

AlterPath™ KVM/net Installation, Configuration, and User's Guide

Software Version 1.1.0



Cyclades Corporation

3541 Gateway Boulevard
Fremont, CA 94538 USA
1.888.CYCLADES (292.5233)
1.510.771.6100
1.510.771.6200 (fax)
<http://www.cyclades.com>

Release Date: June, 2005

Part Number: PAC0302

©2005 Cyclades Corporation

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

Information in this document is subject to change without notice.

All trademarks, trade names, logos and service marks referenced herein, even when not specifically marked as such, belong to their respective companies and are not to be considered unprotected by law.

The following are registered or registration-pending trademarks of Cyclades Corporation: Cyclades and AlterPath.

ActiveX, Microsoft, Microsoft Internet Explorer, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and other countries.

AIX is a registered trademark of International Business Machines Corporation in the United States and other countries.

FreeBSD is a registered trademark of the FreeBSD Foundation.

HP/UX is a registered trademark of the Hewlett Packard Corporation.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

Mozilla and Mozilla Firefox are trademarks of the Mozilla Foundation.

Sun, Sun Microsystems, Java, J2SE, Solaris, are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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.

Table of Contents

Before You Begin

Audience	ix
Document Organization	ix
Typographical Conventions	x
Naming Conventions	xii
Special Text Notations	xii

1 Introduction

Connectivity and Server Capacity	1-2
Product Components	1-2
KVM Terminator	1-3
KVM RP Switch	1-3
Overview of AlterPath KVM/net	1-4
KVM/net Product Features	1-5
Remote Access Over IP	1-5
Web Management Interface for Configuration and Operation	1-5
Cat-5-Based Cabling	1-6
Server-Based Authentication	1-6
Local User Authentication	1-6
User Access Lists Per Port	1-6
Cascading Support with Centralized Port Management	1-6
Flexibility and Scalability	1-7
On-Screen Display Capability	1-7
Mouse Support	1-7
Multi-User	1-7
Event Logging Capabilities	1-7
The Linux Advantage	1-8
Rack Space Convenience	1-8
Setup Diagram	1-9
Types of Users	1-10
Root User	1-10
Admin User	1-10
Regular User	1-10

2 KVM/net Installation

Product Installation Checklist	2-1
KVM RP Package Contents	2-2
Power Cables	2-3
Rack Mounting the KVM/net.....	2-4
Port Connections	2-4
Installing the AlterPath KVM/net	2-5
Installing the KVM Terminator	2-6
About the KVM/net IP Address	2-7
Configure the COM Port.....	2-7
Determining the IP Address	2-7
Running the Configuration Wizard.....	2-8
Changing the Root Password	2-9
Cascading AlterPath KVM/net	2-10
Connecting a Secondary KVM to a Primary KVM/net	2-11
KVM/net components and connections.....	2-12
Mouse Settings	2-13
Windows XP / Windows 2003	2-13
Windows 2000 / ME.....	2-13
Windows 95 / 98 / NT	2-13
Linux with Graphical Desktop	2-13
Internet Explorer - Security Settings.....	2-14
Installing Mozilla with ActiveX Plug-in.....	2-17
Safety Considerations When Rack Mounting	2-20
Activity LEDs on the KVM/net Ports.....	2-21
LED Functions.....	2-21
LED Status Definitions	2-22
Screen Resolution and Refresh Rate	2-22

3 KVM/net OSD Configuration

OSD and Web Configuration	3-1
Configuring the KVM/net through the OSD.....	3-2
Basic Navigation Keys	3-2
Default Key Sequences	3-2
Sun Key Emulation Using a Non-Sun USB Keyboard.....	3-5
KVM OSD Overview.....	3-6
Logging In.....	3-7
OSD Guidelines	3-7
Saving Your Configuration	3-7

Table of Contents

OSD Main Menu	3-8
Configuration Menu	3-9
General Configuration: Windows Summary	3-10
General Configuration: Authentication Type	3-10
Syslog Facility	3-11
Escape Sequence	3-12
Sun Keyboard	3-12
IP Security	3-13
3DES	3-13
Direct Access	3-14
TCP Viewer Port	3-15
Network Configuration	3-16
DHCP	3-16
IP Address	3-17
Netmask	3-17
Gateway	3-18
DNS Server	3-18
Domain	3-19
Hostname	3-19
Date/Time	3-20
Enabling the NTP Server	3-20
User Station Configuration	3-22
Idle Timeout	3-22
Screen Saver Time	3-23
Cycle Time	3-23
Keyboard Type	3-24
Power Management	3-26
Mouse/Keyboard Sync	3-26
Video Configuration	3-27
Switch Next	3-27
Switch Previous	3-28
Port Info	3-28
KVM Ports	3-29
Selecting a KVM Port to Configure	3-29
Activating a Port	3-30
Server Name	3-30
Power Outlet	3-31
Configuring a Server Connected to a Slave	3-32

Table of Contents

Users and Groups	3-32
Configuring Users	3-33
Adding a User	3-33
Changing the User, Admin, or Root Password.....	3-36
Deleting a User	3-37
Local Groups	3-38
Adding a Group	3-40
Adding a User to a Group.....	3-41
Deleting a User from a Group	3-42
Deleting a Group	3-44
User Access Lists Menu.....	3-45
Generic User	3-45
Adding a User to the User Access List.....	3-46
Edit User/Group.....	3-48
Deleting a User from the User Access List	3-50
Cascade Devices.....	3-51
Cascade Devices Menu	3-52
Adding a Secondary Device	3-52
Syslog.....	3-55
Saving Your Configuration	3-56
Loading Your Configuration.....	3-57
Saving your Configuration to an FTP Server.....	3-58
Loading Configuration from an FTP Server	3-60
System Info Menu	3-62
System Info Window	3-64
Reboot	3-65

4 KVM/net Web Configuration

Overview	4-1
Changing the Password	4-2
Hierarchy of Permissions	4-2
Conflicting Permissions.....	4-2
Complementary Permissions	4-2
Logging In.....	4-3
Direct Access to a Port	4-4
KVM/net Web Management Interface.....	4-5
Wizard Mode.....	4-5
Expert Mode.....	4-6
Button Functions	4-7

Table of Contents

Saving Your Configuration	4-7
Configuring in Wizard Mode.....	4-8
Step 1: Network Settings	4-8
Step 2: Access	4-10
To add a User	4-11
To Delete a User.....	4-12
To Change a User's Password.....	4-12
Step 3: System Log	4-13
To Add a Syslog Server.....	4-13
To Delete a Syslog Server.....	4-14
Configuring in Expert Mode.....	4-14
Table of Menu and Forms.....	4-15
Access	4-16
Connect to Server.....	4-16
Power Management	4-17
Power Management > Outlets Manager	4-17
Power Management > View IPDUs Info	4-19
Power Management > Users Manager.....	4-19
To add a user or edit an assigned user:.....	4-20
To delete an assigned user.....	4-21
Power Management > Configuration.....	4-21
Power Management > Software Upgrade	4-22
Configuration	4-23
KVM	4-24
Default Key Sequences	4-24
Configuring the TCP Viewer Port Address	4-29
Verifying the TCP Port Address	4-30
Devices.....	4-30
To add a secondary KVM to be cascaded to a master KVM/net:	4-31
To edit a device configuration:.....	4-32
To delete a device configuration:	4-34
To Configure Ports	4-34
To Enable or Disable a Port	4-36
Users & Groups.....	4-36
To set KVM/net permissions for a user or a group:	4-37
To delete a user/group from the Access List:.....	4-38
To add a user/group to the Access list (to access KVM/net ports):	4-39
To change a user's password.....	4-40
Security	4-41

