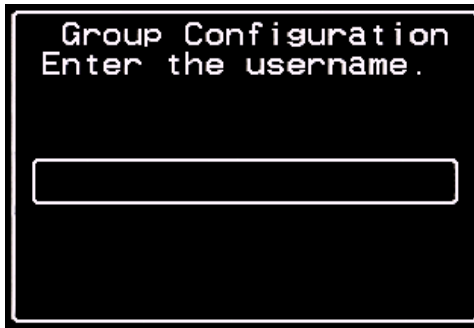
1. From the Local Groups Menu, select **Add User to Group** and press <Enter>.

The system displays the **Add User to Group - Select Group** window as shown:



2. From the resulting window, select the group to which you wish to add the user and then press <Enter>.

The system displays **Group Configuration - Enter the Username** window as shown:

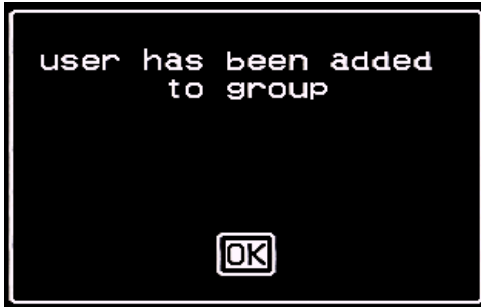


3. From the resulting window, type in the username of the user that you wish to add to the group you just selected.

3: KVM OSD Configuration

4. Press <Enter>.

The system displays the following message:



5. Click on **OK** to complete the procedure.

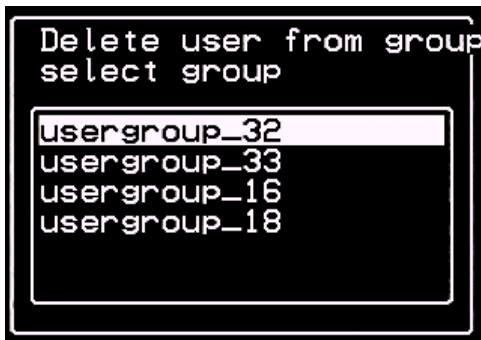
Deleting a User from a Group

(Configure > User and Groups > Local Groups > Delete User from Group)

To delete a user from a group, follow the steps below:

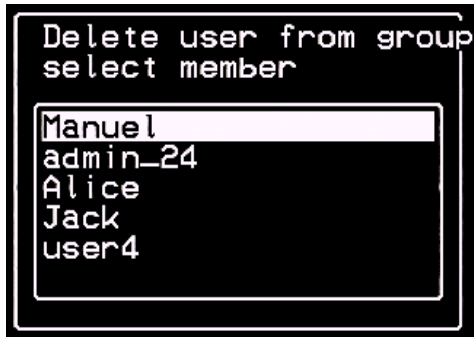
1. From the Local Groups Menu, select **Delete User from Group** and press <Enter>.

The system displays the Delete User from Group - Select Group window as shown:



2. From the resulting window, select from the list the group that you wish to delete, and then press <Enter>.

The system displays the **Delete User from Group - Select Member** window as shown:



3. From the resulting window, select the user that you wish to delete from the group, and then press <Enter>.

The system displays the following message:



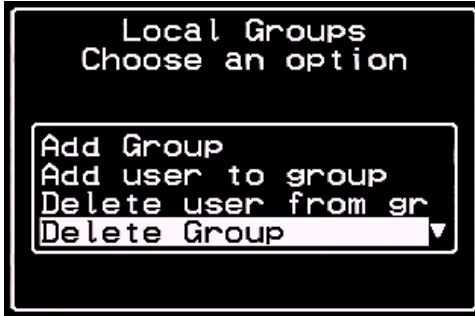
4. Click on **OK** to complete the procedure.

Deleting a Group

(Configure > User and Groups > Local Groups > Delete Group)

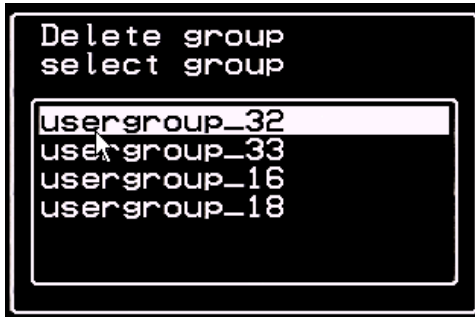
To delete a user group, follow the steps below:

1. From the Local Groups Menu, select **Delete Group** and press <Enter>.



The system displays the Delete Group - Select Group window.

2. From the resulting window, select from the list the group that you wish to delete, and then press <Enter>.



The system displays the following message:



3. Click on **OK** to complete the procedure.

User Access Lists Menu

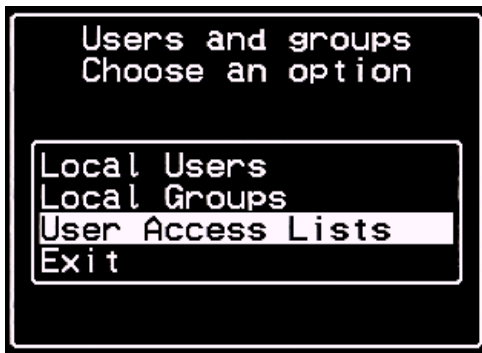
(Configure > Users and Groups > User Access List)

The User Access Lists Menu allows you to add, edit, or delete users from the user access list. The User Access List is a database that defines all KVM users, the ports to which they have access, the types of permissions that they have.

Generic User

The Generic User, which is part of User Access List configuration, allows you to configure the default permission of all regular users in the User Access List. Any user that you add to the User Access List inherits the properties of the Generic User.

To retrieve the User Access List Menu, go to: Configure > Users and Groups > User Access Lists.

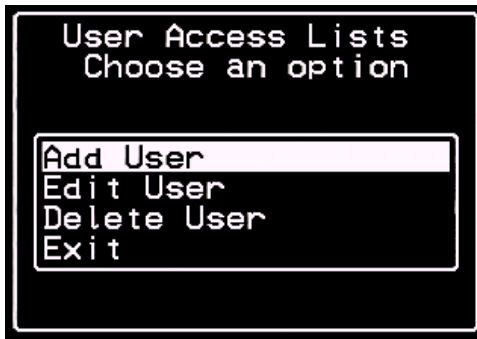


Adding a User to the User Access List

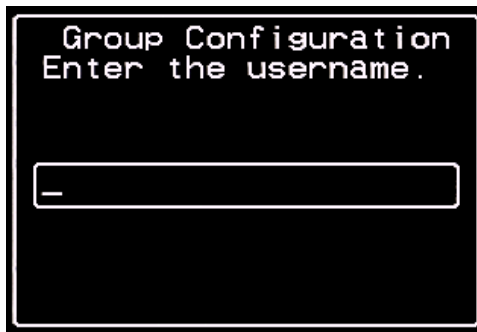
(Configure > Users and Groups > User Access List > Add User)

To add a user to the user access list, follow the steps below:

1. From the User Access Lists Menu, select Add User and press <Enter>.

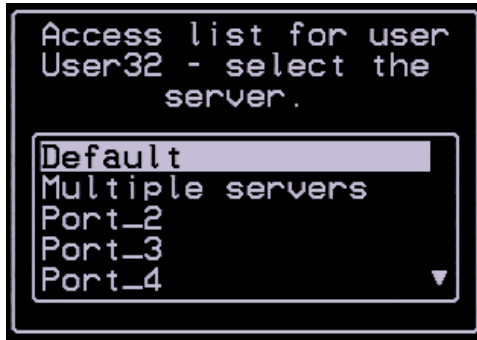


The system displays the **Group Configuration - Enter the Username** window as shown:



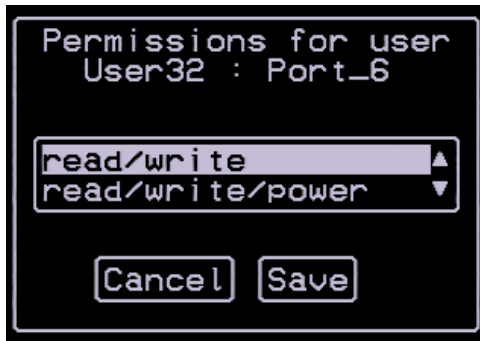
2. Type in the username of the user that you wish to add, and then press <Enter>.

The system displays the Access List for User - Select the Server window as shown:



3. From the resulting window, select the server to which you wish to assign to the user, and then press <Enter>.

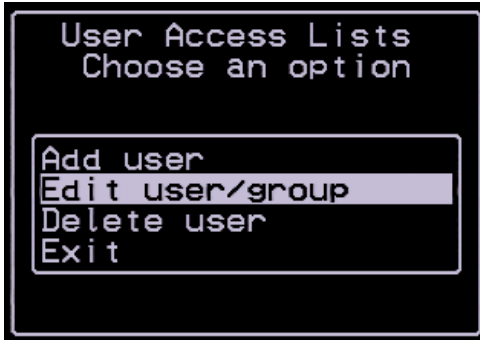
The system displays the Permission for User window as shown:



4. From the resulting window, select the type of user permission you wish to assign.
5. Tab to the **Save** button and press <Enter> to complete the procedure.

Edit User/Group

(Configure > Users and Groups > User Access List > Edit User/Group)

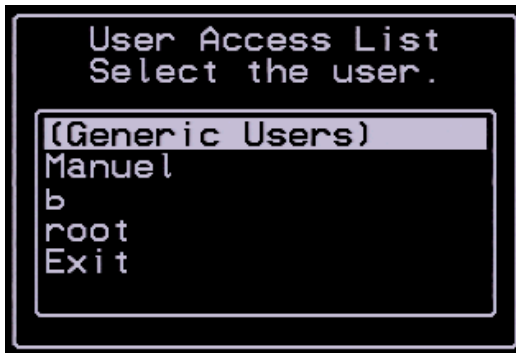


Editing the Generic User

To edit the generic user, follow the steps below:

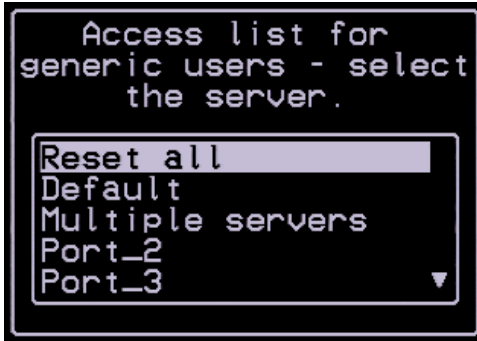
1. From the User Access List - Select the User window, select (**Generic Users**) and press <Enter>.

The system displays the **User Access List - Select the User** window:



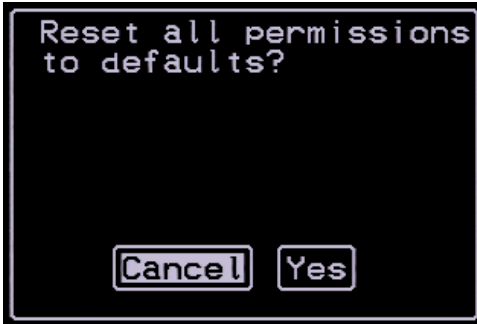
2. From the resulting window, select (**Generic Users**) and press <Enter>.

The system displays the Access List for User - Select the Server window:



3. From the resulting window, select from the list the server you wish to assign or re-assign to the generic user, and then press <Enter>.

If you select Reset All, the system displays the following window:



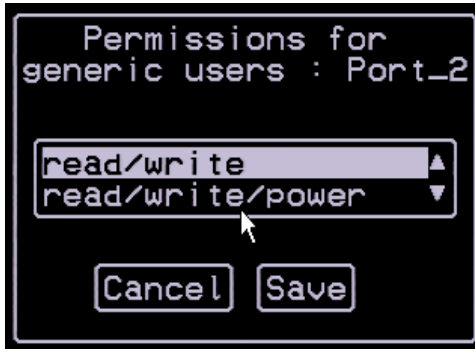
If you select Multiple Servers, the system displays the following window:



3: KVM OSD Configuration

When using the Multiple Servers window, you can specify the servers using a comma (to separate each server) and/or a hyphen (to specify a range of servers).

If you select an individual port (say, Port_2), the system displays the Permissions window as shown:



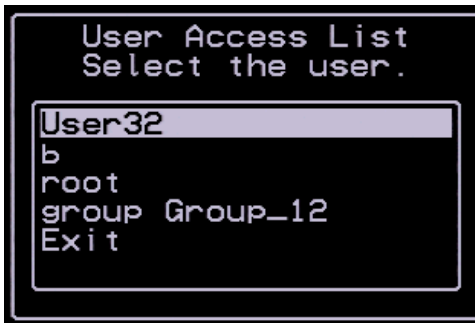
4. From the resulting window, select the type of user permission you wish to assign.
5. Tab to the **Save** button and press <Enter> to complete the procedure.

Deleting a User from the User Access List

(Configure > Users and Groups > User Access List > Delete User)

To delete a user from the user access list, follow the steps below:

1. From the User Access Lists Menu, select **Delete User** and press <Enter>. The system displays the User Access List - Select the User window:

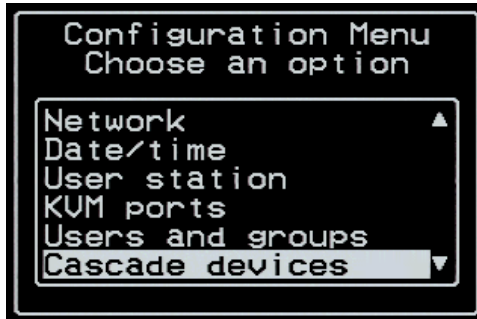


2. From the resulting window, select from the list the user you wish to delete from the User Access List and then press <Enter>. The system displays a message to confirm your deletion.

Cascade Devices

(Configure > Cascade Devices)

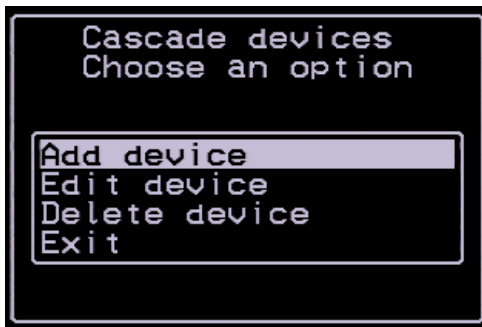
The Cascade Devices option of the Configuration Menu allows you to configure a secondary KVM to be cascaded to the primary KVM switch to increase the number of supportable ports. The secondary device may be another KVM/net switch, a KVM switch or a KVM expander.



Cascade Devices Menu

(Configure > Cascade Devices > Add Device)

The Cascade Devices Menu provides four options:



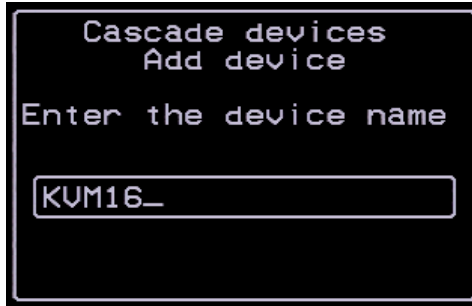
Adding a Secondary Device

To add a secondary device to be cascaded to the primary KVM switch, follow the steps below:

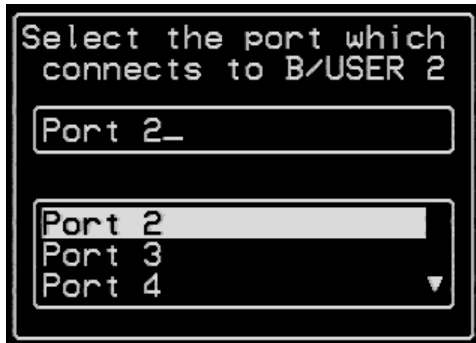
1. From the Cascade Devices Menu, select **Add Device** and press <Enter>.

3: KVM OSD Configuration

The system displays the Add Device - Enter the Device Name window:



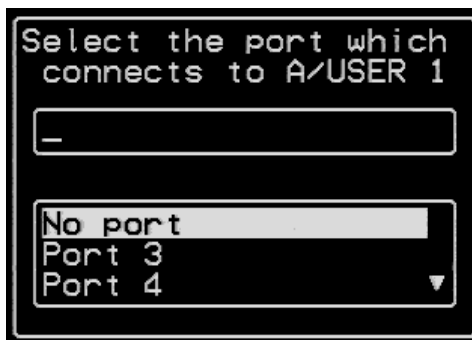
- From the resulting window, select the device type and press <Enter>. The system displays the Port Selection for B/USER 2 window:



NOTE: In the KVM Expander, **User 1** is port **A**; **User 2** is port **B**.

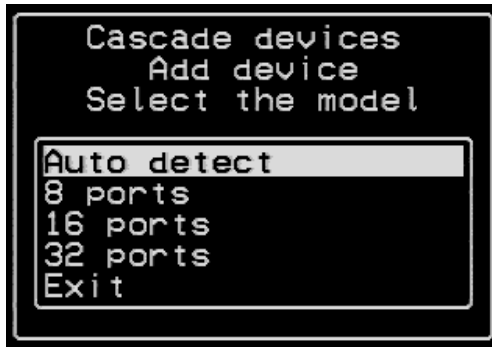
- From the resulting window, select the port that connects to the USER 2 and then press <Enter>.

The system displays the Port Selection for A/USER 1 window:

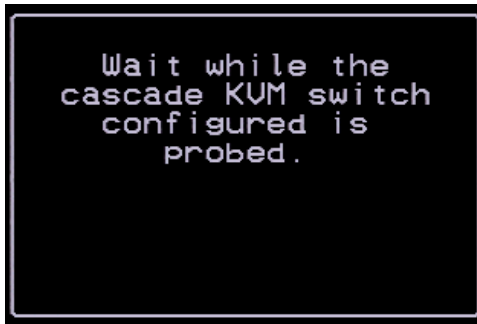


4. From the resulting window, select the port that connects to USER 1, and then press <Enter>.

The system displays the Device Model Selection window:



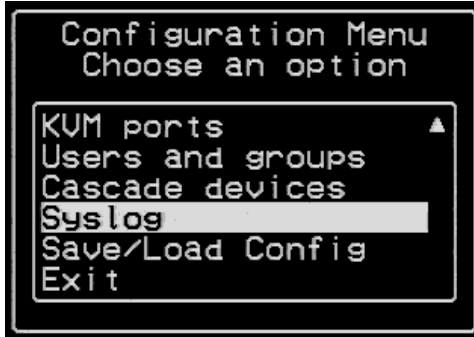
5. From the resulting window, select Auto Detect and press <Enter>. During auto detection, the system displays the following message:



Syslog

(Configure > Syslog)

The Syslog option of the Configuration Menu allows you to enter the IP address of the logging system. (To define the Syslog Facility, go to Configuration > General.)