Table of Contents

Network.....	4-42
Network > Host Settings	4-43
Network > Syslog.....	4-46
Network > Services	4-47
Network > IP Filtering	4-48
IP Filtering: To add a chain:	4-49
IP Filtering: To edit a chain	4-50
IP Filtering: To Edit a Rule	4-50
Additional Fields	4-54
To Add a Rule.....	4-55
Network > IPsec VPN	4-56
To configure VPN	4-57
Network > SNMP.....	4-60
To configure SNMP.....	4-60
Network > Host Table.....	4-64
Network > Static Routes	4-65
AUX Port	4-67
System	4-69
System > Date/Time	4-69
System > Boot	4-70
Information.....	4-72
General	4-72
To view General information:	4-72
Port Status	4-73
Management.....	4-73
Backup Configuration	4-74
Firmware Upgrade.....	4-75
Microcode Upgrade.....	4-76
To update a microcode:	4-76
Microcode Reset.....	4-77
Active Sessions	4-78
Reboot	4-80

5 KVM/net Operation

Logging In.....	5-2
KVM/net Web Management Interface.....	5-3
Connecting to a Server	5-4
Connecting to the Server through the OSD.....	5-6
Returning to the OSD Main Menu	5-8

Table of Contents

KVM/net View Settings.....	5-9
Recommended Settings.....	5-9
Options Menu.....	5-9
Setting the Viewer Options	5-10
Connection Menu	5-11
Overlaying Connection Menu: Navigation Keys.....	5-12
Default Key Sequences.....	5-12
Sun USB Keyboard Emulation.....	5-13
Changing the Root Password.....	5-14
Differences in OSD Functions	5-15
How to Read the Port Numbers	5-15
Cycling Among Servers.....	5-16
Cycle by Server.....	5-16
Cycle by Key Sequence	5-17
Using the KVM RP to Extend Operation	5-18
Operating through the Remote Presence (RP)	5-18
Finishing your Session.....	5-19
Method 1: Exiting from the AlterPath Viewer Client	5-19
Method 2: Exiting by using the escape sequence.....	5-19
Method 3: Exiting by Idle Timeout.....	5-19
Adjusting Screen Brightness and Contrast	5-20
Automatic (Video) Control Adjustment	5-20
Manual (Brightness/Contrast) Control.....	5-21
Sharing Server Connection	5-22
Resetting Your Keyboard and Mouse.....	5-24
Establishing a Power Control Session	5-25
Power Control by Escape Sequence.....	5-25
Power Control Over IP	5-25
Power Management	5-25
Access > Power management > Outlets Manager.....	5-26

6 Remote Authentication

Open Source Authentication Server.....	6-2
Keberos	6-2
WMI Configuration.....	6-2
OSD Configuration.....	6-2
LDAP	6-3
Required Information	6-3
WMI Configuration.....	6-3

Table of Contents

OSD Configuration.....6-3
Windows 2000/2003 Server (AD)6-3
 Kerberos6-3
 LDAP6-3
 Required Information6-3
 WMI Configuration6-4
 OSD Configuration.....6-4
Novell Server (NDS).....6-4
 LDAP6-4
 WMI and OSD Configuration6-4

A Technical Specifications

FeaturesA-1
HardwareA-3

Glossary

Before You Begin

Welcome to the AlterPath™ KVM/net Manual! This manual is designed to help you install, configure, and operate the AlterPath KVM/net, as well as provide necessary information to guide you in your day-to-day operations of the product.

Audience

This manual is intended for System Administrators and regular users of the AlterPath KVM/net. The regular user is expected to have basic knowledge of using a graphical user interface such as Microsoft Windows or a web browser.

Document Organization

The document is organized as follows:

- | | |
|--------------------------|--|
| 1: Introduction | Defines and explains the overall product features and uses of KVM/net. |
| 2: KVM/net Installation | Explains the procedure for installing and setting up KVM/net. |
| 3: KVM/net Configuration | Explains how to use the user interface, highlighting such procedures as how to configure the KVM/net switch, adding or deleting users, defining user access, adding or deleting server connections, and other topics pertaining to KVM/net administration. |
| 4: Web Configuration | Presents the procedures for configuring the KVM/net switch, adding or deleting users, defining user access, adding or deleting server connections and other KVM/net administration tasks, using the web user interface. |
| 5: KVM/net Operation | Presents the procedures for connecting to a port and other operations related to using the web user interface. |

6: Remote Authentication	Explains the purpose and benefits of using a remote authentication server for added data security.
Appendix A:	Provides KVM/net remote authentication guidelines for Kerberos and LDAP.
Glossary	This is a glossary of terms and acronyms used in the manual.

Typographical Conventions

Screen Labels	Words that appear on the screen are typed in boldface . <i>Examples:</i> The Configuration window; the Password field.
Hypertext Links	With the exception of headings and the Table of Contents (which are already linked), all <u>underlined</u> words are hypertext links.
Important words	Certain words are <i>italicized</i> for emphasis.
Screen Levels	Screen levels are indicated by the “greater than” symbol (>), starting from parent to child to grandchild and so forth, or simply to show the sequence in which they appear. <i>Example:</i> Main Menu > Configure > User Configuration
Untitled Data Fields	Some data entry fields of the GUI windows or forms do not have titles. When this field is described in any field definition section of the manual, the field is indicated as either untitled or by its GUI type, and enclosed in angled brackets. <i>Examples:</i> [untitled] Type in the port number in this field.

[*view table*] Select the user from the view table.

Untitled forms	While most forms are identified by it's menu selection, some forms do not bear the title. The manual uses initial capitals to refer to their names or titles. <i>Examples:</i> The Data Buffering form; the VPN Connections form; the Active Ports Session form.
User entry words	Words or characters that you would type in are shown in <i>courier</i> . <i>Example:</i> myPas8word

Naming Conventions

Form	The form is the largest part of the user interface; it contains the user selection or input fields for each selected item in the menu.
Form Names	The form names of the web user interface do not necessarily appear on the actual window. Because some forms do not have titles, these names are used to distinguish each form as well as to reflect the form function.
KVM/net	Short name for AlterPath KVM/net. This manual uses both terms to refer to the KVM/net switch or unit or as a product line.
Select	To <i>select</i> is the same as to <i>click your mouse</i> .

Special Text Notations

This manual uses special text notations to indicate the following:

Note: *This indicates a note or comment.*

Caution: *This is an alert to take notice of a possibility of a loss of function, a loss of configuration information, or of loss or corruption of data.*

Chapter 1

Introduction

Cyclades AlterPath™ KVM/net is a family of CAT-5-based keyboard-video-mouse switches designed to provide you with full access and control of servers or computers across your network and over the internet. The KVM/net offers a simple and secure way to manage remote servers either locally (up to a distance of 500 feet) or remotely (through a standard web browser¹) from anywhere in the world.

The KVM/net provides two types of web user interface:

- Web configuration interface (for administrators)
- Web user interface (for regular users)

The KVM/net allows you to access any server or workstation (*e.g.*, Windows NT, Windows Server 2003, Windows 9x, Linux, etc.) through a dedicated channel or over the network.

The flexibility of CAT-5 cabling (supporting distances of up to 500 feet between the switch and the managed servers) enables the KVM/net to use any data center's existing cabling infrastructure, providing for an easy installation.

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

The KVM/net supports cascading, a feature which allows you to connect other KVM switches as secondary units connected to a primary KVM/net. Cascading allows data managers to centralize port management and increase the number of managed servers to 1024 servers.

1. The KVM/net viewer uses Active-X and supports **Internet Explorer 6.0**, and (in Windows, with an Active X plug-in) **Netscape 7.x, Mozilla, and Firefox**.

Connectivity and Server Capacity

KVM/net supports two concurrent users:

- two local
- one remote and one local
- two remote

For one primary AlterPath KVM/net 16, you can connect up to eight secondary KVM units (or 16 with 1 user each). For an AlterPath KVM/net 32, you can connect up to 16 KVM units (or 32 with 1 user each) as secondaries. Two connections are used for each secondary-to-primary connection 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.

Through cascading, using one port per secondary unit, AlterPath KVM/net allows you to control up to 1024 servers (in a 1-user configuration or 512 servers in a 2-user configuration) from a single KVM/net console either locally or over the Internet Protocol.

Product Components

The AlterPath KVM/net family comprises four product components:

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

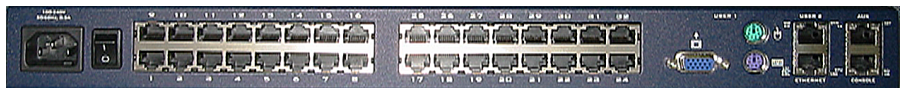


Figure 1.1 - AlterPath KVM/net 32: Back View

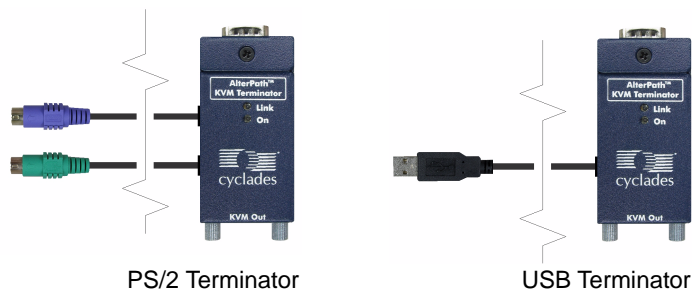
KVM Terminator

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 terminator comes in three models to support the following:

- PC PS/2 (ATP4610)
- PC USB (ATP4630)
- Sun USB (ATP4620)

Note: A PC USB terminator and a Sun USB terminator look identical.



KVM RP Switch

The KVM RP switch allows you to connect a workstation to a local KVM user port so you can switch between your local workstation and the KVM/net. This adds the additional convenience of allowing your workstation to function normally as a workstation, or allowing your workstation to be used as a keyboard, mouse, and monitor plugged directly into the KVM/net. In addition, you can still plug an additional keyboard, mouse, and monitor into the local User 1 port, so another local user can access the KVM/net.

Overview of AlterPath KVM/net

The KVM/net operates by using the keyboard, video, and mouse as the low-level access interfaces to the managed servers, which enables 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/net the only way to manage remote GUI-based servers.

The KVM/net offers advanced options to meet the most demanding user requirements. It provides two types of web interfaces: configuration and user interface. Cascading support, CAT-5-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/net a powerful addition to any data center.



Figure 1.2 - AlterPath KVM/net Product Suite
(From bottom: KVM/net unit front; KVM/net 32 unit back; KVM RP; KVM Terminator.)

KVM/net Product Features

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

- Web Configuration and Operation Interface
- CAT-5-based cabling
- Server-Based Authentication
- Local-User Authentication
- User Access List Per Port
- Cascading Support with Centralized Port Management
- Flexibility and Scalability
- On-Screen Display
- Multi-User
- Event Logging
- Compact 1U design minimizes rack space

Remote Access Over IP

The KVM/net provides users the advantage of accessing servers from any place at any time by enabling full access and server control over the Internet. Unlike an analog KVM switch, KVM-over-IP alleviates the need for physical access to the KVM console. KVM-over-IP allows the user to control the servers using a web browser¹.

Web Management Interface for Configuration and Operation

The KVM/net offers two types of web graphical user interface:

- **Configuration** - Using the web configuration interface, the KVM/net provides a full complement of windows and forms to enable the system administrator full and complete configuration of the KVM/net system and its users.
- **Operation** - Using the web management interface, the regular user can launch the AlterPath Viewer to connect to servers and manage them rap-

1. The KVM/net viewer uses Active-X and supports **Internet Explorer 6.0**, and (in Windows, with an Active X plug-in) **Netscape 7.x, Mozilla, and Firefox**.

ably and easily. The web management interface also allows power management of an IPDU connected to the AUX port.

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/net switch. CAT-5 cabling allows you to use existing cabling infrastructure in the data center. Setup is quick and simple. The KVM/net 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/net.

Server-Based Authentication

The AlterPath KVM/net'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.

In large installations with hundreds of KVM switches that use only locally-stored passwords, each time a new user is added 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

The AlterPath KVM/net also supports local backup user authentication. This allows the system to fall back to local authentication mode in case the server-based authentication server 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/net 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/net 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 eliminates the need to configure the cascaded devices separately.

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. The AlterPath KVM/net chain will automatically connect you to the proper server.

Flexibility and Scalability

Cascading support with centralized port management allows the KVM/net 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/net easily. From the OSD, you can perform tasks such as navigating through the servers, cycling servers, and more.

Mouse Support

The AlterPath KVM/net supports USB and PS/2 mouse interfaces.

Multi-User

The KVM/net supports two concurrent users. The maximum distance between a user and the most remote server is 500 feet. The KVM RP enables an operator to switch the local keyboard, video, and mouse between a local workstation and a server connected to the KVM/net.

The two KVM/net users can be: two remote users (User 1 and User 2), two KVM over IP users (connected to the KVM/net through an Ethernet connection and WEB Management Interface), or one local user and one KVM over IP user.

Event Logging Capabilities

The AlterPath KVM/net provides event logging capabilities that allows your organization to audit its usage and identify who accessed which KVM/net

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/net leverages on Open Source software (Linux), which gives users the freedom to customize its operation or to modify or add features.

Rack Space Convenience

Available in 16 and 32-port models that fit in 1U of rack space, KVM/net helps maximize server availability with scalability and security. Using KVM/net 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/net product components.