To configure the Syslog IP address:

1. From the Configuration Menu, select Syslog and press <Enter>.

The system displays the Syslog Sever window:

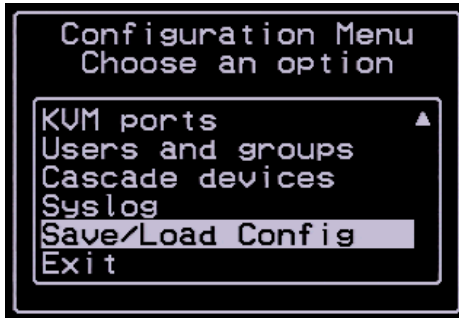


2. From the resulting window, enter the address of the syslog server. Tab to the **Save** button and press <Enter> to complete Syslog configuration.

Save/Load Config

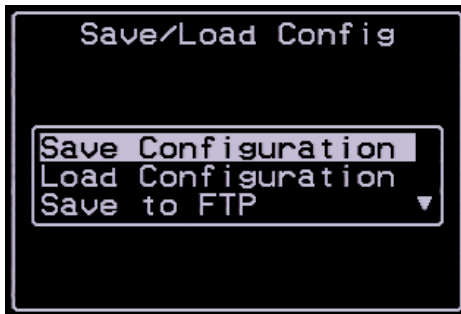
(Configure > Save/Load Config)

The Save/Load Config option allows you to save your configuration to Flash and to upload (or download) the configuration file to (or from) the FTP server.



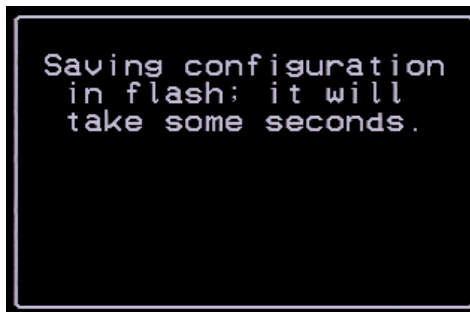
Saving Your Configuration

To save your configuration to Flash, follow the steps below:



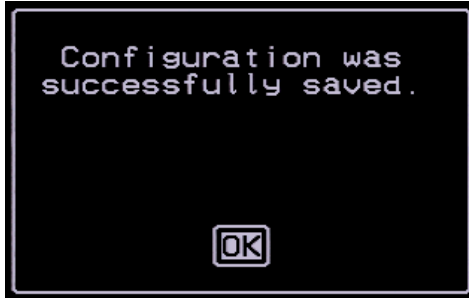
1. From the Save/Load Config window, select Save Config and press <Enter>.

The system displays the following message:



3: KVM OSD Configuration

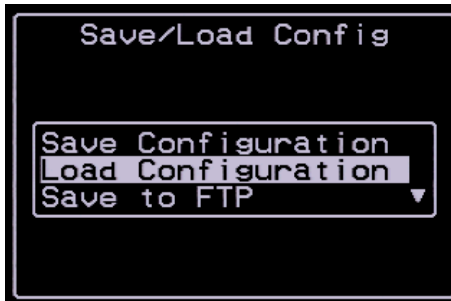
The following message follows:



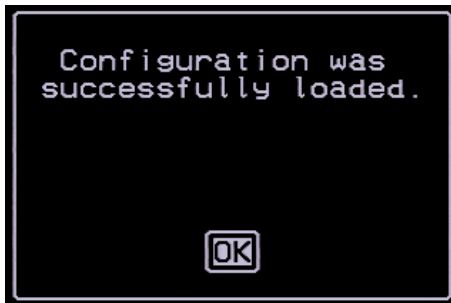
2. Click on **OK** to complete the procedure.

Loading Your Configuration

The Load Configuration command is the same as the shell command: **restoreconf**. The command loads the configuration file from Flash. To load the configuration file, follow the steps below:



1. From the Save/Load Config window, select Load Configuration.
Once the system loads or restores the configuration from Flash, it displays the following message:

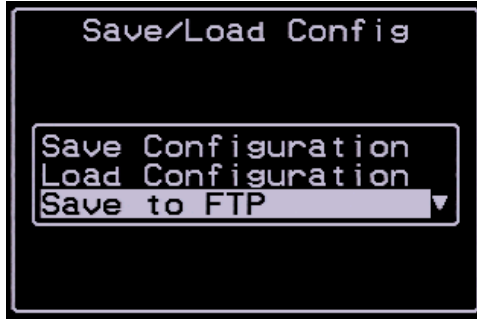


2. Select **OK** to complete the procedure.

Saving your Configuration to an FTP Server

(Configure > Save/Load Config > Save to FTP)

To save your configuration file to an FTP server, complete the procedure below:



1. From the Save/Load Config window, select **Save to FTP** and press <Enter>.

The system displays the **Save to FTP Server - Filename** window:



2. From the resulting window, type in the configuration filename.
3. Tab to the next button and press <Enter>.

3: KVM OSD Configuration

The system displays the **Save to FTP Server - Server** window:



4. From the resulting window, type in the FTP server name.
5. Tab to the next button and press <Enter>.

The system displays the **Save to FTP Server - Username**:



6. From the resulting window, enter your username to access the FTP Server.
7. Tab to the next button and press <Enter>.

The system displays the **Save to FTP Server - Password** window:

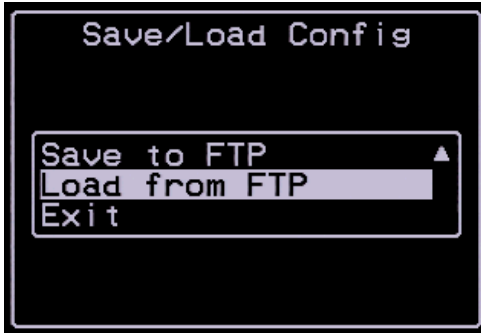


8. From the resulting window, type in your password to access the FTP server.
9. Tab to the **Save** button and press <Enter> to complete the procedure.

Loading Configuration from an FTP Server

(Configure > Save/Load Config > Load from FTP)

To load a configuration file from an FTP server, complete the procedure below:



1. From the Save/Load Config window, select **Load from FTP** and press <Enter>.

The system displays the **Load from FTP Server - Filename** window:



2. From the resulting window, enter the configuration filename.
3. Tab to the forward button and press <Enter>.

3: KVM OSD Configuration

The system displays the Load from FTP Server - Server window:



4. From the resulting window, enter the FTP servername.
5. Tab to the forward button and press <Enter>.

The system displays the Load from FTP Server - Username:



6. From the resulting window, enter your FTP username.
7. Tab to the forward button and press <Enter>.

The system displays the Load from FTP Server - Password:



8. From the resulting window, enter the FTP Server password.
9. Tab to the **Save** button and press <Enter>.

System Info Menu

System Information is the last menu option of the Main Menu. This feature is designed to provide users detailed system information about the KVM. This feature is available only to the Admin user, not to the regular user.

The System Information feature is available from both the OSD and the WMI. The type of retrievable information depends on the current conditions (e.g., connectivity, user, etc.) of the KVM unit.

The information that you can retrieve from the OSD may be classified as follows:

- Board
- Software version
- Memory
- CPU
- Time
- User 1 Connection
- User 2 Connection

To access System Information, follows the step below:

1. From the Main Menu, tab to the System Info and then press <Enter>.

The system displays the KVM system information.

An example of the system information that you can retrieve from the OSD is as follows:

```
1. Board:
KVM
Server ports: 32
User stations: 2
ID: B7DA3C0A000011
```

```
2. Version
Firmware: 1.1.0
Orig. Boot: 2.0.6
Alt. Boot: no code
SYS FPGA: 0x43
MUX FPGA: 0x5b
```

3: KVM OSD Configuration

3. Memory

RAM: 128 Mbytes
Flash: 16 Mbytes
RAM usage: 17%
RAMDISK usage: 100%

4. CPU

Clock: 48 MHz

5. Time

Mon Jul 19 2004 12:35:12 PDT
up 10 min

6. User1 connection

Int. uC, V1.0.4

7. User2 connection

RP main, V1.0.4
RP local, V1.0.4

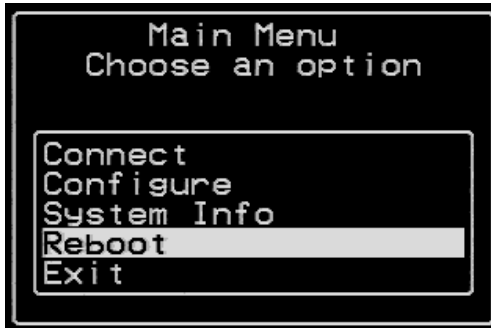
System Info Window

Below is an example of the System Info screen. Use the up and down arrow keys to view the information.

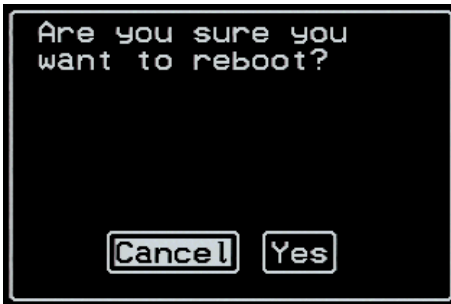


Reboot

To reboot the KVM/net switch, select Reboot from the Main Menu.



The system will display the following message:



Select **Yes** to complete the reboot command.

This page has been intentionally left blank.

Chapter 4

KVM Web Configuration

This chapter presents the procedures for configuring the KVM using the web management interface (WMI). It is organized as follows:

- Overview
- Types of Users
- Logging In
- KVM Web Management Interface
 - Configuring in Wizard Mode
 - Step 1: Network Settings
 - Step 2: Access
 - Step 3: System Log
 - Configuring in Expert Mode
 - Access
 - Configuration
 - Information
 - Management

Overview

This chapter is addressed to the System Administrator who is responsible for configuring and managing the KVM and its users, as well as to those users who are granted administrative access to configure the KVM through the web management interface.

While the main focus of this chapter is on the use of the KVM web interface, it also presents a few configuration procedures using vi, as necessary.

The KVM WMI provides two modes of operation: Wizard and Expert. The organization of the chapter follows, in sequential order, the two modes and the menu selections available from each mode.



*If you are a regular user, refer to **Chapter 5: KVM Operation**.*

Types of Users

The KVM has three types of users:

- root
- admin
- Generic User

Root User

Used for CLI configuration, root is the super user within the UNIX shell. This user cannot be deleted. If you are using the CLI to configure KVM, for security purposes, you must change the root password from the CLI as soon as convenient.

Admin User

Admin is the super user of the KVM WMI in admin mode. The admin or admin user has full read/write access to the WMI and shares with the root user the same default password, **cyclades**.

For security purposes, you must change your admin password as soon as you are logged in. To change the admin user password, go to **Step 2: Access** form of the WMI in Admin mode.

Generic User

The generic user is any user configured to operate the KVM in Access mode. They are responsible for managing alarms and consoles to which they are assigned. As configured by the administrator, a regular user may have admin privileges and therefore has also read/write access to the WMI in admin mode.

<i>User Type</i>	<i>Default Password</i>	<i>Environment</i>	<i>Default Permission Type</i>
root	cyclades	CLI only	Read/Write
admin	cyclades	KVM WMI in Wizard and Expert mode; KVM viewer and OSD	Read/Write
Generic User	as configured by the administrator.	KVM WMI in access mode; KVM viewer and OSD.	No access

Changing the Password

The table below summarizes the methods in which the different users can change their password.

<i>User Type</i>	<i>Where to change the PW</i>	<i>Who can change the PW</i>	<i>How</i>
root	CLI	root user	From system prompt, type in command, passwd , and follow system prompt. Then type in saveconf to save password.
admin	WMI and OSD	root user admin user	From WMI, go to: Configuration > KVM > Users & Groups. From OSD, go to Configure > Users and Groups > Local Users > Change Password.
Regular User	OSD	root user admin user	Same as above.

For more detailed information, refer to the Users and Groups section of this chapter and **Chapter 3: OSD KVM Configuration**.

Hierarchy of Permissions

By default, the Generic User has no access. Any user that you add inherits the access permissions of the Generic User. To override the access permissions of a Generic User, all you need to do is add the user to a group that has the desired permissions.

Conflicting Permissions

When the configured permission for a user in a group varies from the Generic User permission, the system will follow the user's group permission. In short, Group permissions supersede Generic User permissions.

If, for example, User X in Group A has Read/Write access, while the Generic User is configured as Read Only, then the system follows the permissions for Group A. User X should have Read/Write Access.

Complementary Permissions

With regards to port access, if the configured access permissions for a user in a group varies from the generic user, then the access permissions to these

ports are shared. This is true as long as both user types share the same permissions (e.g., Read/Write, Read Only).

For example, if Group A has Read/Write permissions to ports 2, 4, and 6 while the Generic User has Read/Write Permissions to ports 1, 3, and 5, then the system will provide both users (Group A and Generic User) Read/Write Access to ports 1, 2, 3, 4, 5 and 6.

Logging In



IMPORTANT: Take note of this login procedure. All subsequent online procedures in this chapter will assume that you are already logged in.

1. Connect your internet browser to the KVM web interface by typing in the KVM server's IP address (e.g., `http://10.0.0.0`) in the browser's address (URL) field.



To determine the IP address of your KVM, switch on the KVM connected to the Ethernet where there is a DHCP server. When you inquire, based on the MAC address (the 12-digit hexadecimal number located at the bottom of the KVM unit), the server will provide the appropriate IP address.

If there is no DHCP server, use the default static IP address that is pre-configured in the KVM: 192.168.160.10.

See the section on **Determining the IP Address, Chapter 2: KVM Installation**, for more detailed information.

The system brings up the AlterPath KVM Login page:



- Log in as **admin** and type in the password: **cyclades**
The system brings up the KVM web management page.
If another administrator is using the system, the following message appears:

Another administrator [admin] 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.

- Click on the appropriate radio button and then click on the **Apply** button.

Direct Access to a Port

If the Login page is configured to allow Direct Access to a port, then a third field, **port**, should appear on the **Login** panel of the **Login** screen.

Login

username

password

port

- From the port field, enter the port alias or the port number using the following format: **Port_[number]**
Example: Port_4
- Click on GO.
The system connects you to the port.

KVM Web Management Interface

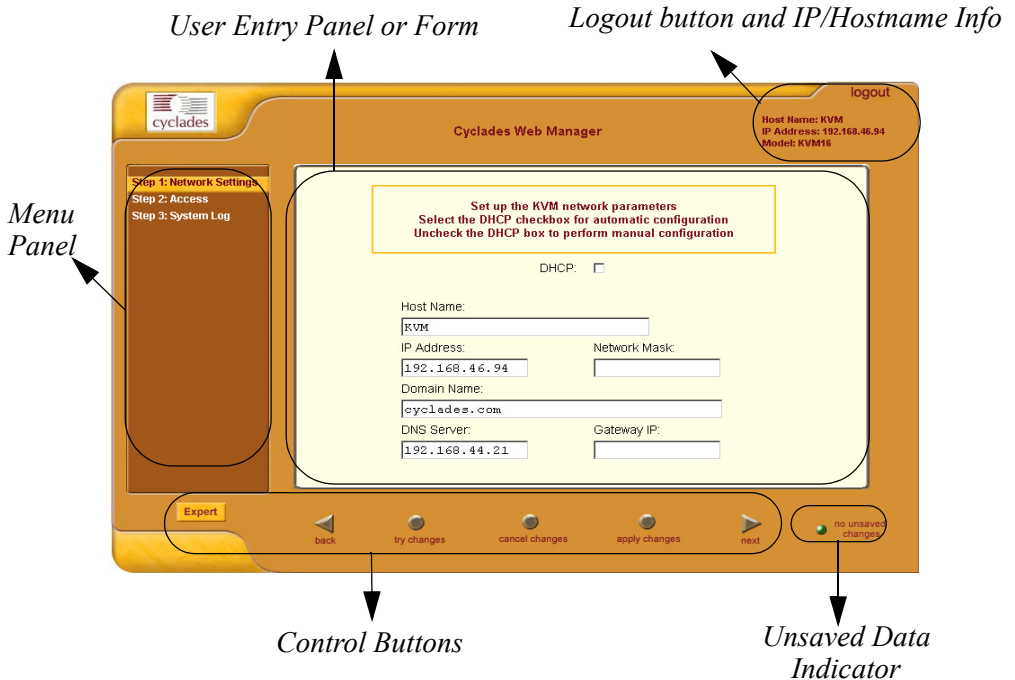
You can use the KVM web management interface in two modes:

- Wizard
- Expert

Wizard Mode

The wizard is designed to simplify configuration by providing users the default parameter values. The system will prompt you for the necessary fields, give instructions during the process and, in some cases, populate the fields automatically.

The Wizard Mode allows you to perform the basic configuration necessary to set up KVM and users in the quickest possible way. When you log on to KVM the first time, the system, by default, is in the Expert Mode. Make sure you select the **Wizard** button located at the bottom of the Menu Panel the first time you configure the web management interface.

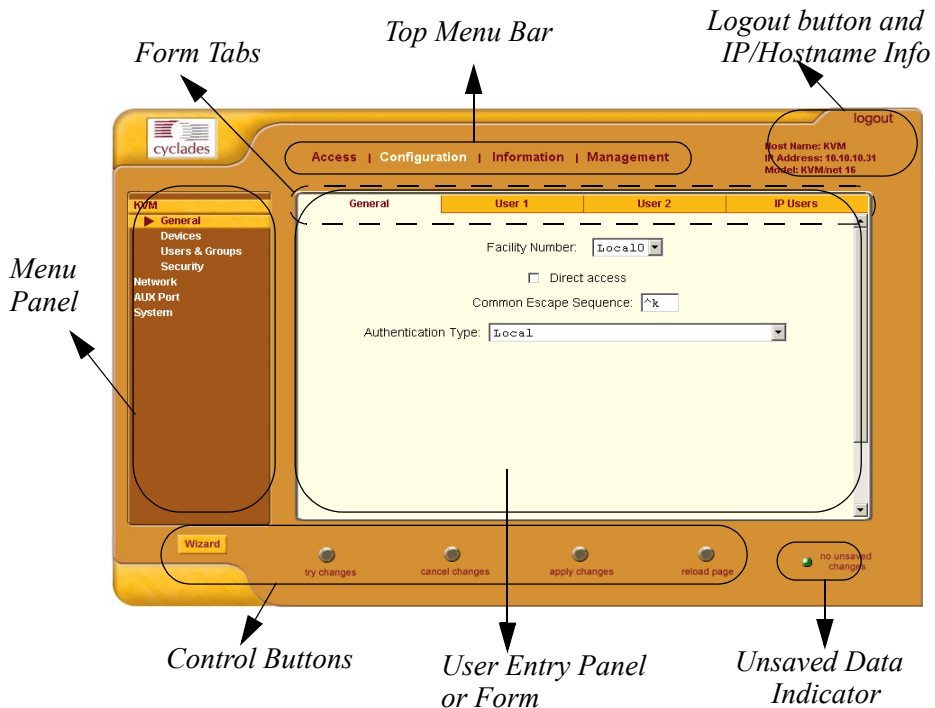


Shown in the previous page is a *typical* configuration window of the KVM web interface in Wizard Mode. The user entry panel or form varies depending on the selected menu item. The KVM uses forms and dialog boxes (*i.e.*, pop-up windows that prompt you for information) to receive your data input.