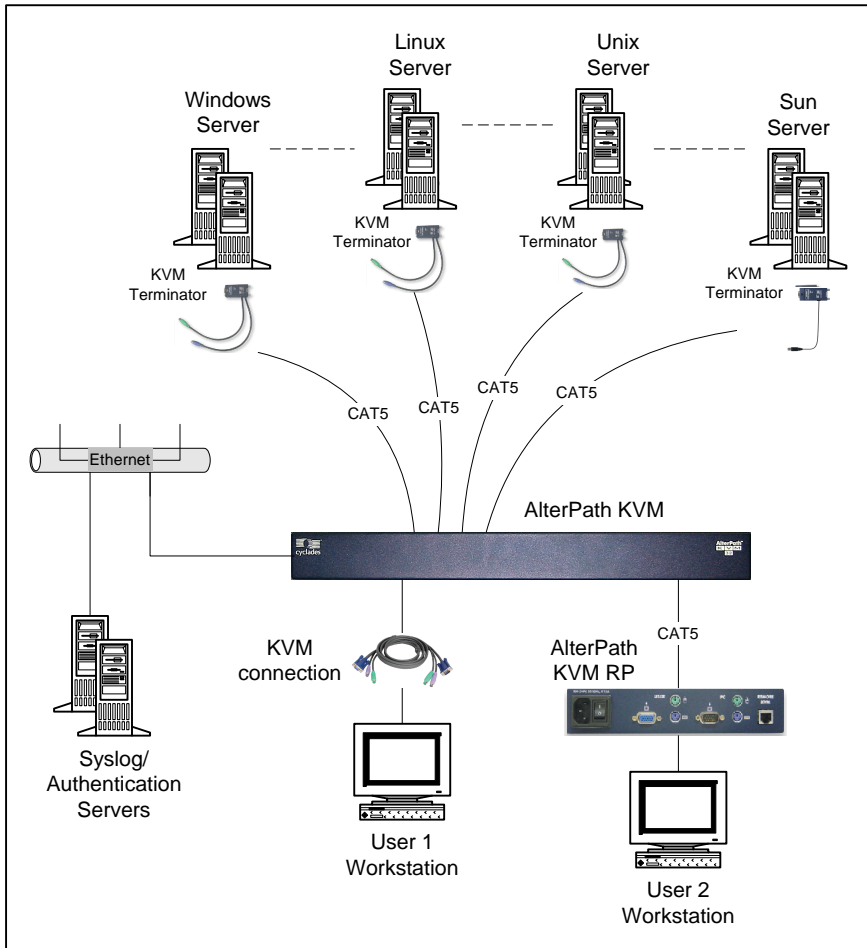


Figure 1.3 - AlterPath KVM/net Setup

Types of Users

KVM/net has three types of users: **root**, **admin**, and the regular user.

Root User

Used in the Linux shell configuration (as in the Configuration Wizard presented in **Chapter 2, KVM/net Installation**), root is the super user of the KVM/net system and cannot be deleted. For security purposes, the root user must change the root password from the Unix shell as soon as possible.

To change the root password:

1. From the Linux shell, log in as **root**, password **cyclades**.
2. Type in the command, **passwd** followed by the new password.

Admin User

The user called admin has full read, write, and system administration privileges of the KVM/net. When running the WMI and the OSD. The default password for the admin user is **cyclades**.

For security purposes, the admin user must change the admin password as soon as possible. To change the admin user password in the WMI, go to **Configuration -> Users & Groups** (or *Step2: Access* in the WMI Wizard).

If the administrator chooses, administrative privileges can be given to additional users, who can then access the WMI and the OSD in admin mode.

Regular User

The regular user is any user configured by the administrator to operate the KVM/net in Access mode. Regular users can access and manage only those consoles to which they are assigned.

<i>User Type</i>	<i>Default Password</i>	<i>Access Privileges</i>	<i>Environment</i>
root	cyclades	Full Read/ Write/Delete, and Admin.	Linux shell only: full access
admin	cyclades	Full Read/ Write/Delete, and Admin.	WMI, OSD: Full Read/Write, power mgmt, admin. Linux shell: IP configuration access. Can write in own directory.
[regular user]	as assigned by the admin.	Limited Read/ Write	WMI, OSD: KVM port access, Power mgmt, as assigned by admin. Linux shell: read access. Can write in own directory.

1: Introduction

Chapter 2

KVM/net Installation

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

- Product Installation Checklist
- Rack Mounting and Connecting the KVM/net Components
- Installing AlterPath KVM/net
- Cascading AlterPath KVM/net
- Mouse Settings
- Internet Explorer: Security Settings

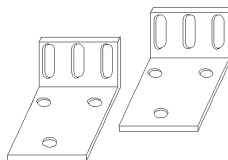
Product Installation Checklist

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

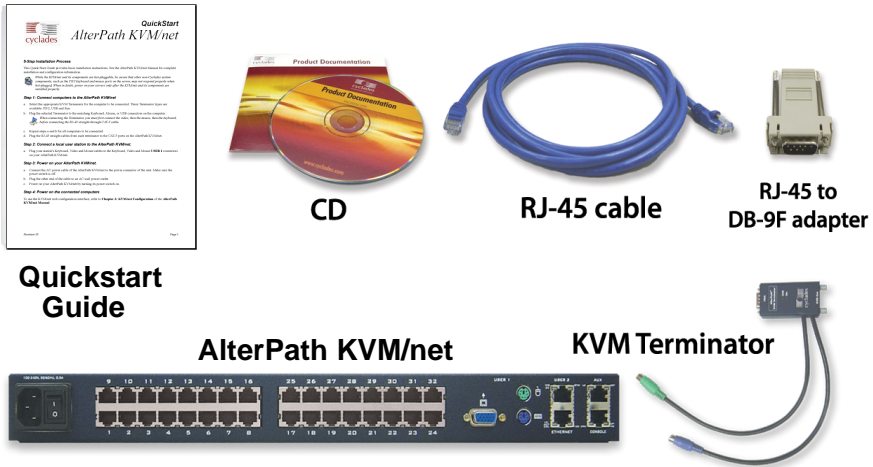
- 1 AlterPath KVM/net
- 1 RJ-45 straight-through cable, with all 4 pairs wired (CAB0018)
- 1 RJ-45 to DB-9F crossover adapter (ADB0036)
- 1 Power cable
- 1 Rack mounting kit (HAR0370)
- 1 Documentation CD
- 1 Quick Start Guide

In addition, you will need to order one or more KVM terminators that support either PS/2 keyboard and mouse, USB keyboard and mouse, or Sun Microsystems USB keyboard and mouse.

The Rack Mounting Kit (P/N HAR0370) is shown below:



2: KVM/net Installation



KVM RP Package Contents

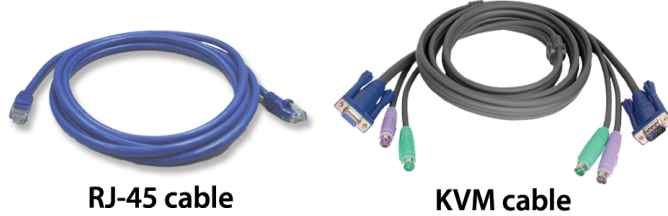
Your AlterPath KVM RP should contain the following items:

- 1 AlterPath KVM RP
- 1 RJ-45 straight-through CAT-5 cable, with all 4 pairs wired (CAB0018)
- 1 Power cable
- 1 KVM cable (CAB00147)
- 4 Bumpon Protec Pads (PAC0149)
- 1 Quick Start Guide

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

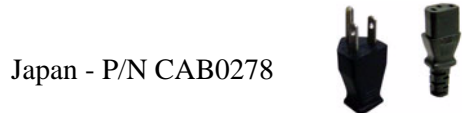
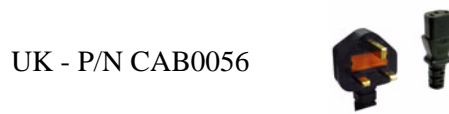
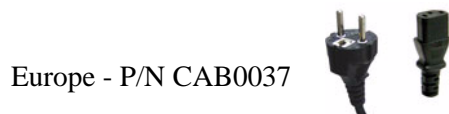
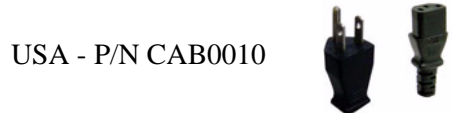
Note: *KVM terminators must be ordered separately.
The power cord and mounting kit are not shown.*

The contents of a typical AlterPath KVM RP package follows:



Power Cables

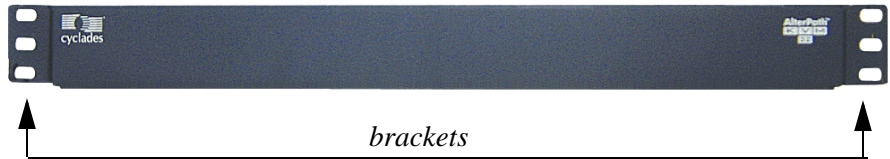
Power cables vary according to the country where the products ship.



Rack Mounting the KVM/net

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

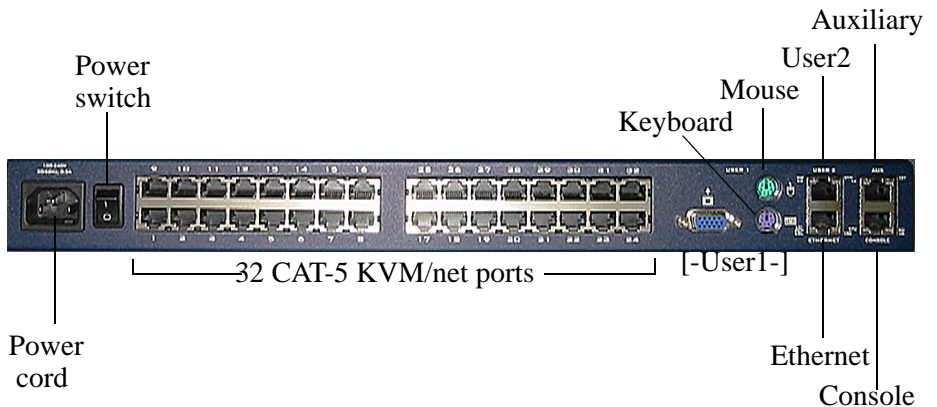
1. Install the brackets onto the front corners of the box using a screw driver and the screws and bolts provided with the rack mounting kit.



2. Mount the KVM/net box in a secure position.
Refer to the “*Safety Considerations When Rack Mounting*” on page 2 - 20 section of this chapter to ensure safety.

Port Connections

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



Installing the AlterPath KVM/net

Caution: *While the KVM/net 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/net and its components are installed properly.*

Caution: Important note about KVM/net port connections:

Be sure that all cables in the path are CAT-5 or better cable with all 4 pairs wired. Be sure that if the path runs through a patch panel, that the patch panel has the connections for all 4 pairs wired. Do not assume that this is always the case for an RJ-45 patch panel.

To install your AlterPath KVM/net, follow the procedure below:

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

Notes: *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.*

There are differences in connections for different terminator types.

<i>Terminator Type</i>	<i>Connection</i>
PS/2	keyboard, video, mouse
Sun-USB, PC-USB	video, USB

- c. Repeat steps a and b for all computers to be connected.
 - d. Plug the RJ-45 straight cables from each terminator to the CAT-5 ports on the AlterPath KVM/net.
2. Connect a local user station to the AlterPath KVM/net.
 - a. Plug your station's Keyboard, Video and Mouse cables to the Keyboard, Video and Mouse **USER 1** connectors on your AlterPath KVM/net.

2: KVM/net Installation

3. *Optional.* Connect the Remote Point Unit (RP) to the AlterPath KVM/net.
 - a. If you are NOT using an AlterPath KVM RP, skip this and proceed to step 4.
 - b. Plug your Keyboard, Video and Mouse to the Keyboard, Video and Mouse connectors on your AlterPath KVM RP.
 - c. Using the supplied KVM cable, plug your station's Keyboard, Video and Mouse to the Keyboard, Video and Mouse Local PC connectors on your AlterPath KVM RP.
 - d. 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/net.
4. Power on your AlterPath KVM/net.
 - a. Connect the AC power cable of the AlterPath KVM/net 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/net by turning its power switch on.
5. *Optional.* Power on your AlterPath KVM RP.

Note: *If you have a workstation connected to your AlterPath KVM RP, the Keyboard interface on your workstation will power the RP, and 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: KVM/net Configuration.

Installing the KVM Terminator

This section provides a more detailed description on how to install the KVM Terminator. To install the KVM Terminator, follow the steps below:

1. *Optional.* If the server VGA connector is too recessed, use an HD15 mini extender. Insert it firmly into the server VGA connector and tighten both screws evenly and firmly, but do not over-tighten.

2. Insert the Terminator onto the server VGA connector (or onto the mini extender installed in step 1) and tighten the screws evenly and firmly, but do not over-tighten.
3. Insert the mouse connector (green) firmly into the mouse receptacle.
4. Insert the keyboard connector (purple) firmly into the keyboard receptacle.
5. Proceed with the KVM/net installation as outlined in the preceding section.

About the KVM/net IP Address

Configure the COM Port

In order to determine the KVM/net's IP address and to run the Configuration Wizard, you will need to configure the COM port as follows:

1. Connect your PC terminal to the console port of your AlterPath KVM/net
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) to access the console.

Determining the IP Address

The KVM/net switch comes with DHCP client enabled. When you connect the ethernet port to your LAN, the KVM/net gets its IP address from your DHCP server automatically. If, however, there is no DHCP server available, then the DHCP request will fail, and the default IP address (192.168.160.10) will be used.

To determine the IP address, log on to the console as root. Then enter the command: **ifconfig**

A display containing the IP address of the KVM/net will shown on the console.

2: KVM/net Installation

Once the KVM/net is assigned an IP address, any user on the network should be able to access the KVM/net through the web user interface.

Running the Configuration Wizard

Using the Configuration Wizard through the console is another method by which you can determine as well as configure the KVM/net IP address.

Run the Configuration Wizard as follows

1. Log into the console port as **root**, using the password: **cyclades**.
2. Enter the command: **wiz**

The system launches the Configuration Wizard. Accept the default values by pressing the <Enter> key or provide your own parameter values. This procedure highlights some critical questions from the wizard:

Set to defaults (y/n)[n]: Press <Enter> to accept default value.

Hostname [kvm]: Press <Enter> to accept default hostname, otherwise enter your own hostname.

Do you want to use DHCP to automatically assign an IP for your system? (y/n)[n]: Press <Enter> to accept default value.