As mentioned, the web interface always starts from the Expert Mode. To configure in Wizard Mode, you must select the **Wizard** button.

Expert Mode

Designed for advanced configuration, clicking the **Expert** button at the bottom of the menu panel switches the web interface from Wizard to Expert Mode. Shown below is a typical KVM screen in Expert Mode. The Expert Mode adds a top menu bar to support a wider array of menu choices.



The top menu bar is the primary menu; the left menu panel is the secondary menu. Based on what you select from the top menu bar, the left menu selections will change accordingly.

Occasionally, an Expert Mode menu selection will comprise multiple forms such as the one shown above. These forms are identified by their tabs. Select the tab to access the form that you want.

Button Functions

The control buttons located at the bottom of the KVM Web Configuration window provide you the following functions for operating the interface.

<i>Button Name</i>	<i>Use this button to:</i>
Wizard / Expert	Switch the KVM Web Configuration Screen to either Wizard or Expert Mode. The Expert Mode is the default mode; in this mode, the Wizard button is visible and vice versa.
Try Changes	Test or run the system based on the settings from the current form without having to save the configuration.
Cancel Changes	Cancel your changes or reverts back to the original configuration values.
Apply Changes	Save your changes to the KVM Flash card.
Reload Page	Reloads or refreshes the current page.
Next	Traverse to the next screen or form.
Back	Return to the previous screen or form.
Help?	Invoke the online help sub window which provides help information relating to the current form.

Saving Your Configuration

The **Unsaved Changes** indicator on the lower right hand corner of the KVM web configuration window serves to remind you that you have made a configuration entry or change which has not been saved.



Unless you do not need to save your configuration, be sure to select the **Apply Changes** button to save your configuration to Flash.

Configuring in Wizard Mode

As shown in the menu, the Wizard Mode configuration is composed of three steps:

Step 1: Network Settings

Step 2: Access

Step 3: System Log

Step 1: Network Settings

The Network Settings form enables you to configure the KVM for networking. To configure the network settings for the KVM, follow the following steps:

1. From the main menu of the web interface, select **Step 1: Network Settings**.

The system brings up the DHCP page (shown below). By default, the DHCP checkbox is checked, which means that the system is configured to use a DHCP server for network configuration.



2. If DHCP is your preferred setting, proceed to **Step 2: Access**; if not, click on the checkbox to deselect DHCP and enter your network settings manually.

The Network Settings entry fields should appear as shown:

The screenshot shows the 'Cyclades Web Manager' interface for network configuration. The top left features the 'cyclades' logo and a 'logout' button. The top right displays system information: 'Host Name: KVM', 'IP Address: 192.168.46.94', and 'Model: KVM16'. A left sidebar contains a navigation menu with 'Step 1: Network Settings' (highlighted), 'Step 2: Access', and 'Step 3: System Log'. Below the menu is an 'Expert' button. The main content area has a yellow background with a central instruction box: 'Set up the KVM network parameters. Select the DHCP checkbox for automatic configuration. Uncheck the DHCP box to perform manual configuration.' Below this, there is a 'DHCP:' checkbox which is currently unchecked. The form includes several input fields: 'Host Name' (containing 'KVM'), 'IP Address' (containing '192.168.46.94'), 'Network Mask' (empty), 'Domain Name' (containing 'cyclades.com'), 'DNS Server' (containing '192.168.44.21'), and 'Gateway IP' (empty). At the bottom, there is a navigation bar with buttons for 'back', 'try changes', 'cancel changes', 'apply changes', and 'next', along with a 'no unsaved changes' indicator.

3. Type in the network information in the corresponding entry fields, and then select **Apply Changes**.
4. Select the **Next** button OR proceed to **Step 2: Access**.

Step 2: Access

The Access form allows you to add or delete users from the User Access List. It also allows you to set or change the password for each user.

1. From the main menu of the web interface, select **Step 2: Access**.

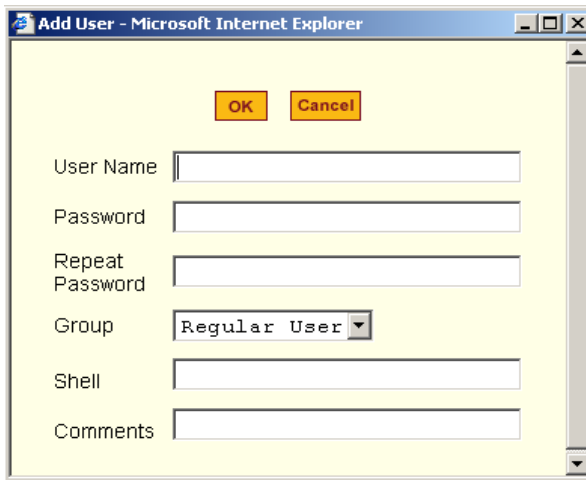
The system brings up the Access form:



The Access form is composed of a Users list box and three buttons: **Add**, **Change Password**, and **Delete**.

To add a User

1. From the Access form, select the **Add** button.
The system displays the **Add User** dialog box:



2. Type in the necessary information as follows:

<i>Field Name</i>	<i>Definition</i>
User Name	Name of the user to be added to the Access List.
Password	The user password required to access the port.
Repeat Password	As indicated.
Group	Optional. Select whether the user is a Regular User or an Admin .
Shell	Optional. The default shell the user will get when they ssh or telnet into the KVM. Choices are: sh or bash .
Comments	Optional. Notes pertaining to the current user or setting.

3. From the dialog box, select **OK** when done.
4. From the Access form, select **Apply Changes** to save your configuration.



To define a new user group, select the **Expert** button to switch to the Expert Mode, and then select **Configuration** (top menu) > **Users and Groups** (side menu).

To Delete a User

1. From the users list box of the Access form, select the user that you want to delete.
2. Click on the **Delete** button
3. Click on the **Apply Changes** button.

To Change a User's Password

*It is recommended that you change your admin password as soon as you begin configuring the KVM system. If you haven't changed your password, now is the time to change it using the **Change User Password** dialog box.*

1. From the Users List box of the Access form, select the user whose password you would like to change.
2. Select the **Change Password** button.
The system displays the Change User Password dialog box:

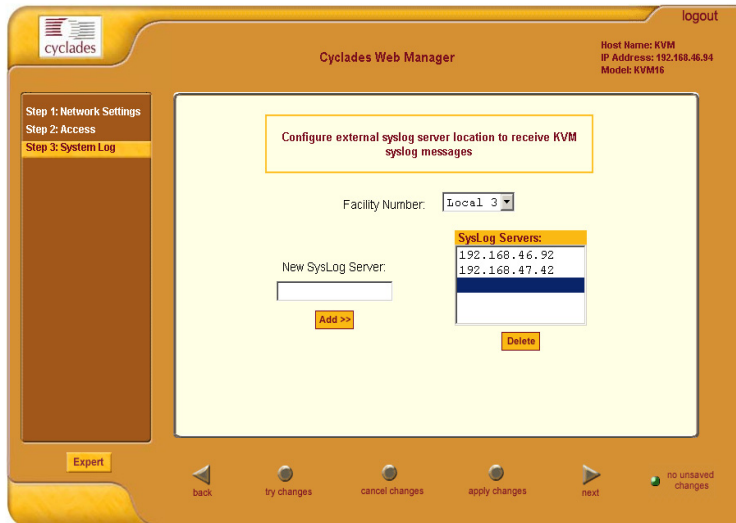
3. Enter the password in both fields and then click **OK**.
4. From the Access form, select **Apply Changes** to save your configuration.

Step 3: System Log

The System Log form is used to assign or add syslog servers to external server locations. These servers receive KVM syslog messages. You can also delete the servers from their locations.

1. Select Step 3: System Log from the main menu.

The system brings up the System Log form:



To Add a Syslog Server

1. From the **Facility Number** dropdown list, select the facility number from which you want to configure your syslog servers.
2. From the New Syslog Server field, enter the IP address of the syslog server that you are adding, and then select the Add button. (Repeat this step for as many servers you need to add.)

The new server appears in the Syslog Servers list box.

3. Select **Apply Changes** to save your configuration.

To Delete a Syslog Server

1. From the **Facility Number** dropdown list, select the facility number from which you want to configure your syslog servers.

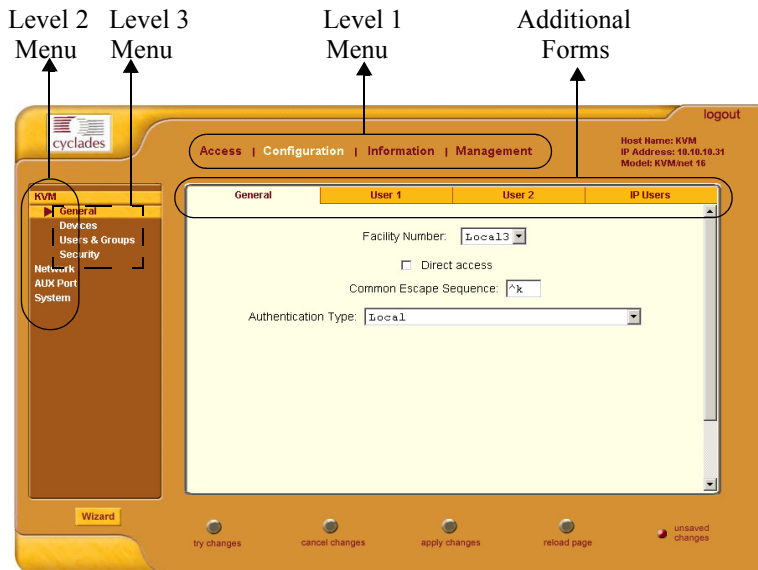
- From the Syslog Server list box, select the syslog server that you want to delete from the current facility location, and then select **Delete**. (Repeat this step for as many servers you need to delete.)
- Select **Apply Changes** to save your configuration.

Configuring in Expert Mode

This section presents the procedures for configuring the KVM web interface in Expert Mode. This mode is designed for the admin user who needs to configure the KVM beyond the capabilities of the basic wizard mode. A main difference between the two modes is the addition of a top menu bar in the Expert Mode to support a wider array of menu choices.

The top menu bar is the primary menu; the left menu panel is the secondary menu. Based on what you select from the top menu bar, the selections from the left menu panel changes accordingly.

Additionally, the left menu selection can have child windows or forms which are presented as tabbed forms within the initial form or as a second column (Level 3 menu) in the left menu panel.



Typographically, the menu path for, say, the **User 2** form would be:
Configuration > KVM > General > User 2.

Table of Menu and Forms

The forms that compose the entire configuration interface in Expert Mode are as follows:

<i>Menu Selection</i>	<i>Form Name</i>
Access	
> Connect to Server	<i>This is a form by itself.</i>
> Power Management	Outlets Manager (tab 1)
	View IPDUs Info (tab 2)
	Users Manager (tab 3)
	Configuration (tab 4)
	Software Upgrade (tab 5)
Configuration	
> KVM	General (tab 1)
	User 1 (tab 2)
	User 2 (tab 3)
	IP Users (tab 4)
	Devices
	Users & Groups
	Security
> Network	Host Settings
	Syslog
	Services
	IP Filtering
	VPN
	SNMP
	Host Table
	Static Routes
> AUX(iliary) Port	<i>This is a form by itself.</i>
> System	Date/Time
	Boot
Information	
> General	<i>This is a form by itself.</i>
> Port Status	<i>This is a form by itself.</i>

<i>Menu Selection</i>	<i>Form Name</i>
Management	
> Backup Configuration	<i>This is a form by itself.</i>
> Firmware Update	<i>This is a form by itself.</i>
> Microcode Update	<i>This is a form by itself.</i>
> Microcode Reset	<i>This is a form by itself.</i>
> Active Sessions	<i>This is a form by itself.</i>
> Reboot	<i>This is a form by itself.</i>



Most of the form fields are defined in the procedure section of each form. For a more detailed definition of the field names or terms, refer to the **Glossary** of this manual.

Access

The **Access** form is used by a regular or admin user to select and access ports as well as to view power management (IPDU settings) information. The first selection, **Connect to Server**, is designed for the KVM regular user and is discussed in more detail in **Chapter 5: KVM Operation**.

Access

<i>Menu Selection</i>	<i>Use this form to:</i>
Connect to Server	Select and connect to a port.
Power Management	View and edit IPDU settings. This menu comprises five tabbed forms: Outlets Manager, View IPDUs Info, Users Manager, Configuration, and Software Upgrade.

Power Management

Power Management comprises five tabbed forms, which are designed to configure any Cyclades AlterPath Power Manager unit connected to the KVM switch.

<i>Menu Selection</i>	<i>Use this form to:</i>
Outlets Manager	Switch on/off and lock/unlock outlets; reboot network devices.
View IPDUs Info	View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.
Users Manager	Add or delete users assigned to specific outlets.
Configuration	Enable over current protection, syslog and alarm notification from any specified port. The form allows you to set a current alarm threshold that, once exceeded, will have the KVM sound an alarm or send a notification message.
Software Upgrade	Upgrade the AlterPath Power Manager software.

Power Management > Outlets Manager

The **Outlets Manager** form allows you to check the status of all IPDUs connected to the Console Server including their outlets. Any user who has Administration privileges can turn on, turn off, cycle (*i.e.*, to automatically switch off and on), lock, and unlock the outlets.

1. From the top menu, select **Access**; from the left menu, select **Power Management**.

The system displays the **Outlets Manager** tabbed form:

The screenshot displays the 'Outlets Manager' interface. At the top, there is a navigation bar with 'Access | Configuration | Information | Management' and a 'logout' link. The left sidebar shows 'Connect to Server' and 'Power Management'. The main content area has tabs for 'Outlets Manager', 'View IPDUs Info', 'Users Manager', 'Configuration', and 'Software Upgrade'. The 'Outlets Manager' tab is active, showing a table with the following data:

Outlet	Outlet Name	Outlet State	Power Up Interval
1	out1	Yellow lightbulb icon, Open padlock icon	0.50
2	out2	Yellow lightbulb icon, Open padlock icon	0.50
3	out3	Yellow lightbulb icon, Open padlock icon	0.50
4	out4	Yellow lightbulb icon, Open padlock icon	0.50
5	out5	Yellow lightbulb icon, Open padlock icon	0.50
6	out6	Yellow lightbulb icon, Open padlock icon	0.50
7	out7	Yellow lightbulb icon, Open padlock icon	0.50
8	out8	Yellow lightbulb icon, Open padlock icon	0.50

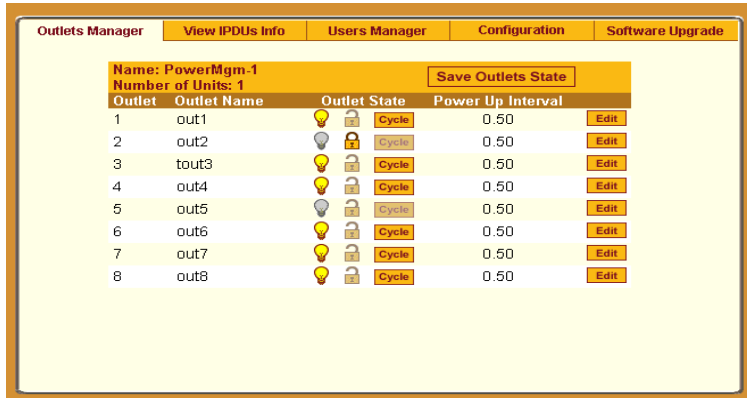
At the bottom of the interface, there are buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'no unsaved changes'.

In the example above, the yellow bulbs and the opened padlock indicate that the outlets are switched on and unlocked, respectively.

















4: KVM Web Configuration

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

In the sample form below, outlet 1 has been locked and outlet 2 has been switched off and locked.



The screenshot shows the 'Outlets Manager' configuration window. At the top, there are navigation tabs: 'Outlets Manager', 'View IPDUs Info', 'Users Manager', 'Configuration', and 'Software Upgrade'. Below the tabs, the window title is 'Name: PowerMgm-1' and 'Number of Units: 1'. A 'Save Outlets State' button is located in the top right corner. The main content is a table with the following columns: 'Outlet', 'Outlet Name', 'Outlet State', 'Power Up Interval', and 'Edit'.

Outlet	Outlet Name	Outlet State	Power Up Interval	Edit
1	out1	  Cycle	0.50	Edit
2	out2	  Cycle	0.50	Edit
3	tout3	  Cycle	0.50	Edit
4	out4	  Cycle	0.50	Edit
5	out5	  Cycle	0.50	Edit
6	out6	  Cycle	0.50	Edit
7	out7	  Cycle	0.50	Edit
8	out8	  Cycle	0.50	Edit

3. To save your changes, click on the **Save Outlets State** button located in the form.
4. Click on the **Apply Changes** button located at the bottom of the configuration window.

Power Management > View IPDUs Info

The IPDU Info form allows you to view all IPDU information (e.g., number of outlets for each unit, current, temperature, alarm threshold levels, and firmware) by serial port.

The form stores historical values of the maximum current and the maximum temperature.

To view the IPDU information, perform the following steps:

1. From the top menu, select **Access**; from the left menu panel, select **Power Management**; from the form tabs, select **View IPDUs Info**.

The system brings up the **IPDUs Info** form:

The screenshot shows a web interface with a top navigation bar containing five tabs: 'Outlets Manager', 'View IPDUs Info' (which is selected), 'Users Manager', 'Configuration', and 'Software Upgrade'. Below the tabs, the main content area is titled 'Serial Port 4: General Information'. This section includes two buttons: 'Clear Max Detected Current' and 'Clear Max Detected Temperature'. The information displayed is as follows:

Name: PowerMgm-4	Syslog: ON	Number of Outlets: 8
Number of Units: 1	Buzzer: ON	Over Current Protection: OFF
Master Unit Information:		
Model: PM8 15A	Software Version: 1.2.0	
Alarm Threshold: 15.0A		
Current: 0.0A	Maximum Detected: 0.4A	
Temperature:	Maximum Detected:	

2. To delete the stored values for the maximum detected current, select the **Clear Max Detected Current** button.
3. To delete the stored values for the maximum detected temperature, select the **Clear Max Detected Temperature** button.