System IP[192.168.160.10]: Press <Enter> to accept default IP, otherwise enter your own IP address.

.
. .
.

Are all the parameters correct? (y/n)[n]: Enter **y** if correct, otherwise press <Enter> and re-start the configuration wizard.

Do you want to save your configuration to Flash? (y/n)[n]: Enter **y** to save your configuration in Flash. This last question concludes the wizard.

3. If you want to confirm your configuration, enter the command: **ifconfig** from the console.

The system will list all the parameter values that you have just configured though the Configuration Wizard.

Note: *If you reboot a KVM/net that has an IP address that was assigned using DHCP, the IP address can change during the next boot sequence.*

Changing the Root Password

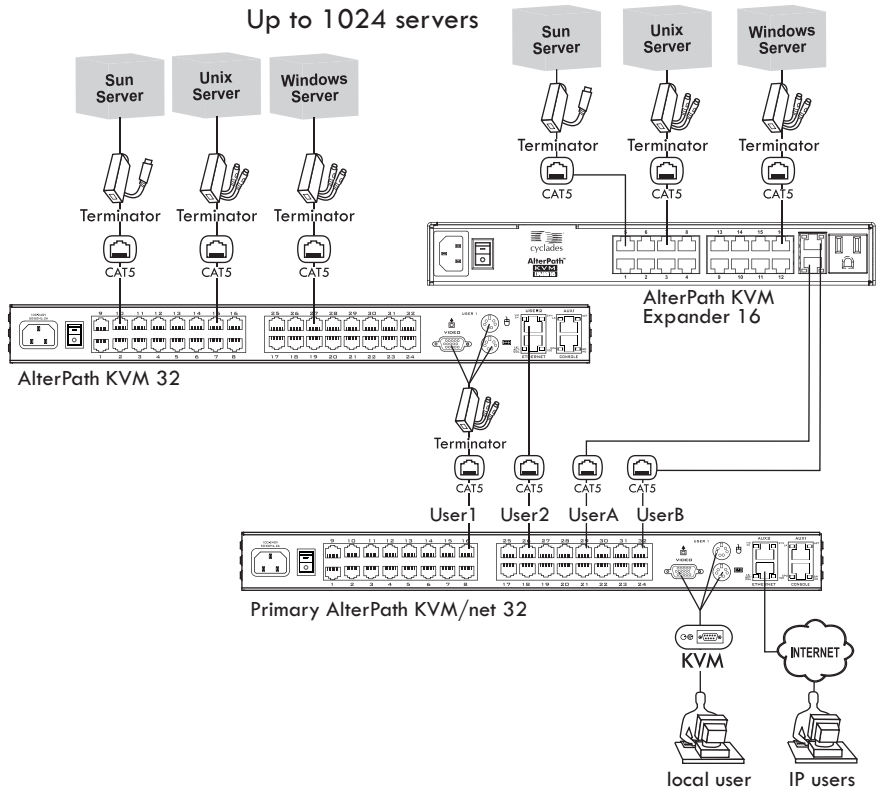
For security, you should consider changing your root password at the soonest convenience.

To Change your root password, follow the procedure below:

1. Open your terminal emulation application (HyperTerminal, Kermit, or Minicom).
2. Log in as: **root** Password: **Cyclades**
3. At system prompt, enter the command: **passwd**
4. Type in your new password when prompted.
5. Save your new password to Flash by typing in: **saveconf**
6. Close your terminal session.

Cascading AlterPath KVM/net

A typical cascading configuration is shown here:



The AlterPath KVM/net can be cascaded to support up to 1024 computers. You will need to use a single-user configuration to connect a primary KVM/net 32 to up to 32 secondary KVM 32 units. For this configuration, you connect one CAT-5 cable from a primary KVM port to the USER 2 port of a secondary KVM unit. Repeat this for each secondary KVM unit you wish to cascade.

You can support up to 512 computers with a 2-user configuration. You will need to connect a KVM/net 32 to up to 16 secondary KVM 32 units. For this configuration, you connect one CAT-5 cable from a primary KVM port to the USER 2 port of a secondary KVM unit and another CAT-5 cable from another primary KVM port to the USER 1 port (using a PS/2 terminator) of the same

secondary KVM unit. Repeat this for each secondary KVM unit you wish to cascade.

Connecting a Secondary KVM to a Primary KVM/net

To connect a secondary KVM to a primary KVM/net perform the following steps:

1. Ensure that all hardware (KVM/net switches and computers) to be connected are switched off.
2. Connect a CAT-5 cable from a primary KVM/net port to the **USER 2** (for remote station) port of the secondary KVM.

Note: *For a single-user configuration, skip Steps 3 and 4.*

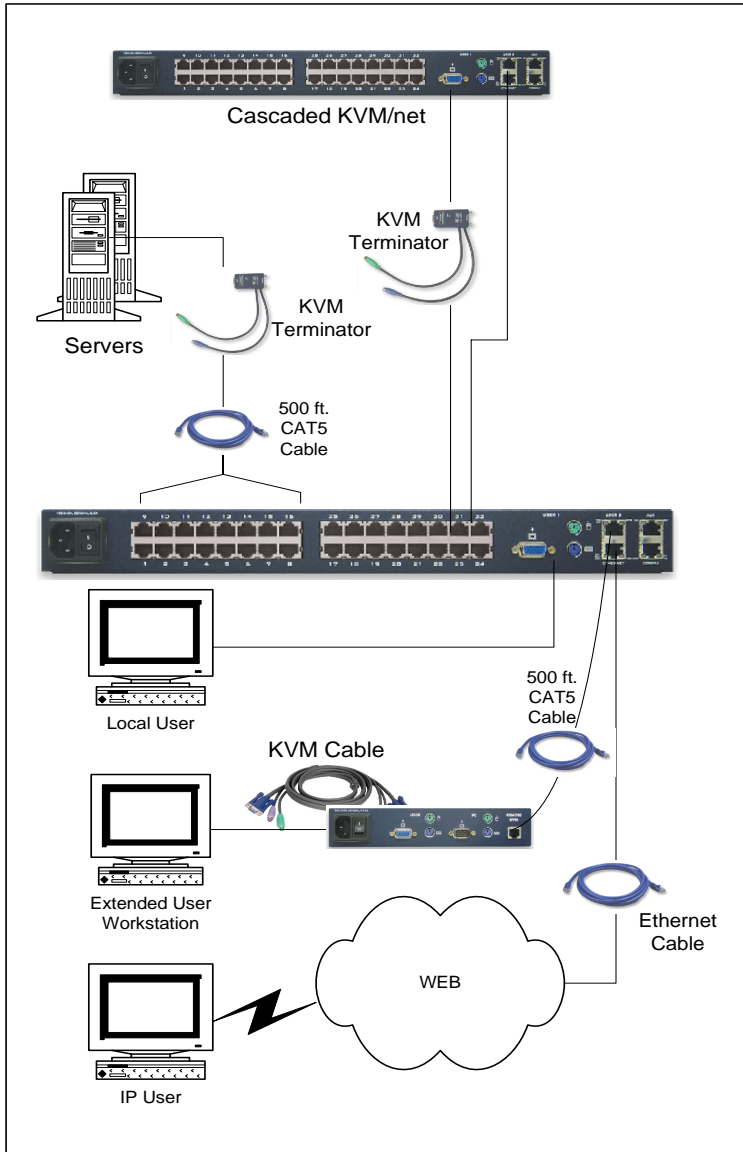
3. Connect a KVM Terminator to the **USER 1** (for local station) port of the secondary KVM.
4. Connect CAT-5 cable from a primary KVM/net port to the KVM Terminator connected to the secondary KVM USER1 port.
5. Repeat steps 1 through 4 for each secondary KVM to be connected to the primary KVM/net.

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

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

KVM/net components and connections

Below is a schematic diagram of the KVM/net components and connections as discussed in the installation procedure.



Mouse Settings

For optimal mouse performance, ensure that your mouse pointer acceleration and related enhancement features are disabled so 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 moving 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 moving 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
- To set these values, use the *xset* command:
- ```
> xset m 1 1
```

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

```
> xset m 0
```

Or reset the acceleration and threshold to the default values (acceleration 2/1, threshold 4) as follows:

## 2: KVM/net Installation

```
> xset m default
- OR -
> xset m 1 10
```

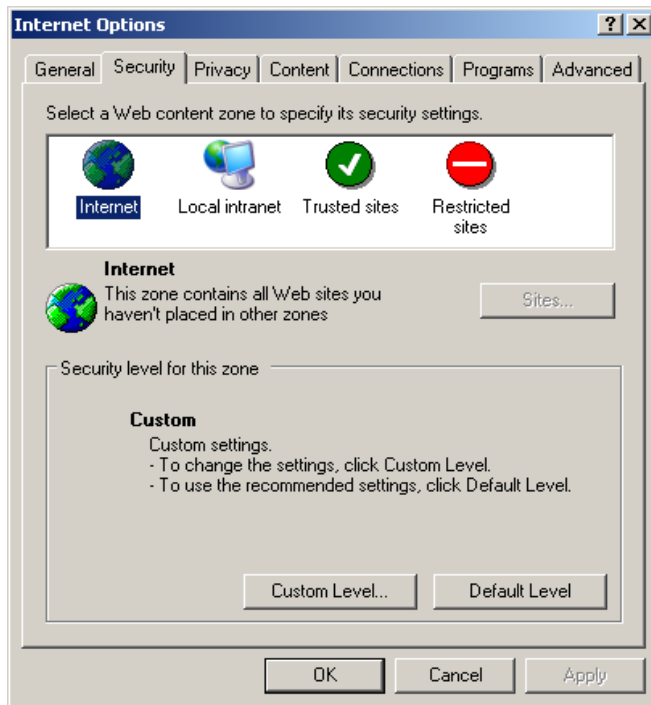
All servers work with any of the above settings, albeit each system may vary slightly.

### **Internet Explorer - Security Settings**

Installing Windows XP SP2 in the workstation affects the Internet Explorer Security settings. This procedure is for users who may encounter a security error after installing XP SP2 and attempt to connect to a server on the KVM/net through the AlterPath viewer. For ActiveX to download successfully, configure the Security Settings as follows:

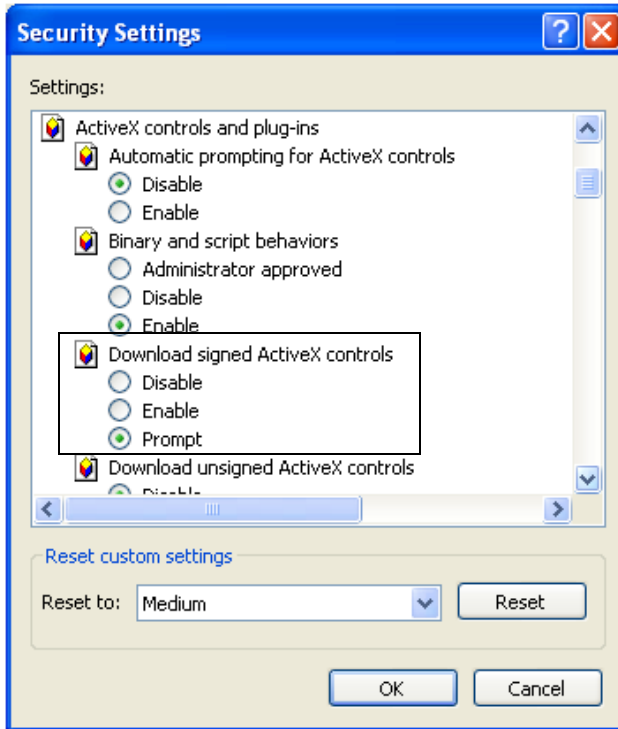
1. From the Internet Explorer menu bar, select **Tools > Internet Options > Security Tab**.

The system displays the **Security** tabbed form.





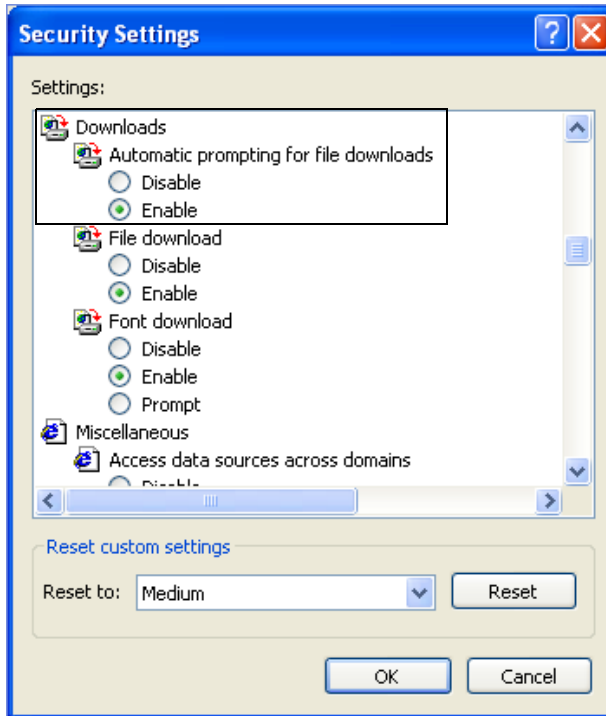
2. If your web content zone is set up for local intranet, then select **Local intranet**; otherwise, keep the default **Internet** setting.
3. From the **Security** tabbed form, click on the **Custom Level** button. The system displays the **Security Settings** form.
4. From the Security Settings form, look for the primary heading, **ActiveX controls and plug-ins**, and its third subheading, **Download signed ActiveX controls** as shown:



5. For the subheading, **Download signed ActiveX controls**, you have two options: **Enable** or **Prompt**.  
 If you select **Enable**, then your configuration ends here. Press the **OK** button to save your configuration.  
 If you select **Prompt**, then you must proceed to step 6.