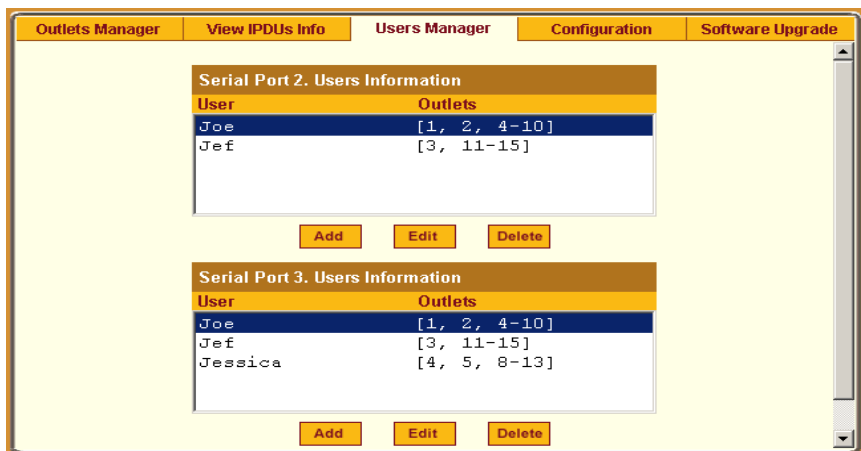
Power Management > Users Manager

The Users Management form of Power Management allows you to assign users to selected outlets for each KVM port and vice versa.

To add a user or edit an assigned user:

1. From the top menu bar, select **Access**; from the left menu panel, select **Power Management**; from the tabs, select **Users Manager**.

The system brings up the **Users Manager** form:

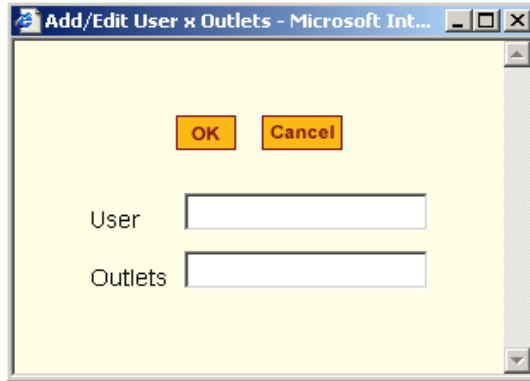


2. To edit an assigned user, select the user you wish to edit from the Serial Port view table and then select the **Edit** button that corresponds to the table.

- OR -

To add or assign a new user select the **Add** button from the appropriate KVM Port view table.

The system brings up the **Add/Edit User x Outlet** dialog box:



3. From the resulting dialog box, modify or enter in the corresponding fields the user and the outlets to which the user is assigned, and then select the **OK** button.



*In the **Outlets** field, use the comma to separate each outlet; use the hyphen to indicate a range of outlets (e.g., 1, 3, 6, 9-12).*

*Selecting **Edit** will not allow you to edit or delete the user, only the outlet assignments for that user.*

4. Verify your entry by checking the appropriate Serial Port table from the Users Manager form.
5. Select the **Apply Changes** button located at the bottom of the Access Power Management form.

To delete an assigned user

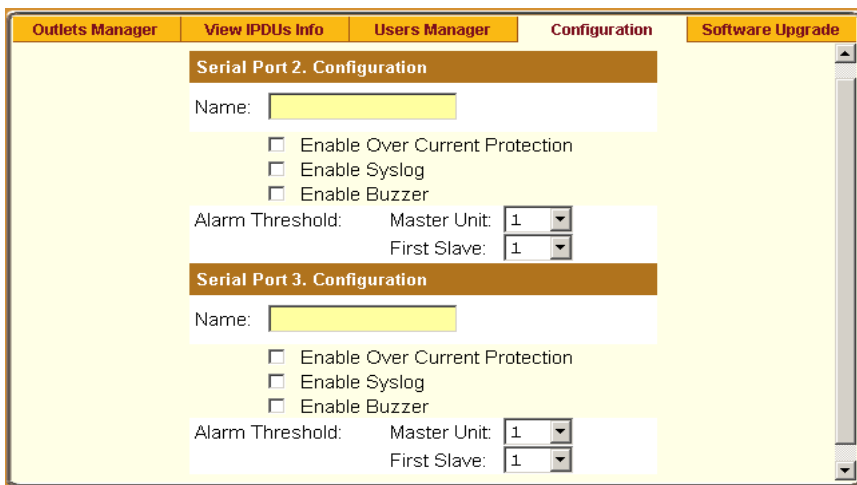
1. Select the user you wish to delete from the appropriate KVM Port view table.
2. Based on the KVM Port view table that you are working on, select the corresponding **Delete** button.

Power Management > Configuration

To configure IPDUs to generate alarms or syslog files, perform the following steps:

1. From the top menu, select **Access**; from the left menu panel, select **Power Management**; from the default Outlets Manager form select the **Configuration** tab.

The system brings up the Configuration form:



The screenshot shows a web interface with a top navigation bar containing five tabs: "Outlets Manager", "View IPDUs Info", "Users Manager", "Configuration", and "Software Upgrade". The "Configuration" tab is active. Below the tabs, there are two configuration sections. The first section is titled "Serial Port 2. Configuration" and contains a "Name:" field with a yellow input box, three checkboxes for "Enable Over Current Protection", "Enable Syslog", and "Enable Buzzer", and an "Alarm Threshold:" section with "Master Unit:" and "First Slave:" dropdown menus, both set to "1". The second section is titled "Serial Port 3. Configuration" and contains identical fields and options as the first section.

2. From the Configuration form, select the KVM Port you wish to configure and then click on the appropriate radio buttons to enable/disable Over Current Protection, Syslog, and Buzzer.
3. If enabling the buzzer or alarm notification, provide the Alarm Threshold (1-100 amps) for that primary or secondary unit.
4. Click on the **Apply Changes** button at the bottom of the form.

Power Management > Software Upgrade

The **Software Upgrade** form of Power Management allows you to upgrade the Power Management software for a selected serial port. The first line of the form shows the **latest software version available**. The presence of an **Upgrade** button indicates that a new software version for that master or slave port is available.

To upgrade the software for a selected port, perform the following steps:

1. From the top menu, select **Access**; from the left menu, select **Power Management**; from the tabs, select **Software Upgrade**.

The system brings up the **Software Upgrade** form:

Serial Port 1:	Name: PowerMgm-1	Number of Units: 2
Master Unit		
Software Version: 1.3.0		
Slave 1:		
Software Version: 1.3.0		

2. Select the **Refresh** button to ensure that all software information on the form is up-to-date.
3. From the Software Version list, select the software you wish to update, and then select the **Update** button to the right of the listed version.



*The above form example does not have an **Update** button associated with any of the software versions listed which means that they are up-to-date and there is no need to update them.*

4. Select the **Apply Changes** button at the bottom of the configuration window to save your configuration.

Configuration

Configuration, the second primary menu selection, is composed of four menu selections with the following child menus and forms:

- **KVM - General** (composed of four tabbed forms), Devices, Users & Groups, and Security)
- **Network** - Host Settings, Syslog, Services, IP Filtering, VPN, SNMP, and Host Table.
- **AUX Port** - no other forms associated.
- **System** - Date/Time and Boot

KVM

Composed of four tabbed forms, the first selection allows you to configure the following KVM settings:

<i>Form Name</i>	<i>Use this form to:</i>
General	Define the Facility Number (i.e., the location of the managed server/s), IP settings, and authentication type.
User 1	Configure the first user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands or escape sequences.
User 2	Configure the second user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands or escape sequences.
IP Users	Configure the web user's console and keyboard settings: Idle Timeout, Screen Saver Timeout, and various key commands or escape sequences.

Default Key Sequences

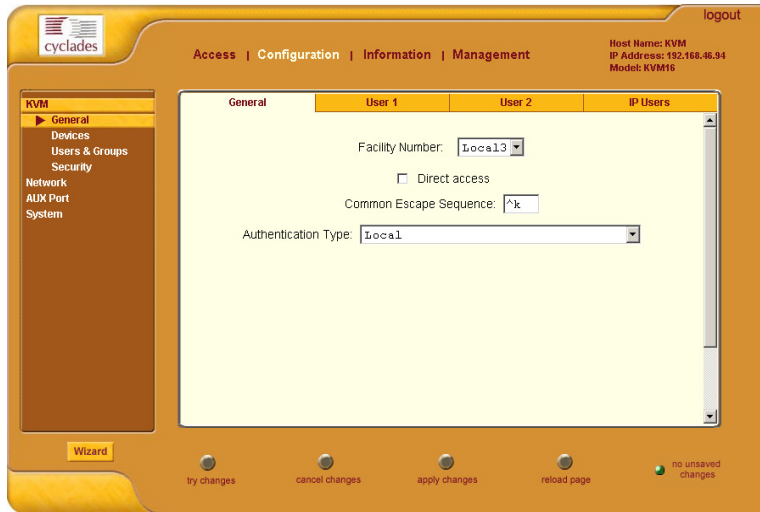
A main component of the KVM settings is defining the key sequences for users when using the AlterPath Viewer. A *key sequence* (also known as *escape sequence*) is a sequence of special characters used to send a command to a device or program. In this case the escape sequence is sent to the KVM application. Typically, an escape sequence begins with an escape character.

Aside from the navigation keys listed above, you can use the following key sequences to perform a specific action:

<i>Key Sequence</i>	<i>Action</i>
Ctrl-K, and then Q	Quit command - closes the session to a port and takes you back to the KVM Main Menu.
Ctrl-K, and then P	Port command - initiates a power control session.
SCROLL LOCK twice, and then L	RP Switch to Local command - switches the Alter-Path KVM RP video display to the local computer.
SCROLL LOCK twice, and then R	RP Switch to Remote command - switches the Alter-Path KVM RP video display to the remote computer.
Ctrl-K, and then C	KVM Switch command - switches from the currently connected server to the next server that you are authorized to access.
Ctrl-K, and then V	Video command - controls screen brightness and contrast.
Ctrl-K, and then S	Keyboard and Mouse Synchronization command - resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM.

1. To configure the KVM Settings from the top menu, select **Configuration**; from the left menu, select **KVM**.

The system displays the first of four forms under KVM which is the **General** form:



2. From the **General** form, complete the data entry fields as follows:

<i>Field Name</i>	<i>Definition</i>
Facility Number	Define the Facility Number (i.e., the location of the managed server/s).
Direct Access	Select this check box to enable direct access to a port as the user logs in from the Login screen.
Common Escape Sequence	The recommended key combinations are the control key followed by a letter key (e.g., Ctrl + Q).
Authentication Type	Choice of authentication services are: None, Local, Radius, TacacsPlus, Ldap, Kerberos, and NTLM. NOTE: See Appendix B for more detailed information about LDAP and Kerberos authentication.

3. Click on Apply Changes to save your configuration.
4. If you need to configure another facility, select a new Facility Number and then repeat steps 2 and 3.

- OR -

Proceed to the next form by clicking on the **User 1** tab.
The system brings up the **User 1** form:

The **User 1** form is used to configure the first user's console and keyboard settings.

- From the **User 1** form, complete the data entry fields as follows:

<i>Field Name</i>	<i>Definition</i>
Idle Timeout	The time (in minutes) it takes the system to timeout after it remains idle.
Screen Save Timeout	The time (in minutes) it takes for the screen saver to activate after the system remains idle.
Keyboard Type	From the drop-down list, select the keyboard type assigned to User 1.
Quit	Key sequence for quit.
Power Management	Key sequence for Power Management.
Mouse/Keyboard Sync	Key sequence for M/K synchronization.
Video Control	Key sequence for video control.
Switch Next	Key sequence for switching to the next screen.
Switch Previous	Key sequence for switching to the previous screen.
Port Info	Key sequence for invoking the Port Information screen.

- Click on **Apply Changes** to save your configuration.

7. Proceed to the next form by clicking the **User 2** tab. The system brings up the **User 2** form:

The screenshot shows the 'User 2' configuration form. At the top, there are four tabs: 'General', 'User 1', 'User 2', and 'IP Users'. The 'User 2' tab is selected. The form contains the following fields:

- Idle Timeout:
- Screen Saver Timeout:
- Keyboard type:
- Escape Sequences** section:
 - Quit:
 - Power Management:
 - Mouse/Keyboard Sync:
 - Video Control:
 - Switch Next:
 - Switch Previous:
 - Port Info:

The **User 2** form is used to configure the second user's console and keyboard settings.

8. Complete the data entry fields for **User 2** and then click on the **Apply Changes** button to save your configuration. For a definition of the fields, see the field definition table from step 5.
9. Proceed to the next form by clicking on the **IP Users** tab. The system brings up the **IP Users** form:

The screenshot shows the 'IP Users' configuration form. At the top, there are four tabs: 'General', 'User 1', 'User 2', and 'IP Users'. The 'IP Users' tab is selected. The form contains the following fields:

- Idle Timeout (min):
- TCP Viewer Ports:
- Escape Sequences** section:
 - Quit:
 - Power Management:
 - Mouse/Keyboard Sync:
 - Video Control:
 - Switch Next:
 - Switch Previous:
 - Port Info:

The **IP Users** form is used to configure the following web user's console and keyboard settings.

10. Complete the data entry fields for Web User and then click on the **Apply Changes** button to save your configuration.

Configuring the TCP Viewer Ports Address

By default, if no addresses are specified, the system automatically assigns the available port addresses to the KVM starting at 5900. When an additional port is added, the system automatically assigns the address 5901. To override this default, you can assign your own port address to the KVM through the IP Users form.

To configure the TCP viewer ports address, follow the procedure below:

1. In the **TCP Viewer Ports** field of the **IP Users** form, type in the available TCP port address of your choice using any of the following methods:
Use the plus sign (+) to assign a TCP port address which will be incremented by 1 for each additional TCP port that is added (*e.g.*, 5903+).
Use the hyphen (-) to indicate a range of addresses (*e.g.*, 5903-5907)
Use the comma (,) to separate two TCP port addresses. (*e.g.*, 5901,5903)
Combine commas and hyphens, as necessary (*e.g.*, 1901,5903-5905,5907).
2. Click the Save button to save your configuration.

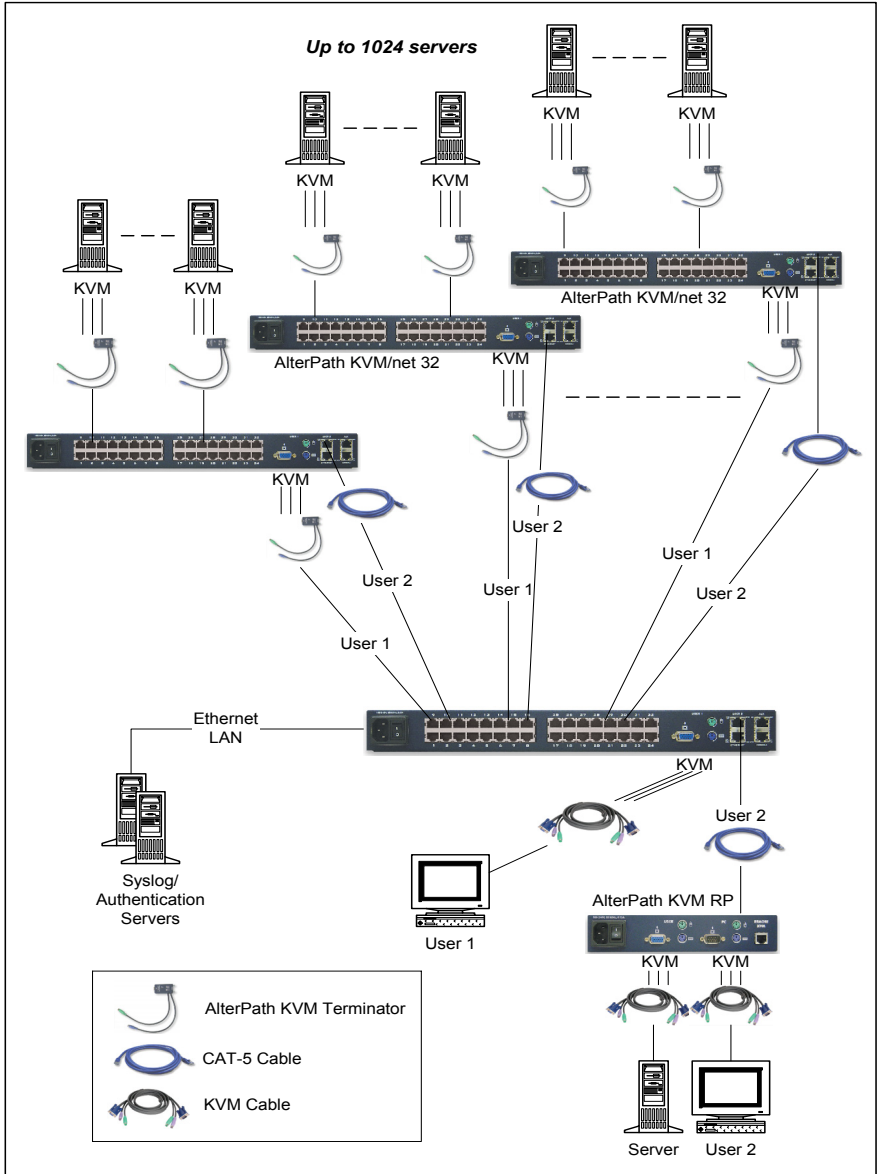
Verifying the TCP Port Address

If you need to verify the new address, follow the procedure below:

1. Log onto the KVM web management interface.
2. Access an output port on the KVM.
3. From a command prompt window, enter the command: **netstat -n**
The system should display the TCP port address(es) that you assigned to the KVM.

Devices

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*. The diagram below illustrates cascading:



If you already understand cascading, skip this introduction and proceed to the procedural sections.

Cascading refers to the multiple connections of slave or secondary devices to a primary KVM for as many allowable tiers or hierarchies. For example, a 2-tier, cascaded configuration can have secondary KVM units connected to a primary KVM. The diagram below shows a basic cascaded configuration of a primary KVM 32 with all KVM components.

Using the KVM 32, 32 primary KVM units or switches can be cascaded for a total of up to 32 units (regardless of how many times they are cascaded). A 2-user configuration can control up to 512 servers; a single user, up to 1024 servers (*i.e.*, from a single keyboard-monitor-mouse console, either locally or remotely through the ethernet LAN).

To add a secondary KVM to be cascaded to a master KVM:



IMPORTANT: *When physically cascading with only one user, ensure that the CAT-5 cable is connected to **USER 2** of the secondary KVM switch since connecting a CAT-5 single user to **USER 1** will not work.*



*In the KVM Expander, **User 1** is **User A**; **User 2** is **User B**.*

1. From the top menu, select **Configuration**; from the side menu, select **Devices**.

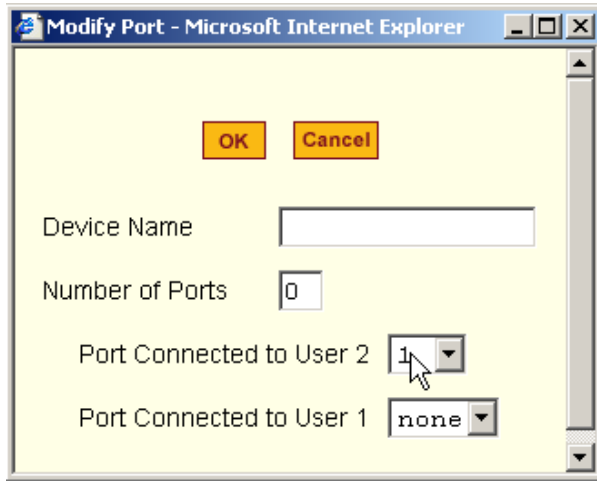
The system displays the **Devices** configuration form:

The screenshot shows the KVM web configuration interface. The top navigation bar includes "Access | Configuration | Information | Management" and a "logout" link. The left sidebar menu is expanded to "Devices". The main content area displays a table with the following data:

Device Name	Physical ID	Number of Ports
master		16
sa	master:1	32

Below the table are four buttons: "Edit Device", "Delete Device", "Add Device", and "Ports". At the bottom of the interface, there are four status indicators: "try changes", "cancel changes", "apply changes", and "reload page". A "no unsaved changes" indicator is also present.

- From the **Devices** configuration form, select the **Add** button. The system brings up the **Modify Port** dialog box:



- Complete the dialog box as follows:

<i>Field Name</i>	<i>Definition</i>
Device Name	Name of the secondary device or KVM switch.
Number of Ports	Number of ports contained in the device to be cascaded.
Port Connected to User 2	The secondary KVM port to be connected to the User 2 port of the primary KVM.
Port Connected to User 1	The secondary KVM port to be connected to the User 1 port of the primary KVM.

- Select the **OK** button when done.
- From the configuration window, select **Apply Changes** to save your configuration.



You must connect to **USER 2** of the secondary KVM switch (**User B** of the Expander) the port to be used for cascading from the primary KVM. In a 2-user arrangement, in addition to connecting to **USER 2** of the cascaded KVM switch, use a PS2 Terminator to connect from a port on the primary KVM switch to **USER 1** of the secondary KVM switch (**User A** of the Expander).

To edit a device configuration:

1. From the top menu, select **Configuration**; from the side menu, select **Devices**.
The system brings up the **Devices** configuration form.
2. From the Device list box, select the line item you wish to edit, and then select the **Edit** button.
The system brings up the Modify Port dialog box which is similar to the dialog box used for adding a port.
3. From the dialog box, modify the configuration as necessary (see field definition table from the preceding procedure), and then select the **OK** button.
4. From the configuration window, select **Apply Changes** to save your configuration.

To delete a device configuration:

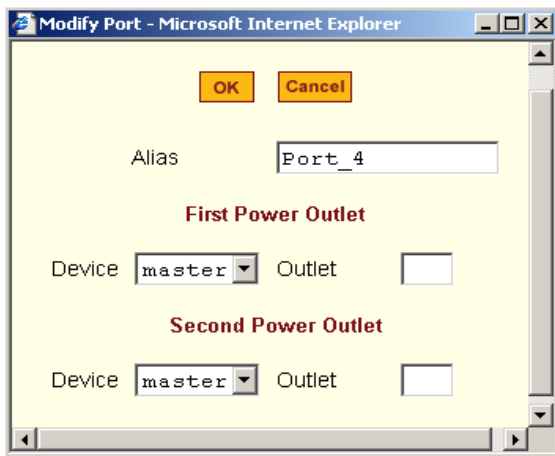
1. From the top menu, select **Configuration**; from the side menu, select **Devices**.
The system brings up the Cascading configuration form.
2. From the Device list box, select the line item you wish to delete, and then select the **Delete** button.
The system deletes the selected line item from the Device list box.
3. From the configuration window, select **Apply Changes** to save your configuration.

To Configure Ports

The Ports dialog box is used to modify the power outlet assignments for each port connected to the KVM, as well as to enable/disable the ports.

1. From the Devices form (**Configuration > KVM > Devices**), select the Device that contains the port(s) to be configured.

The system brings up the Modify Port dialog box:



2. Enter the Device and Outlet information, as necessary, and then select the **OK** button.
3. Select the **Apply Changes** button to save your configuration.

To Enable or Disable a Port

1. From the **Devices** configuration form (**Configuration > KVM > Devices**), select the device that contains the port(s) you wish to enable or disable.
2. From the resulting dialog box, select the ports to be enabled/disabled, and then select the **Enable** or **Disable** button.
3. Verify your configuration change by checking the port status from the Ports list box.
4. Select the **Apply Changes** button to save your configuration.

Users & Groups

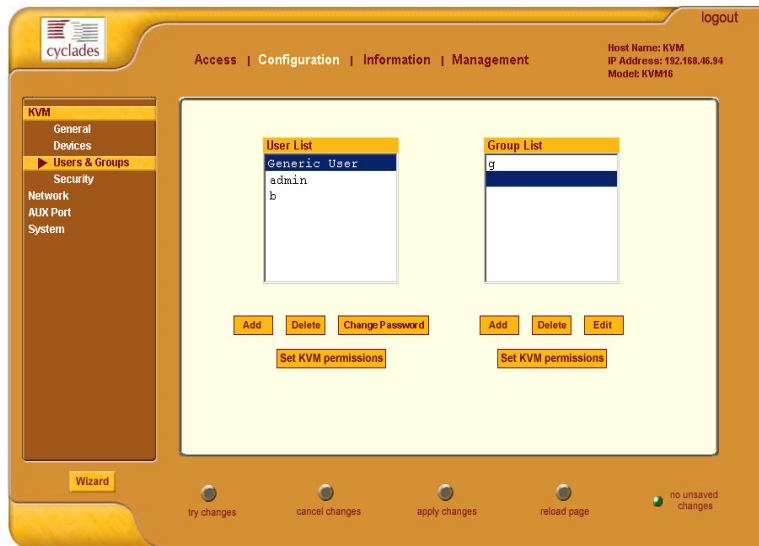
The **Users & Groups** configuration form allows you to:

- Set specific KVM permissions (*i.e.*, by individual port) for each user.
- Assign or change user passwords.
- Add or delete users from the User Access List.
- Set specific KVM permissions by group.
- Add or delete user groups from the Group Access List.

To set KVM permissions for a user or a group:

1. From the top menu, select **Configuration**; from the side menu, select **KVM > Users & Groups**.

The system invokes the **Users & Groups** configuration form:



2. From the **User List** box, select the user to be configured for KVM permissions.
- OR -
From the **Group List** box, select the group to be configured for KVM permissions.
3. Select the corresponding **Set KVM Permissions** button.

The system displays the Set KVM Permissions form:

KVM Access List for user a

Default Access List

Default Permission: Full access

Device	Permissions
master	-

4. Complete the form as follows:

<i>Field Name</i>	<i>Definition</i>
Default Access List	Select this check box if you want to include the current user to the default Access List.
Default Permission	The default permission for the current user.
[Device view list]	List of devices and type of permission for each device.
Set Permissions for the Device	Button to invoke a dialog box to set or reset the permission for a selected device (from the Device view list).

5. Select **OK** when done.
6. Select **Apply Changes** at the bottom of the configuration window.

To delete a user/group from the Access List:

1. Go to **Configuration > KVM > Users & Groups**.
2. To delete a user, select the user to be deleted from the **User List** box
- OR -
To delete a group, select the group name to be deleted from the **Group List** box.
3. Select the corresponding **Delete** button.
4. Verify your deletion by checking the list box.
5. Select **Apply Changes** to save your configuration change.

To add a user/group to the Access list (to access KVM ports):

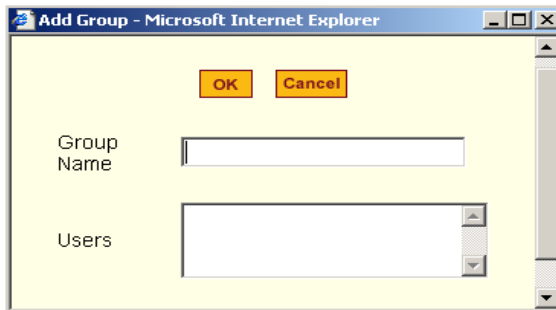
1. Go to **Configuration > KVM > Users & Groups**.
2. To add a user or a group to the Access list, select the appropriate **Add** button.
If you selected the **Add** button for the User List, the Add User dialog box appears as follows:

The screenshot shows a web browser window titled "Add User - Microsoft Internet Explorer". The main content area is yellow and contains a form with the following elements:

- Two buttons at the top: "OK" and "Cancel".
- A "User Name" text input field.
- A "Password" text input field.
- A "Repeat Password" text input field.
- A "Group" dropdown menu with "Regular User" selected.
- A "Shell" text input field.
- A "Comments" text input field.

Use the above dialog box for entering single users. For multiple users within a group, use the Add Group dialog box and use a comma (,) to separate each username.

If you selected the **Add** button for the Group List, the Add Group dialog box appears as follows:



3. Complete the fields, as necessary. For multiple users, use a comma (,) to separate each user in the **Users** entry text box.
4. Click on **OK**.
5. From the configuration window, select **Apply Changes** to save your configuration.

To change a user's password

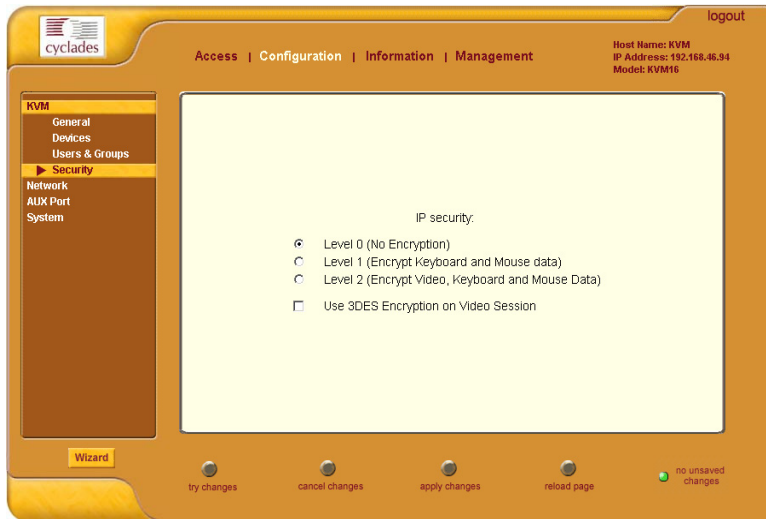
1. Go to **Configuration > KVM > Users & Groups**.
2. From the **User List** box, select the user whose password you would like to change, and then select the **Change Password** button.
The system brings up the Change User Password.
3. From the dialog box, type in the new password twice, and then select the **OK** button.
4. From the configuration window, select the **Apply Changes** button to save your configuration.

Security

The Security form allows you to configure your IP security.

1. From the top menu, select **Configuration**; from the side menu, select **KVM > Security**.

The system displays the Security form:



2. Check the appropriate radio buttons.



The system uses RC4 as the default encryption if 3DES is not selected.

3. Select the **Apply Changes** button to complete the procedure.

Network

Network configuration (which is the second of four primary options that belong to the top **Configuration** menu) comprises eight forms:

<i>Form</i>	<i>Use this form to:</i>
Host Settings	Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.
Syslog	Define the Syslog Servers to enable system logging.
Services	Define or activate the method of access (<i>i.e.</i> , Telnet, SSH, SNMP, Client, or NTP).
IP Filtering	Configure the selective filtering of packets that may potentially crack your network system or generate unnecessary traffic.
VPN	Configure IPsec tunnels to establish a secure connection between KVM and a security gateway machine.
SNMP	Configure the SNMP server to manage complex networks.
Host Table	View hosts list; create, edit, and delete hosts.
Static Routes	View, create and delete routes from the table.

Network > Host Settings

The Host Settings form allows you to configure the network settings for the KVM.

1. From the top menu, select **Network**; from the side menu, select **Host Settings**.

The system brings up the **Host Settings** form:

The screenshot shows the KVM web interface. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The side menu on the left is expanded to 'Host Settings'. The main content area displays the 'Host Settings' form with the following fields:

- DHCP
- Host Name:
- Console Banner:

At the bottom of the form, there are five buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'no unsaved changes' (with a green indicator).

2. By default, the DHCP field is check marked. If you wish to disable DHCP and enter the host settings manually, click the checkbox to remove the check mark.

The system should add the following fields to your form:

The screenshot shows the 'Host Settings' form with the following fields:

- DHCP
- Host Name:
- Console Banner:
- Ethernet Port**
- Primary IP:
- Network Mask:
- Secondary IP:
- Secondary Network Mask:
- MTU:
- DNS Service**
- Primary DNS Server:
- Secondary DNS Server:

- From the Host Settings form, complete or edit the following fields, as necessary:

<i>Field Name</i>	<i>Definition</i>
DHCP	This default configuration is used if you are using DHCP for your network settings.
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.
<i>Ethernet Port</i>	
Primary IP	The 32-bit numeric IP address of the KVM unit on the Internet.
Network 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 KVM unit on the Internet.
Secondary Network Mask	The network mask of the secondary IP.
MTU	Maximum Transmission Unit used by the TCP protocol.
<i>DNS Service</i>	
Primary DNS Server	Address of the Domain Name Server.
Secondary DNS Server	Address of the backup Domain Name Server.
Domain Name	The name that identifies the domain (e.g., domainname.com).
Gateway IP	The gateway numeric identification number.

- Select **Apply Changes** when done to save your configuration to flash.

Network > Syslog

The Syslog form allows you to configure one or more syslog servers to receive KVM-generated syslog messages. The KVM generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit trailing purposes. You can also use this form to delete syslog servers.

This form is the same as **Step 5: System Log** form in Wizard mode.

1. From the top menu, select **Configuration**; from the left menu, select **Network > Syslog**.

The system brings up the **Syslog** form.

2. Complete the form as follows:

<i>Field Name</i>	<i>Definition</i>
Facility Number	Facility number to identify the location of the Syslog Server.
New Syslog Server	Name of the Syslog Server that you wish to add.
Syslog Servers	List of all Syslog Servers connected to the KVM.

3. Select **Apply Changes** when done.

Network > Services

By selecting the appropriate box, the Services form allows you to enable or disable the daemons to use to allow different incoming connections.

1. From the top menu, select **Configuration**; from the side menu, select **Network > Services**.

The system invokes the Services form.



2. Select the service(s) you would use to access devices.
3. Select **Apply Changes** when done.

Network > IP Filtering



*If you already understand how IP filtering works, skip this section and proceed to the procedure section, **IP Filtering - To Add a Chain**.*

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 (*e.g.*, 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 IP Filtering form is structured in two levels:

- Chain
- Rule

Structure of IP Filtering

IP Filtering configuration is structured on two levels:

- The IP Filtering form which contains a list of chains.
- The chains which contain the rules that control 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.

Rule

Each chain has a sequence of rules that address the following:

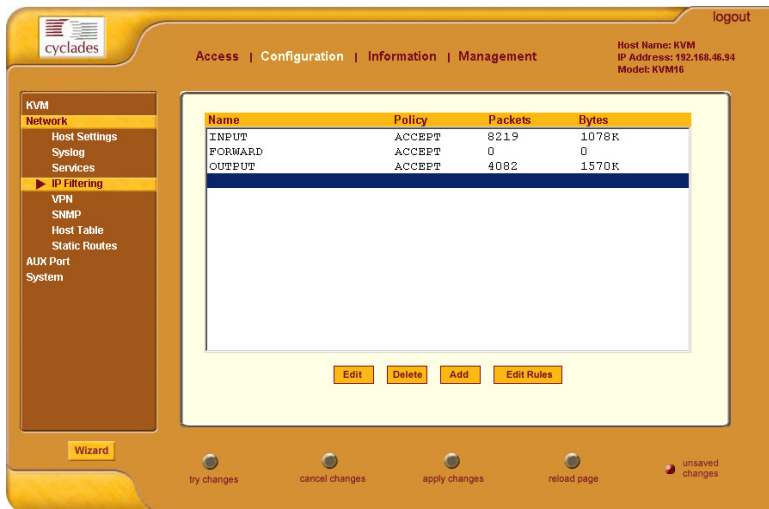
- How the packet should appear in order to match the rule.
Some information about the packet is checked according to the rule, for example, the IP header, the input and output interfaces, the TCP flags and the protocol.
- What to do when the packet matches the rule.
The packet can be accepted, blocked, 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.

IP Filtering: To add a chain:

1. From the top menu, select **Configuration**; from the left menu, select **Network > IP Filtering**.

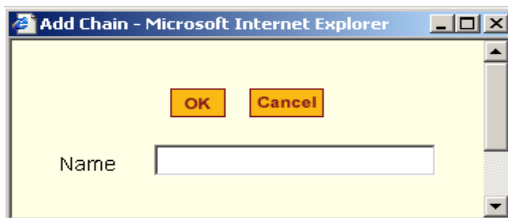
The system brings up the IP Filtering configuration form:



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 system brings up the **Add Chain** dialog box:



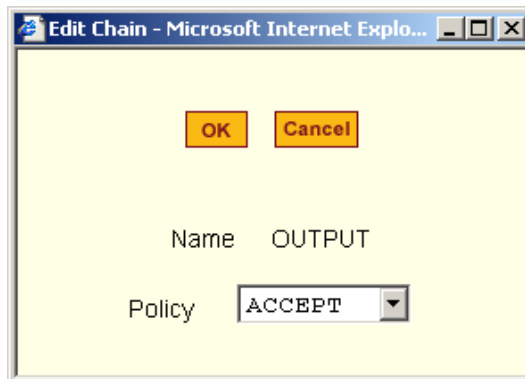
3. Enter the name of the chain that you are adding to the filter table, and then select **OK**. (Spaces are not allowed in the chain name.)

4. After entering a new chain name, click on the **Edit Rules** button to access the next dialog window to enter the rules for that chain.
5. Select **OK** to commit your changes.
6. To add rules to your new chain, see *IP Filtering: To Add a Rule* section.

IP Filtering: To edit a chain

1. From the IP Filtering form (**Configuration > Network > IP Filtering**), select the Chain you wish to edit from the Chain list box (or filter table), and then select the **Edit** button.

The system brings up the **Edit Chain** dialog box:



2. Modify the **Policy** field, as needed, and then select **OK**.
3. Verify your entry from the main form and then select **Apply Changes** to save your changes.
4. If you need to edit any rules for this chain, proceed to *IP Filtering: To Edit a Rule* section.

IP Filtering: To Edit a Rule

1. From the IP Filtering form (**Configuration > Network > IP Filtering**), select from the Chain list box (or filter table) the chain containing the rule(s) that you would like to edit, and then select the **Edit Rules** button.

The system brings up the **Edit Rules** form:

Packets	Bytes	Target	Source	Destination	Proto
0	0	DROF	anywhere	anywhere	Icmp
0	0	DROF	anywhere	anywhere	Icmp

Buttons: Edit, Delete, Add, Up, Down, OK

In the example above, each line represents a rule for the INPUT chain that you selected from the Chain list box from **Step 1**. Now you must select from the above list box the rule you wish to edit.

2. From the Rules list box of the Edit Rules form, select the rule to be edited and then select the **Edit** button.

The system brings up the **Edit Rule** dialog box:

3. From the **Edit Rule** dialog box, complete the following data fields as necessary:

<i>Field Name</i>	<i>Definition</i>
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.

<i>Field Name</i>	<i>Definition</i>
Inverted	Select this box to invert the target action (<i>i.e.</i> , 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.
Inverted	Select this box to invert the target action (<i>i.e.</i> , 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 text input field; otherwise, select one of the other options.
Inverted	Select box to invert the target action (<i>i.e.</i> , 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 will appear only for the chains INPUT and FORWARD.
Inverted	Select box to invert the target action (<i>i.e.</i> , 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 to invert the target action (<i>i.e.</i> , the action assigned to the target will be performed to all interfaces except to the one just defined).
Fragments	Indicates the fragments or unfragmented packets to be checked. The IP Tables can check for: <ul style="list-style-type: none"> - 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.

<i>Field Name</i>	<i>Definition</i>
Inverted	This ICMP option will be applied to all rules except the currently selected rule.

Additional Fields

If you selected **Log** from the **Target** field, the following options also appear:

LOG Options Section

Log Level Log Prefix

TCP sequence
 TCP options
 IP options

<i>Field Name</i>	<i>Definition</i>
Log Level	The log level classification to be used based on the type of error message (e.g., alert, warning, info, debug, etc.).
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.
IP Options	Check box to include IP options in the log.

If you selected **Reject** from the **Target** field, the following field appears:

REJECT Options Section

Reject with

<i>Field Name</i>	<i>Definition</i>
Reject with	“Reject with” means that the filter will drop the input packet and send back a reply packet according to any of the reject types listed below. Using tcp flags and appropriate reject type, the packets are matched with the REJECT target.
Choices are:	
icmp-net-unreachable	ICMP network unreachable alias.

<i>Field Name</i>	<i>Definition</i>
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.

4. Click on the **OK** button when done.
5. Click on the **Apply Changes** located at the bottom of the ACS configuration window to save your configuration.

To Add a Rule

The forms and dialog boxes for adding a rule is similar to the ones used for editing a rule. Refer to *IP Filtering: To Edit a Rule* procedure section for a definition of the user input fields.

1. From the **IP Filtering** form, select the chain to which you wish to add a rule (or if you are adding a new chain, select the **Add** button and follow the procedure for adding a chain.)
2. Click on the **Edit Rule** button.
The system brings up the **Edit Rule for Chain** dialog box.
3. From the **Edit Rule for Chain** dialog box, click on the Add button.
The system brings up the **Add Rule** dialog box.
4. Complete the **Add Rule** dialog box. (Refer to *IP Filtering: To Edit a Rule* section for a definition of the input fields, as needed.)
5. Click on the **Apply Changes** button located at the bottom of the ACS configuration window to complete the procedure.

Network > VPN

The VPN configuration form allows you to configure one or more VPN connections to other systems or KVM devices.

Select one of the existing VPN connections and click the edit button or click the add button to add a new one. This 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 you already understand how VPN works, skip this section and proceed to the next procedure, **To configure VPN**.*

A VPN, or Virtual Private Network lets the KVM and a whole network communicate securely when the only connection between them is over a third network which is untrustable. The method is to put a security gateway machine in the network and create a security tunnel between the KVM and the gateway. The gateway machine and the KVM encrypt packets entering the untrusted net and decrypt packets leaving it, creating a secure tunnel through it.

Often it may be useful to have explicitly configured IPsec tunnels between the KVM and a gateway of an office with a fixed IP address (in this case every machine on the office network would have a secure connection with the KVM), or between the KVM and the KVM administrator machine, which must, in this case, have a fixed IP address. You can add this connection descriptor to both the Console Server and the other end. This is the advantage of using left and right instead of using local remote parameters.

If you give an explicit IP address for left (and left and right are not directly connected), then you must specify leftnextthop (the router which KVM sends packets to in order to get them delivered to right). Similarly, you may need to specify rightnextthop (vice versa).

The Role of IPsec

IPsec is used mainly to construct a secure connection (tunnel) between two networks (ends) over a not-necessarily-secure third network. In the KVM, the IPsec is used to connect the KVM switch securely to a host or to a whole network--configurations usually referred to as *host-to-network* and *host-to-host tunnel*. Practically, this is the same thing as a VPN, but here one or both sides have a degenerated subnet (*i.e.*, only one machine).

The IPsec protocol provides encryption and authentication services at the IP level of the network protocol stack. Working at this level, IPsec can protect any traffic carried

over IP, unlike other encryption which generally protects only a particular higher-level protocol (e.g., SSH for login, SSL for Web work and so on). The implementation of IPsec used by the AlterPath KVM is FreeSWAN (www.freeswan.org).

You can use IPsec on any machine that does IP networking. Wherever required to protect traffic, you can install dedicated IPsec gateway machines. IPsec can also run on routers, firewall machines, various application servers, and end-user desktop or laptop machines.

Authentication Keys

To establish a connection, the Console Server and the other end must be able to authenticate each other. For FreeS/WAN, the default is public key authentication based on the RSA algorithm.

To configure VPN



*For the VPN to function properly, ensure that you have also enabled IPsec from the **Services** form.*

1. Select **Network** from the top menu bar, and then select **VPN Connections** from the left menu panel.

The system brings up the **VPN Connections** form:



- 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 system brings up the **New/Modify Connection** dialog box:

The image shows two instances of the 'New/Modify Connection' dialog box. The left instance has 'Authentication Protocol' set to 'ESP' and 'Authentication Method' set to 'RSA Public Keys'. It features fields for 'Connection Name', 'Remote ("Right")' (ID, IP Address, NextHop, Subnet, RSA Key), and 'Local ("Left")' (ID, IP Address, NextHop, Subnet, RSA Key). The 'Boot Action' is set to 'Ignore'. The right instance has 'Authentication Protocol' set to 'ESP' and 'Authentication Method' set to 'Shared Secret'. It includes the same fields as the left instance but also has a 'Pre Shared Secret' field at the bottom.

If the selected **Authentication Method** is **RSA Public Keys**, the left dialog box is used. If the **Authentication Method** is **Shared Secret**, the right dialog box is used.

- Edit or complete the appropriate fields from either dialog box as follows:

<i>Field Name</i>	<i>Definition</i>
Connector Name	Name of the VPN connection.
Authentication Protocol	Authentication protocol used to establish a VPN connection.
Authentication Method	Authentication method used to establish a VPN connection.

<i>Field Name</i>	<i>Definition</i>
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.
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.

Network > 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 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 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 KVM by SNMP. There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in KVM cannot permit the public community to read SNMP information.*

To configure SNMP:

1. From the top menu bar, select **Networks**; from the left menu panel, select **SNMP Daemon Settings**.

The system invokes the SNMP Daemon Settings form:



2. Type in the following System Information, as necessary:

<i>Field Name</i>	<i>Definition</i>
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 (e.g., me@mymachine.mydomain)
SysLocation	The physical location of the system (e.g., mydomain).



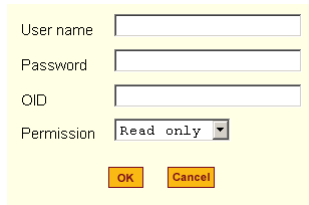
If you are using SNMPv3, skip steps 2 and 3; proceed to step 4.

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 system invokes the New/Modify SNMP Daemon Configuration dialog box.



The dialog box contains the following fields and controls:

- User name:
- Password:
- OID:
- Permission:
- Buttons:

7. Complete the form and when done, select the **OK** button from the dialog box.
8. Verify your entry or modification from the respective tables of the SNMP Configuration form.
9. Select the **Apply Changes** button to complete the procedure.

Network > Host Table

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.

1. From the top menu, select **Network**; from the left menu, select **Host Table**.

The system invokes the Host Table form:

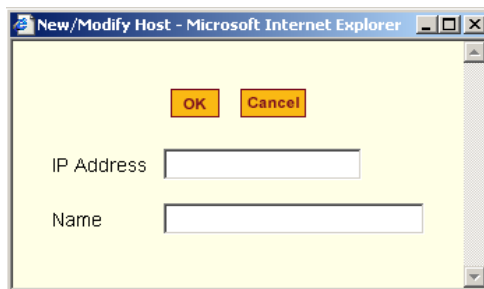


2. To edit host, select the host IP address from the Host Table and then click on the **Edit** button. (If the list is long, use the **Up** and **Down** buttons to go through each item in the list.)

- OR -

To add a host, click the **Add** button.

The system brings up the following dialog box:



3. Type in the new or modified host address in the **IP Address** field, and the host name in the **Name** field, and then select the **OK** button.
4. To delete a host, select the host you wish to delete from the Host Table form, and then select the **Delete** button from the form.
5. Select the **Apply Changes** button to save your configuration to Flash.

Network > 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.

You can add or edit a hard-coded static route by clicking on the corresponding buttons. They'll bring you to a dialog box to enter the route to be added. To delete a static route, highlight the route and select **Delete**.

1. From the top menu, select **Network**; from the left menu, select **Static Routes**.

The system brings up the Static Routes table form:



Refer to the field definitions in Step 3 for the meaning of each field in the table.

2. To edit a static route, select a route from the Static Routes form, and then select the **Edit** button.

- OR -

To add a static route, select the **Add** button from the form.

The system invokes the **New/Modify Route** dialog box:

3. Complete the dialog box as follows:

<i>Field Name</i>	<i>Definition</i>
Route	Select Default , Network , or Host .
Network IP	<i>This field appears only if Network is selected.</i> The address of the destination network.
Network Mask	<i>Only if Network is selected.</i> The mask of the destination network.
Host IP	<i>Only if Host is selected.</i> The IP address of the destination host.
Go to	Select Gateway or Interface .
[Adjacent field]	The address of the gateway or interface.
Metric	The number of hops.

4. Select **Apply** when done.

AUX Port

The **AUX(iliary) Port** form is used to configure the auxiliary port settings to suit the profile or the device to be connected (in this case, a modem or a power management) to the KVM unit.

1. From the top menu, select **Configuration**; from the side menu, select **AUX Port**.

The system brings up the Auxiliary Port form.

From the **Profile** field of the Auxiliary Port form, select Power Management or PPP. If you select PPP, the following additional fields will appear on the form:

The screenshot displays the KVM Web Configuration interface. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The host information is shown as 'Host Name: KVM', 'IP Address: 192.168.46.34', and 'Model: KVM16'. The left sidebar menu has 'KVM', 'Network', 'AUX Port', and 'System' options, with 'AUX Port' selected. The main content area shows the 'AUX Port' configuration form for the 'PPP' profile. The form includes the following fields and controls:

- Profile: PPP (dropdown menu)
- Baud Rate (kbps): 9600 (dropdown menu)
- Flow Control: None (dropdown menu)
- Data Size: 8 (dropdown menu)
- Parity: None (dropdown menu)
- Stop Bits: 1 (dropdown menu)
- Modem Initialization: A text area containing 'TIMEOUT 10', '" \d\\ \dATZ', and 'OK\r\n-ATZ-OK\r\n "' (dropdown menu)
- Local IP address: (text input field)
- Remote IP address: (text input field)
- Authentication Required:

At the bottom of the form, there are five buttons: 'Wizard', 'try changes', 'cancel changes', 'apply changes', and 'reload page'. A red indicator for 'unsaved changes' is visible in the bottom right corner.

2. To configure the Aux Port for PPP, complete the fields as shown below and select **Apply Changes** when done.

<i>Field Name</i>	<i>Definition</i>
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.
Modem Initialization	The modem initialization string.
Local IP Address	The 32-bit local IP address.
Remote IP Address	The 32-bit remote IP address
Authentication Required	Select checkbox if authentication is required.
MTU/MRU	The maximum transmission unit / maximum receive units for the PPP.
PPP Options	The options for this protocol.

System

The **System** menu, which is the fourth selection under the **Configuration** menu, comprises two forms: **Date/Time** and **Boot**.

System > Date/Time

The Date/Time form is used to enable the KVM to work as an NTP client, synchronizing your system clock with the *true time* (i.e., the average of many high-accuracy clocks around the world). By default, NTP is disabled; you may enter the time and date manually using the Time/Date form.

Manual Setting

To set time and date manually, perform the following steps:

1. From the top menu, select **Configuration**; from the left menu, under **System**, select **Date/Time**.

The system brings up the **Date/Time** form:



The screenshot shows the KVM web configuration interface. The top navigation bar includes 'Access | Configuration | Information | Management'. The left sidebar menu is expanded to 'System', with 'Date/Time' selected. The main content area displays the 'Date/Time' configuration form. At the top, 'Network Time Protocol' is set to 'Disable'. Below this, there are two sections: 'Date' and 'Time'. The 'Date' section has dropdown boxes for 'Month' (10), 'Day' (4), and 'Year' (2004). The 'Time' section has dropdown boxes for 'Hour' (14), 'Minute' (49), and 'Second' (51). At the bottom of the interface, there are buttons for 'Wizard', 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'unsaved changes'.

2. If you are not using NTP, complete the date and time fields by selecting the appropriate numbers from the dropdown list boxes.
3. Click on the **Apply Changes** button to complete the procedure.

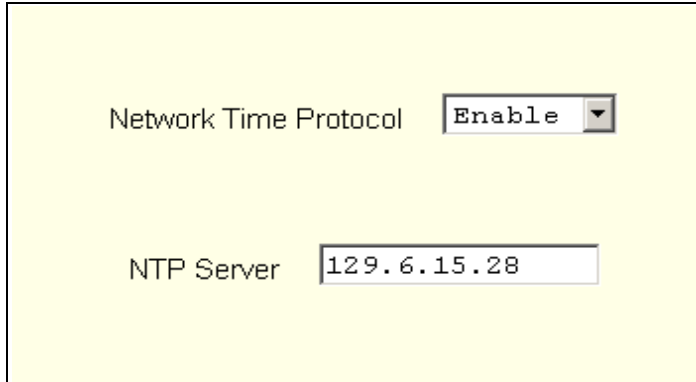
NTP Setting

To set the time and date through NTP, perform the following steps:

1. Choose **Enable** from the **Network Time Protocol** field of the Date/Time form.

The system invokes the **NTP Server** field.

2. Type in the address of the NTP server in the **NTP Server** field.



The screenshot shows a configuration form with two fields. The first field is labeled 'Network Time Protocol' and has a dropdown menu with 'Enable' selected. The second field is labeled 'NTP Server' and contains the IP address '129.6.15.28'.

3. Click on the **Apply Changes** button.

System > Boot

Boot configuration defines the settings for loading the operating system.

The KVM can boot from its internal firmware or from the network. By default, the unit boots from Flash. If you need to boot from the network, install one TFTP or BOOTP server with the firmware to boot from, and then choose **boot from network** and fill in the fields. You may skip Flash test and RAM test for a faster boot.

To configure the KVM boot settings:

1. From the top menu bar, select **Configuration**; from the left menu panel, under **System**, select **Boot Configuration**.

The system brings up the Boot Configuration form:



2. Complete the fields as follows:

<i>Field Name</i>	<i>Definition</i>
IP Address assigned to Ethernet	As indicated.
Watchdog Timer	Sets the Watchdog Timer to Active or Inactive.
Unit boot from	Specify whether to boot unit up from Flash or from the Network.
Boot Type	Select from the following types of booting: bootp, tftp, or both.
Boot File Name	Filename of the boot program you want to use.
Server's IP Address	As indicated.
Console Speed	Select from: 4800 through 118200.
Flash Test	Select this to test boot from the Flash card. You can Skip this test, or do a Full test.

<i>Field Name</i>	<i>Definition</i>
RAM Test	Select this to test boot from RAM. You can Skip this test, do a Quick test or a Full test.
Fast Ethernet	Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value): 100BaseT Half-Duplex 100BaseT Full-Duplex 10BaseT Half-Duplex 10BaseT Full-Duplex
Fast Ethernet Max. Interrupt Events	The maximum number of packets that the CPU will handle.

3. Select **Apply Changes** to save your configuration to Flash.

Information

The **Information** menu provides two forms for viewing information:

- General
- Port Status

General

Use the General form to view system information in the following categories:

- System (e.g., Kernel version, Date, Uptime, etc.)
- CPU
- Memory
- Ram Disk Usage
- Fan Status

To view General information:

1. From the top menu, go to **Information**; from the side menu, select **General**.

The system brings up the following view form:



An example of the types of general information available from this window is as follows:

System Information

Kernel Version: Linux version 2.4.17_mvl21-linuxplanet
(root@exodus.cyclades.com)
(gcc version 2.95.3 20010315 (release/MontaVista)) #409
Thu Aug 5 17:50:53 PDT 2004
AlterPath-KVM16-Linux V_1.1.0a (August/04/04) a
Date: Tue Oct 5 10:45:39
Up Time: 56 min
Power Supply State: SINGLE

CPU Information

Cpu: 8xx
Clock: 48MHz
Revision: 0.0 (pvr 0050 0000)

Bogomips: 47.82

Memory Information

MemTotal: 127140 kB

MemFree: 96328 kB

MemShared: 0 kB

Buffers: 3952 kB

Cached: 16424 kB

SwapCached: 0 kB

Active: 8888 kB

Inactive: 18252 kB

HighTotal: 0 kB

HighFree: 0 kB

LowTotal: 127140 kB

LowFree: 96328 kB

SwapTotal: 0 kB

SwapFree: 0 kB

Ram Disk Usage

Filesystem	1k-blocks	Used	Available	Use%	Mounted
------------	-----------	------	-----------	------	---------

/dev/ram0	8992	8992	0	100%	/
-----------	------	------	---	------	---

Fan Status

Fan 1: '8000' rotations per minute

Fan 2: '0' rotations per minute

Port Status

Use the Port Status form to view the system status of each KVM port.

1. From the top menu, select **Information**; from the side menu, select **Port Status**.

The system brings up the **Port Status** view form:



Management

The Management menu comprises seven forms relating to system and software management such as booting, backing up, and handling configuration data.

<i>Menu Selection</i>	<i>Use this menu to:</i>
Backup Configuration	Use a FTP server to save or retrieve your configuration data.
Firmware Update	Upload firmware from the web to the KVM and save the new software version or update.
Microcode Update	Update any of the micro controller microcodes that are stored in the KVM terminator, main KVM, local KVM, and internal KVM switch.
Microcode Reset	Reset any of the micro controller microcodes.

<i>Menu Selection</i>	<i>Use this menu to:</i>
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 KVM to use a FTP server to save and retrieve its configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from the KVM by pinging the FTP server.

1. From the top menu, select **Management**; from the left menu, select **Backup Configuration**.

The system brings up the **Backup Configuration** form:

The screenshot displays the KVM web configuration interface. At the top, there is a navigation bar with 'Access | Configuration | Information | Management' and a 'logout' link. The left sidebar contains a menu with options: Backup Configuration (selected), Firmware Upgrade, Microcode Upgrade, Microcode Reset, Active Sessions, and Reboot. The main content area is titled 'FTP Server' and contains four input fields: 'Server IP', 'Path and Filename', 'Username', and 'Password'. Below these fields are two buttons: 'Save to FTP server' and 'Load from FTP server'. At the bottom of the interface, there is a 'Wizard' button and a status bar with indicators for 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'no unsaved changes'.

2. Complete the fields and then select one of the following buttons:
 - **Save to FTP server** - select this if you want to save your configuration to the FTP server.
 - **Load from FTP server** - select this if you want to load your configuration from the FTP server to the KVM.
3. Select the **Apply Changes** button when done. The configuration loaded should run after a reboot.

Firmware Update

To upgrade your KVM firmware, perform the following steps:

1. From the top menu, select **Management**; from the side menu, select **Firmware Update**.

The system brings up the Firmware Update form:

2. From the Firmware Update form, complete the fields as follows:

<i>Field Name</i>	<i>Definition</i>
Type	The method of upload.
FTP Site	The address of the FTP site.
Username	Username of the person who is doing the upload.
Password	Password associated with the Username.
File Version	The full path and filename of the image to be loaded.
Run Checksum	Runs the checksum program to verify the accuracy of the uploaded data.

3. Select the **Upgrade Now** button.
4. Select the **Apply Changes** button at the bottom of the configuration window.

Microcode Update

Through an FTP server, the Microcode form is used to update any of the micro controller microcodes that are stored separately in each of the following target locations:

- KVM Terminator
- KVM Switch (internal)
- KVM Main
- KVM Local
- KVM Video Compression Module

To update a microcode:

1. From the top menu, select **Management**; from the side menu, select **Microcode Update**.

The system brings up the Microcode form:

2. Complete the input fields as follows:

<i>Field Name</i>	<i>Definition</i>
Target	The specific KVM microcode that you wish to update (i.e., KVM Terminator, KVM Switch (internal), KVM Main, and KVM Local).

Field Name	Definition
FTP server	Address of the FTP server used to update the microcode.
User	The authorized user name.
Password	The user's password.
Directory	Location (directory path) of the microcode file.
Filename	The microcode filename.

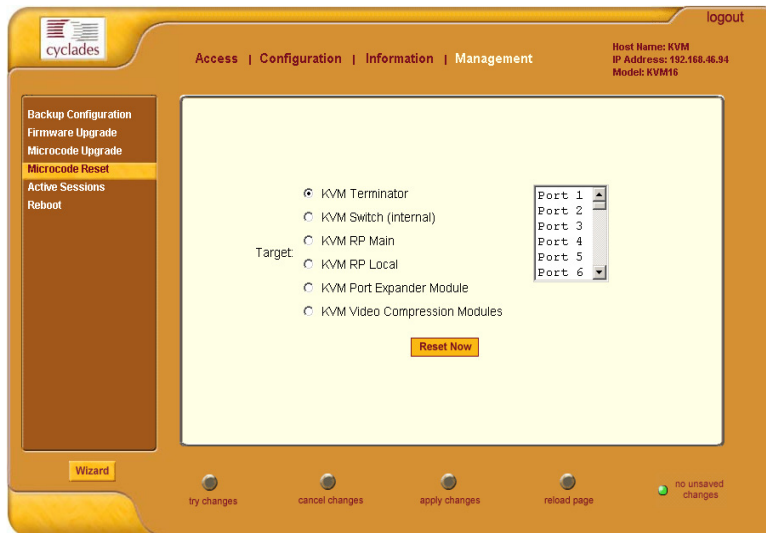
- From the scrollable port list, select the port to which the target is connected.
- Select the **Upgrade Now** button.

Microcode Reset

The Microcode Reset form is used to reset the hardware associated with the afore-discussed microcodes.

- From the top menu, select **Management**; from the side menu, select **Microcode Reset**.

The system brings up the Microcode Reset form:



- From the form select the microcode or hardware target.
- From the scrollable port list, select the port to which the target is connected, and then select the **Reset Now** button.

Active Sessions

The Active Sessions form is designed to provide you a quick status, and usage information (e.g., user, tty, Login time, JCPU, etc.) pertaining to all active server sessions. You may also kill or refresh a session.

Open sessions are displayed with their identifications and statistics data for login, session and CPU usage for the specific client. JCPU relates all processes attached to that port including running background processes. PCPU relates the current processing time.

1. From the top menu bar, select **Management**; from the left menu panel, select **Active Sessions**.

The system invokes the Active Sessions window:



What the heading and column name means:

<i>Field / Column</i>	<i>Definition</i>
Uptime	System uptime in minutes and seconds (mm:ss).
# Users	Number of current users.
User	The user who initiated the session.
TTY	The name of the serial port.
From	The network machine to which the port is connected.
Login@	The day and time of the last login.

<i>Field / Column</i>	<i>Definition</i>
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.

2. To kill or refresh a session, select from the Active Sessions view table the session you wish to delete or refresh.
3. Click on the **Kill Session** or **Refresh** button.
4. From the configuration window, click on the **Apply Changes** button.

Reboot

The Reboot form allows you to reboot the system by clicking the **Reboot** button (go to **Management > Reboot**) as shown:



Chapter 5

KVM Operation

This chapter discusses the procedures and requirements for operating the AlterPath KVM, and is organized as follows:

- Basic Navigation Keys
- Default Key Sequences
- Changing Your Password
- Connecting to a Server
- Cycling Between Servers
- Remote Operation
- Operating through the Remote Unit (RP)
- Adjusting Screen Brightness and Contrast
- Sharing Server Connection
- Synchronizing Keyboard and Mouse
- Establishing a Power Control Session
- Logging Events
- Operating through a Web Browser
- Upgrading Software

Basic Navigation Keys

Below is a short list of keyboard controls to help you navigate through the KVM on-screen display. For the keys to work, ensure that your window is selected so that it is in the *active* state.

<i>Key</i>	<i>Action</i>
TAB	Changes between fields on the window
UP / DOWN	Scrolls within a menu
LEFT / RIGHT	Selects a button in a button field
BACKSPACE	Deletes 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 / Commit changes

Default Key Sequences

A *key sequence* (also known as *escape sequence*) is a sequence of special characters used to send a command to a device or program, in this case the KVM application.

Aside from the navigation keys, you can use the following key sequences to perform a specific action:

<i>Key Sequence</i>	<i>Action</i>
<Ctrl-K>, and then <Q>	Quit command - closes the session to a port and takes you back to the KVM Main Menu.
<Ctrl-K>, and then <P>	Port command - initiates a power control session.
<Scroll Lock> twice, and then <L>	RP Switch to Local command - switches the AlterPath KVM RP video display to the local computer.
<Scroll Lock> twice, and then <R>	RP Switch to Remote command - switches the AlterPath KVM RP video display to the remote computer.
<Scroll Lock> twice, and then <N> or <F>	RP Beep On/Off - switches the beeper on or off when switching between devices (local-remote). Use <N> for ON and <F> for OFF.
<Ctrl-K>, and then <. >	Move to the next port - switches from the currently connected server to your next authorized server.
<Ctrl-K>, and then < , >	Move to the previous port - switches from the currently connected server to the previous server.
<Ctrl-K>, and then <V>	Video command - controls screen brightness and contrast.
<Ctrl-K>, and then <S>	Keyboard and Mouse Synchronization command - resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM.

NOTE: The default key sequence ^KP is also used for controlling the power outlet in cascading. By typing <Ctrl-K><P>, while connected to a server in a KVM port, an OSD menu opens which allows you to switch on/off or cycle

(i.e., switch OFF and ON quickly and sequentially) the connected server that is powered by the AlterPath PM.

Changing the Root Password

If you are a system administrator or a user with admin privileges, you can change your password by using your terminal emulation program.

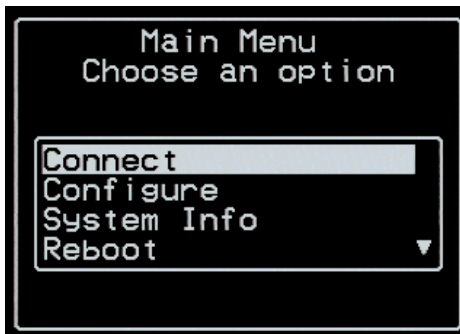
1. Connect your PC terminal to the console port of your AlterPath KVM.
2. Configure your COM port as follows:
 - Serial Speed: 9600 bps
 - Data Length: 8 bits
 - Parity: None
 - Stop Bits: 1 stop bit
 - Flow Control: None
 - ANSI emulation
3. Open your terminal emulation application (HyperTerminal, Kermit, or Minicom).
4. Log in as: **root** Password: **Cyclades**
5. Upon system prompt, enter the command: **passwd**
6. Type in your new password when prompted.
7. As prompted, type in your password again to confirm.
8. Save your new password to Flash by typing in: **saveconf**
9. Close your terminal session.

Logging In

1. To log in to the KVM application, type in your log in name followed by your password in the respective fields.

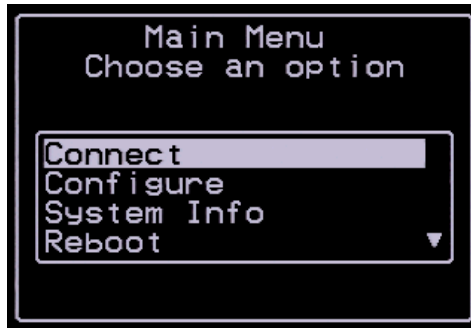


2. Tab to the **OK** button and press <Enter>. The system displays the KVM main menu.



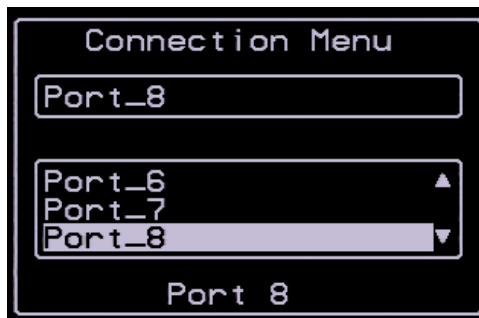
Connecting to a Server

1. To connect to a server, select **Connect** from the main menu.



2. Press <Enter>.

The system brings up the Connection menu which lists all KVM ports by name. The menu selections are chronologically arranged from local ports to cascaded ports and devices, in ascending order.



3. From the Server Connection menu, select the server to which you wish to connect.

- OR -

From the quick search box, enter the KVM port name (this field is case-sensitive). If a match is found, the system will automatically highlight the port name from the list.

4. Press <Enter>.

Using the Search Box

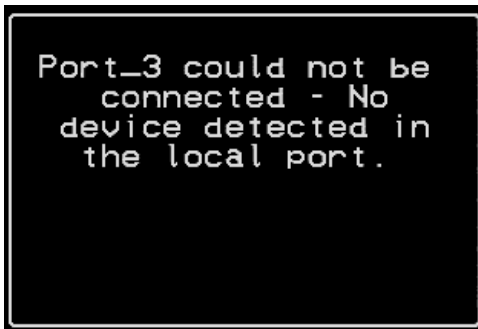
The quick search box of the Connection Menu is designed to speed up the connection process by allowing you to type in the first letters of the port name. Based on your search entry, the port name list box will automatically scroll to the port that matches your entry. The search box works for both **User 1** and **User 2** connecting to any KVM port in the master or cascaded KVM units.

Successful / Unsuccessful Connection

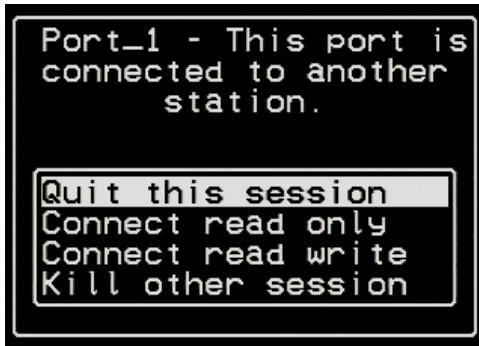
When you connect to a port, the system takes you to the console of the selected server on that port:



If there is no device connected, the system displays the following error message:



If the port is already connected to another station, the system displays the following message:



Select the appropriate action to continue.

Cycling Between Servers

Cycle refers to the capability to access or connect from one authorized server to another. There are two ways in which you can cycle between servers:

- Cycle by Server (automatic)
- Cycle by Key Sequence (manual)

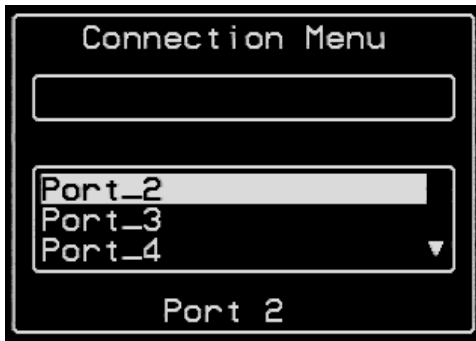
Cycle by Server

Cycle by Server (or automatic cycling) enables you to view all authorized servers on a continuous basis until all servers have been exhausted and then start over again.

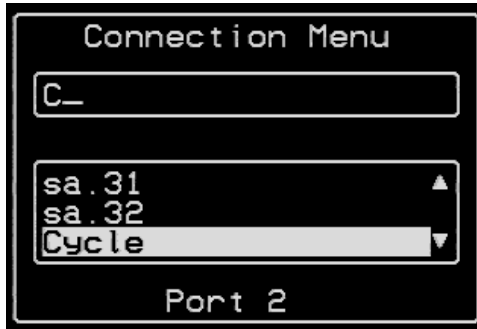
To initiate cycling by server, perform the following steps:

1. From the Main Menu, choose **Connect** and press <Enter>.

The system brings up the Server Selection Menu:

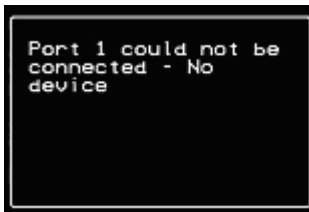


- From the Server Selection window, select **Cycle** and then press <Enter>.



- To stop the cycling, enter the escape sequence (default: **Ctrl-K, Q**) to abort the process and close the session.

In the cycle process, if there is no device attached to the port associated with the next logical port, a message will appear to indicate that there is no device connected:



Cycle by Key Sequence

Cycle by Key Sequence allows you to view or access the next server manually (that is, one key sequence at a time).

To step forward through ports, press <Ctrl-K> followed by the period (.) key.

To step backward through ports, press <Ctrl-K> followed by the comma (,) key.

To quit the session and return to the previous menu, press <Ctrl-K><Q>.

Remote Operation

You can operate your AlterPath KVM remotely using the AlterPath KVM RP. KVM supports two concurrent users:

- One local user at the KVM switch
- One remote user at the AlterPath RP location.

The AlterPath RP may be placed up to 500 feet away from the KVM unit. The KVM RP enables the remote user to select the local keyboard, video, and mouse console between a local station and a server connected to the KVM.



See Chapter 2: *KVM Installation* for details on how to install the AlterPath KVM RP.

Operating through the Remote Unit (RP)

You can select the keyboard, video, and mouse remote console between a local station and a server connected to the KVM using any of the following methods:

- Press the button at the AlterPath KVM RP unit to switch the local video display between a local station and a server connected to the KVM.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + R to switch the local video display to the remote server connected to the KVM.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + L to switch the local video display to the local station connected to the KVM RP.

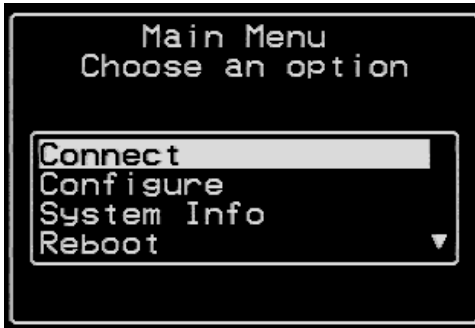
Finishing your Session

There are three ways to end your session:

- Select **Exit** from the KVM Main Menu
- Press the escape sequence (**Ctrl-K, Q**)
- Through Idle Timeout

Method 1: Exiting through the Main Menu

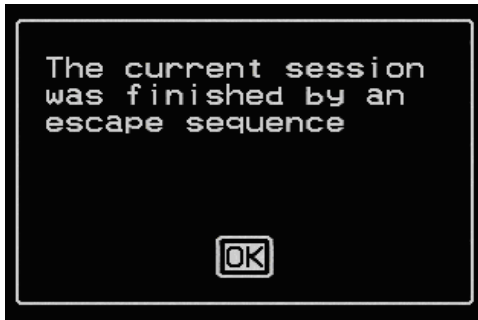
Return to the Main Menu and select **Exit**.



Method 2: Exiting by using the escape sequence.

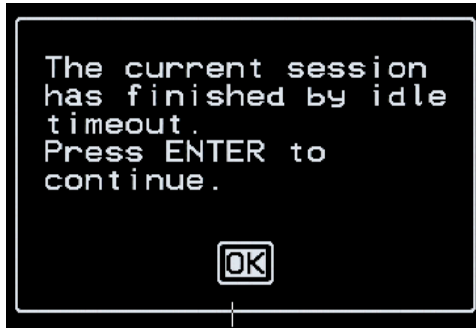
Press **Ctrl-K** keys followed by the **Q** key.

The system will close the session and send the following message:



Method 3: Exiting by Idle Timeout

Leaving your system idle will eventually close the session based on the configured idle time. When this happens, the system closes the session and sends the following message:



The idle time is set by the KVM administrator.

OSD Screen Saver

The OSD Screen Saver consists of a black screen that activates after a period of inactivity. You can configure the time or period of inactivity before the screen saver activates from the OSD.

Designed to prevent the monitor screen from being “burned,” the screen saver is displayable on the workstation of the local user or remote (RP) user.

Operating through the Remote Unit (RP)

You may configure and operate your KVM remotely from your station connected to the AlterPath KVM RP. To switch your Keyboard, Video and Mouse (KVM) console from your local PC to the remote server connected to the KVM switch, you may do any of the following:

- Toggle the switch button located in front of your KVM RP unit.
- Press **ScrLK** twice then **L**, to switch to the local PC.
- Press **ScrLK** twice then **R**, to switch to the remote server connected to the KVM.

Adjusting Screen Brightness and Contrast

To adjust screen brightness, press the video control key sequence (**Ctrl-K** followed by the **V** key, default).

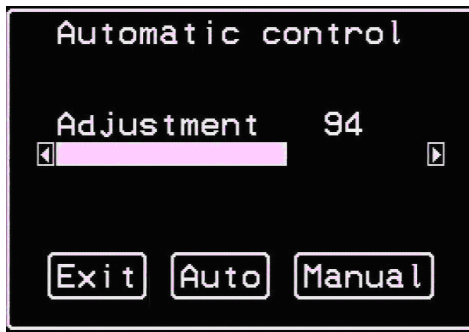
Depending on which window was accessed last, the system will display either one of the following overlaying windows:

- Automatic (Video) Control Adjustment
- Manual Brightness and Contrast Control

Automatic (Video) Control Adjustment

The Automatic Video 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 will be poor.



In the Automatic Control screen, press the <Tab> key to move from the Adjustment field to the **Exit/Auto/Manual** buttons. Once you are in one of the buttons, select the right or left arrows to move from one button to another.

Manual (Brightness/Contrast) Control

The Manual Control window is used to control the levels of video brightness and contrast. As in the Automatic Control overlay window, use the <Tab> key to move between the **Brightness/Contrast** fields and the **Exit/Auto/Manual** buttons.



Sharing Server Connection

The AlterPath KVM supports shared connections to a server. This feature is implemented based on the type of access permissions each of the users have for the specified server port.

When a user connects to a server that is already in use, the software autodetects the event and presents a menu to the connecting user. Options available under this menu will vary depending on the connecting user access permissions. Also, a notification is presented to the current user, depending on the action selected by the connecting user. To better understand how this is done consider the following definitions:

- Read-only mode: session mode of a user with read-only permission for the server port
- Read-write mode: session mode of a user with read-write, read-write-config, read-write-power or full access permission for the server port

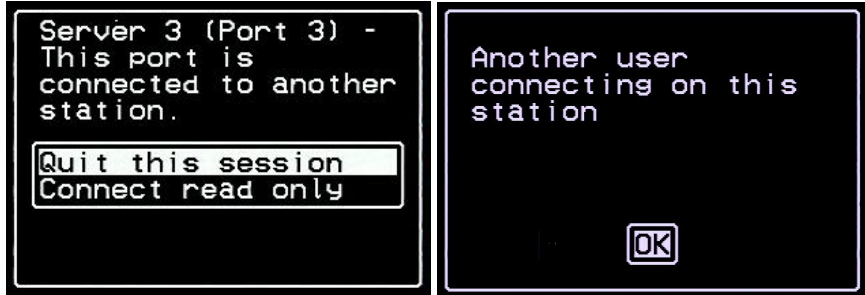
The following two options are always presented in the menu to the connecting user:

- Quit: Just quits the connection attempt and returns to the Server Connection Menu

5: AlterPath KVM Operation

- Connect read-only: connects the user in read-only mode and notifies the new connection to the previous user.

The menu presented to the connecting user and the notification message to the previous user are as follows:

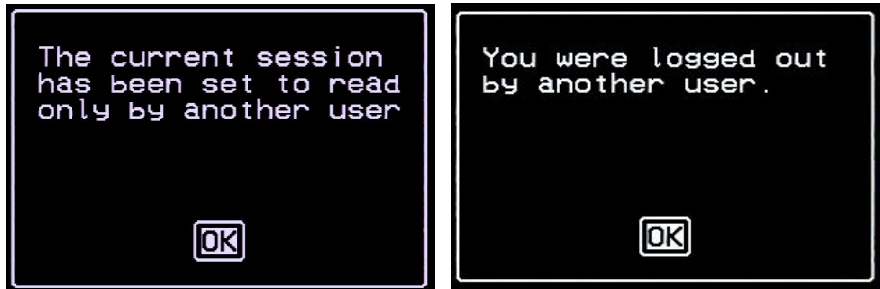


If the connecting user has either read-write, read-write-config, read-write-power or full access permission to the server port, the following additional options are presented in the menu:

- Connect read write: connects the user in read-write mode and the previous user is notified of the event. If the previous user is in read-write mode, its access mode is changed to read-only and he is notified of the event
- Kill the other session: kills the existing session and connects the user in read-write mode. The previous user is notified of the event and is disconnected from the server port.

The menu presented to the connecting user and the notification messages to the previous user are as follows:





The connecting user is always granted the highest privilege mode based on its permission rights when the previous user is in read-only mode.

Once two users are connected to a server port, either user may choose at any time to change his/her access mode (or disconnect from the session by issuing an escape sequence command).

Synchronizing Your Keyboard and Mouse

There may be circumstances when your recently connected server do not support full operation of keyboard and mouse. To fix this, just issue a Keyboard/Mouse Sync command (default keys: Ctrl-K, and then S). This key sequence invokes the following confirmation window:



Select **Yes** to enable your keyboard and mouse again.



See also the section on **Mouse Settings, Chapter 2: KVM Installation.**

Establishing a Power Control Session

If you have an AlterPath PM powering one or more computers connected to your KVM unit, you may initiate a power control session at any time once you are connected. You first connect to the desired computer following the *Connecting to a Server* section of this chapter. Then press, at any time, the power command key sequence (**Ctrl-K** then **P**, default).

If you have correctly performed the Power Outlet configuration option as described under Server Configuration (Chapter 3), the system will bring you a Power management window which will:

- Indicate if the power outlet configured for the selected server is ON or OFF.
- Allow you to select power ON, OFF, or CYCLE.
- Allow you to exit from the Power Control Session.

Logging Events

You can audit the use of your KVM unit by checking log files. Logging capabilities and message treatment are supported through a daemon called *syslog-ng*. Its basic function is to read and log messages to the system console; log files, remote servers and/or users as specified by its configuration file.

The *syslog-ng* can filter messages based on their content and perform an action (*e.g.*, send an email or a pager message). To access this function, you need to configure the *syslog-ng.conf* file.

The *syslog-ng.conf* file is read at startup and is re-read after receiving a hang-up signal. When reloading the configuration file, all destination files are closed and re-opened as appropriate. The *syslog-ng* reads from various sources (files, TCP/UDP connections, syslogd clients), filters the messages and takes an action (writes in files, sends SNMP trap, pager or email, or syslogs to a remote server).

KVM Web Operation

Using the KVM web interface allows you to:

- Connect to a server
- Perform power management

To operate the KVM switch from the web, enter the IP address of the KVM on your internet browser as provided by your KVM administrator.

Once connected, login your username and password (also as provided by your KVM administrator).

Upon logging in successfully, the system displays the Connection form:



The screenshot displays the Cyclades Web Manager interface. At the top left is the 'cyclades' logo. The main header reads 'Cyclades Web Manager - Regular User'. On the top right, there is a 'logout' link and system information: 'Host Name KVM', 'IP Address 192.168.46.94', and 'Model KVM16'. A left-hand navigation menu contains 'Connect' and 'Power Management'. The main content area is a light yellow rectangle containing a dropdown menu with 'Port_2' selected and a 'Connect' button below it.

Connecting to a Server

To connect to a server, follow the following steps:

1. From the Connection form, select the port to which you wish to connect.
2. Click on Connect.

The system connects you to the server.

Power Management

Depending on your access rights, KVM/net allows you to remotely view and manage all Intelligent Power Distribution Units (IPDUs) connected to the KVM/net unit. Power management configuration comprises five tabbed forms, of which only the first two are available to the regular user:

<i>Form Title</i>	<i>Use this form to:</i>
Outlets Manager	Switch on/off and lock/unlock outlets; reboot network devices.
View IPDUs Info	View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.
Users Manager	<i>For admin user only.</i> This form is used to Add or delete users assigned to specific outlets.
Configuration	<i>For admin user only.</i> This form is used to enable over power protection, syslog and alarm notification from any specified port. The form allows the administrator to set a current alarm threshold that once exceeded will have the KVM/net sound an alarm or send a notification message.
Software Upgrade	<i>For admin user only.</i> This form is used to upgrade the AlterPath Power Manager software.

If you have admin privileges and you need to configure Power Management using the other tabbed forms, refer to **Chapter 3: KVM/net Configuration** for a detailed explanation of these forms.

Access > Power management > Outlets Manager

The **Outlets Manager** form allows you to check the status of all IPDUs connected to the Console Server, including their outlets. Any user who has Administration privileges can turn on, turn off, cycle, lock and unlock the outlets.

1. From the top menu, select **Access**; from the left menu, select **Power Management**.

The system invokes the following form:

Host Name: KVM
IP Address: 10.10.10.31
Model: KVMnet 16

Outlets Manager | View IPDUs Info | Users Manager | Configuration | Software Upgrade

Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State	Power Up Interval
1	out1	ON UNLOCKED	0.50
2	out2	ON UNLOCKED	0.50
3	tout3	ON UNLOCKED	0.50
4	out4	ON UNLOCKED	0.50
5	out5	ON UNLOCKED	0.50
6	out6	ON UNLOCKED	0.50
7	out7	ON UNLOCKED	0.50
8	out8	ON UNLOCKED	0.50

In the example above, the yellow bulbs (*i.e.*, the actual color online when the switch is ON) and the opened padlock indicate that the outlets are switched on and unlocked.

- To switch on/off an outlet, click on the light bulb; to lock/unlock an outlet, click on the padlock.

In the sample form below, outlet 2 is switched off and locked.

Outlets Manager | View IPDUs Info | Users Manager | Configuration | Software Upgrade

Name: PowerMgm-1
Number of Units: 1

Outlet	Outlet Name	Outlet State	Power Up Interval
1	out1	ON UNLOCKED	0.50
2	out2	OFF LOCKED	0.50
3	tout3	ON UNLOCKED	0.50
4	out4	ON UNLOCKED	0.50
5	out5	ON UNLOCKED	0.50
6	out6	ON UNLOCKED	0.50
7	out7	ON UNLOCKED	0.50
8	out8	ON UNLOCKED	0.50

5: AlterPath KVM Operation

3. To save your changes, click on the **Save Outlets State** button located in the form.
4. From the lower control buttons of the main window, click on the **Apply Changes** button.

Access > Power Management > View IPDUs Info

The IPDU Info form allows you to view all IPDU information (e.g., number of outlets of each unit, current, temperature, alarm threshold levels, firmware, etc.) by serial port.

The form stores historical values of the maximum current and the maximum temperature.

To view IPDU information, perform the following steps:

1. From the top menu bar, select **Access**; from the left menu panel, select **Power Management**; from the form tabs, select **View IPDUs Info**.

The system brings up the **IPDUs Info** form:

Serial Port 4: General Information		
Name: PowerMgm-4	Syslog: ON	Number of Outlets: 8
Number of Units: 1	Buzzer: ON	Over Current Protection: OFF
Master Unit Information:		
Model: PMB 15A	Software Version: 1.2.0	
Alarm Threshold: 15.0A		
Current: 0.0A	Maximum Detected: 0.4A	
Temperature:	Maximum Detected:	

2. To delete the stored values for the maximum detected current, select the **Clear Max Detected Current** button.
3. To delete the stored values for the maximum detected temperature, select the **Clear Max Detected Temperature** button.

A: Technical Specifications

Features

Operating System

- Linux®

Accessibility

- Local (KVM) or Remote (CAT5) User Interfaces

Security

- Local, RADIUS, TACACS+, LDAP and Kerberos authentication
- Token-based strong authentication (SecurID)
- Local backup user authentication support
- User Access Lists per port
- User Access Logging
- System Event Syslog

Server Management

- Access through On Screen Display (OSD)
- Support for port name assignment
- Simultaneous access on the same port (port sharing)
- Cascading with centralized port management (access and configuration)
- Programmable cycling of screens
- Support for VGA resolutions up to 1600 x1200

System Management

- On Screen Display (OSD) for configuration
- Web Management Interface (WMI) for configuration

Appendix A: Technical Specifications

Cabling

- CAT5-based Terminators
- Compatible with PS/2, USB and Sun keyboard/mouse interfaces
- Support for CAT5, CAT5e, CAT6 and CAT7 UTP cabling
- Support for up to 500 ft. distance between Terminator and KVM switch

Upgrades

- Upgrades are available on FTP site at no additional charge
- Flash upgradeable
- TFTP support for network boot

Part Numbers:

ATP4016 AlterPath™ KVM16
16-port switch

ATP4032 AlterPath™ KVM32
32-port switch

ATP4610 AlterPath™ KVM
Terminator PS/2
Server-side Unit, PS/2

ATP4710 AlterPath™ KVM RP
Remote User Interface Unit

Hardware

CPU

- MPC855T (PowerPC Dual-CPU)

Memory

- 128MB DIMM SDRAM / 16MB Compact Flash

Interfaces

- 1 Ethernet 10/100BT on RJ-45
- 1 RS-232 Console on RJ-45
- 1 RS-232 Auxiliary Port on RJ-45
- 16 or 32 RJ-45 KVM Ports (CAT5-based)
- 1 VGA HD15 female and 2 MiniDIN6 (PS/2)

User Interface:

- 1 RJ-45 User Interface (CAT5-based)

Power

- Internal 100-240VAC, 50/60 Hz

Operating Temperature

- 50°F to 112°F (10°C to 44°C)

Storage Temperature

- -40°F to 185°F (-40°C to 85°C)

Humidity

- 5% to 90% non-condensating

Dimensions

- (WxDxH) TBD

Certification FCC Part 15, A

- EN55022, A

This page has been intentionally left blank.

B: KVM Remote Authentication

This section provides some guidelines for configuring remote authentication in the KVM using LDAP and Kerberos. It attempts to address the unique implementation requirements of each protocol from different platforms.

It is assumed that the user already has a fully functional authentication server in place, an administrator who can manage the server, and the username and password for the server has been already configured.

The authentication server administrator must add the KVM/net user, **admin**, to the authentication server. This is to enable the admin user to log in and manage the KVM properly when they are not using local authentication.

Cyclades recommends that the local password and the remote authentication server password be different. Using the same password will not signal a failure of the authentication server and can mislead the administrator because the user will always authenticate.

Remotely authenticated users need not exist in the local KVM user database since they are added automatically with READ/WRITE access to all ports on the KVM. The added users, however, cannot authenticate locally even after entry in the local user database. The system grants local access only if a local password has been set for the user.

LDAP

Regarding LDAP, the KVM web management interface assumes that the distinguished name of the search base is:

“Ldap Base Domain Name” or “**dc=**”

For configurations that use “Organization” or “**o=**” the admin user must edit the configuration file (`/etc/ldap.conf`) using **vi /etc/ldap.conf** and modify the line to “**base o=...**” from “**base dc=...**”

Open Source Authentication Server

Keberos

Required Information:

- Realm name and KDC address
- Realm username (principal) and password
- User admin and realm password

Hostname sensitive (*i.e.*, hostname cannot be a canonicalized error)

The KVM and the authentication server should both have an entry in the hosts file of the KVM.

To add the name and IP address to the KVM host file, use the KVM/net WMI (**Configuration > Network > Host Table**).

Set the KVM hostname by typing in the hostname from the console. The default KVM should be returned if it is new.

Time and Timezone sensitive (clock skew errors)

- KVM and KDC may need to use NTP service using the same NTP server.
- KVM can be set for NTP from the WMI (**Configuration > System > Date/Time**).
- Set the timezone if you are not in the PST zone.

From the console, type in: **set_timezone**

WMI Configuration

Required KVM/net WMI fields:

- Authentication Type: Kerberos

Authentication Down Local

- Kerberos Server (Realm) <192.168.47.125>
- Kerberos Realm Domain Name <cyclades.com>

OSD Configuration

- Authentication Type <Kerberos>
- Authentication down local <Yes/No>
- 1st Authent. server <192.168.47.125>
- Authent. domain <cyclades.com>

LDAP

Required Information

- Domain name and LDAP server address
- Domain username and Domain user password
- User **admin** and Domain password

WMI Configuration

LDAP allows anonymous binds so the only required fields in the WMI are:

- LDAP Server <192.168.47.125>
- LDAP Base Domain Name <dc=cyclades,dc=com>

OSD Configuration

- Authentication Type <LDAP>
- Authent. Down Local <Yes/No>
- 1st Authent. Server <192.168.47.125>
- LDAP Base <dc=cyclades,dc=com>
- LDAP Binddn
- LDAP Attribute
- Authent. Secret
- Secure Auth. <Yes/No>

Windows 2000/2003 Server (AD)

Kerberos

The requirements for Kerberos authentication is the same as that of the Open Source Authentication server.

LDP

Required Information

- Domain name and LDAP server address
- AD username and AD user password
- User **admin** and Domain password

You may want to create an AD user just for authentication binds (Ldap User Name)

WMI Configuration

The aforementioned fields require entries in the KVM/net WMI:

- LDAP Server <192.168.47.59>
- LDAP Base Domain Name <rdcyclades.com>
- LDAP User Name <joe@rdcyclades.com>
- LDAP password <abc123>
- LDAP Login Attribute <samaccountname>

OSD Configuration

- Authentication Type <LDAP>
- Authent. Down Local <Yes/No>
- 1st Authent. Server <192.168.47.125>
- LDAP Base <dc=rdcyclades,dc=com>
- LDAP Binddn <joe@rdcyclades.com>
- LDAP Attribute <samaccountname>
- Authent. Secret <abc123>
- Secure Auth. <Yes/No>

Novell Server (NDS)

LDAP

Ideally the NDS administrator is not named, “admin” to avoid exposing the server administrator password.

Required information is the same as that for Open Source Authentication Server.

WMI and OSD Configuration

See Open Source Authentication Server.

Glossary

3DES

Derived from DES which is an acronym for Data Encryption Standard. DES was originally developed by IBM as Lucifer in the early 1970's. The NSA and NIST used a modified version of Lucifer and named it DES. DES was adopted as the federal standard in 1976 (FIPS (46-3) and ANSI standard X9.32).

However, DES became vulnerable as computers got more powerful and so NIST defined 3DES or Triple DES in 1999. 3DES uses three stages of DES so it is much more secure and suffices for most applications currently. In 2001, NIST replaced DES by AES (Advanced Encryption Standard). It is hoped that AES will remain strong enough for the next 10-20 years.

Advantages of 3DES:

It is easy to implement in both hardware and software compared to other algorithms.

It is based on DES which is a very trusted cipher. DES has been studied thoroughly for over 25 years now and is proven to have sound basics though the keylength is too small now. It is much faster than public key cryptography methods like the RSA method. (Source: [www.3DES and Encryption](http://www.3DESandEncryption.com), Kenneth Castelino)

Authentication

The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.

Basic In/Out System (BIOS)

Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.

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).
CAT-5 (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.
DHCP	<p>Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.</p> <p>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.</p>
Escape Sequence	<p>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.</p> <p>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.</p>

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.
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 <i>IP Security Protocol</i> , IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as for access and trustworthiness control. IPsec provides similar services as SSL, but it works on a network layer. Through IPsec you can create encrypted tunnels (VPN) or encrypt traffic between two hosts.
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	<p>A number used by software to separate the local subnet address from the rest of a given Internet protocol address</p> <p>Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e. 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.</p>
NTP	<i>Network Time Protocol</i> . 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.
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.

- 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.
- 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.

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.