## 2: KVM/net Installation

6. Go to the heading, **Downloads**, and then subheading, **Automatic prompting for file downloads** as shown:



7. Under the subheading, **Automatic prompting for file downloads**, select **Enable**.
8. Select the **OK** button.

## Installing Mozilla with ActiveX Plug-in

To install Mozilla 1.7 with ActiveX plug-in for Windows, follow the steps below:

1. From your internet browser, go to: <http://www.mozilla.org/products/mozilla1.x/>

The browser opens the following page:



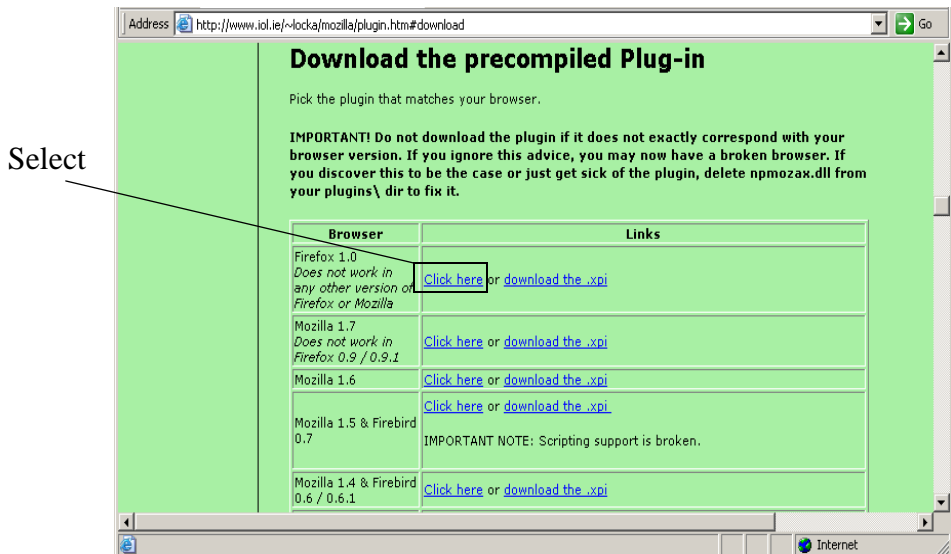
2. From the Download Now section of the page, select **Windows, English**.
3. Go to: <http://www.iol.ie/~locka/mozilla/plugin.htm>

## 2: KVM/net Installation

The browser displays the following page:



4. From the left menu panel of this page, click on **Download the Plug-in**. The browser displays the following page:



5. From the top row of the table (Mozilla 1.7), select **Click here** to start the plug-in installation.  
The system displays a Software Installation dialog box with the following message: A web site is requesting to install Mozilla 1.7 ActiveX Plug-In.
6. Click on **Install** to proceed with the installation.  
After the installation, the system displays a Successful Installation notice.
7. Click on OK.
8. Restart Mozilla.
9. To confirm that ActiveX is installed, after starting Mozilla, go to **Help > About plug-ins**. It shows all plug-ins installed in your Mozilla. Check to ensure that ActiveX is included.

### **Safety Considerations When Rack Mounting**

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

#### *Operating Temperature*

The operating temperature range that Cyclades recommends for the KVM/net is: 50° to 112°F (10°C to 44°C).

#### *Elevated operating ambient temperature*

If you install the KVM/net 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 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*

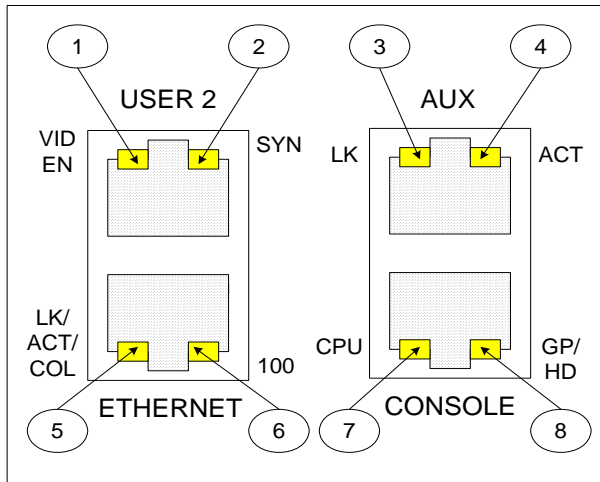
Maintain reliable earthing of rack mounted equipment by inspecting supply connections other than direct connections to the branch circuit such as power strips or extension cords.

## Activity LEDs on the KVM/net Ports

The KVM/net unit comes with paired 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.

| <i>LED No.</i> | <i>Function</i>                           |
|----------------|-------------------------------------------|
| 1 and 2        | Monitors KVM CAT5 video output interface. |
| 3 and 4        | Monitors async interface.                 |
| 5 and 6        | Monitors Ethernet signals.                |
| 7              | Monitors CPU control.                     |
| 8              | Not used.                                 |

### LED Status Definitions

| <i>LED No.</i> | <i>Label</i> | <i>Color</i> | <i>Status</i>                                             |
|----------------|--------------|--------------|-----------------------------------------------------------|
| 1              | VID EN       | Off          | No video signal.                                          |
| 1              | VID EN       | Green        | Video enabled.                                            |
| 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        | Steady = Link, Blinking = Activity.                       |
| 5              | LK/ACT/COL   | Orange       | Collision.                                                |
| 6              | 100          | Green        | Speed 100.                                                |
| 6              | 100          | Off          | Speed 10.                                                 |
| 7              | CPU          | Green        | CPU control active.                                       |
| 8              | GP/HD        |              | Not Used                                                  |

### Screen Resolution and Refresh Rate

The table below summarizes the refresh rates for various screen resolutions.

| <i>Resolution</i>                 | <i>Refresh Rates (Hz)</i>                  |
|-----------------------------------|--------------------------------------------|
| 640 x 480                         | 60, 72, 75, 85, 90, 100, 120               |
| 720 x 400<br>(standard text mode) | 75                                         |
| 800 x 600                         | 60, 70, 72, 75, 85, 90, 100, 120, 160      |
| 1024 x 768                        | 60, 70, 72, 75, 85, 90, 100, 120, 150, 160 |
| 1152 x 864                        | 60, 70, 75, 85                             |
| 1150 x 900                        | 66                                         |
| 1280 x 1024                       | 60                                         |



# Chapter 3

## KVM/net OSD Configuration

---

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

- Configuring the KVM/net through the OSD
  - Basic Navigation Keys
  - Default Key Sequences
  - KVM/net 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/net:

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

## Configuring the KVM/net through the OSD

### Basic Navigation Keys

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

| <i>Key</i>                 | <i>Action</i>                             |
|----------------------------|-------------------------------------------|
| <b>TAB</b>                 | Changes between fields on the window      |
| <b>UP / DOWN</b>           | Scrolls within a menu                     |
| <b>LEFT / RIGHT</b>        | Selects a button in a button field        |
| <b>BACKSPACE</b>           | Deletes the character left to the cursor  |
| <b>PAGE UP / PAGE DOWN</b> | Pages within a menu                       |
| <b>END</b>                 | Moves to the end of a menu                |
| <b>HOME</b>                | Moves to the top of a menu                |
| <b>ENTER</b>               | 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/net application. Typically, an escape sequence begins with an escape character, but this is not universally true.

In KVM/net, the default key sequence (Ctrl-K, Q) for closing a window (which does not save any changes made) while connected to a port is also called *escape sequence*.

You can use the following default key sequences to perform a specific action:

| <i>Key Sequence</i>      | <i>Action</i>                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Ctrl-K> <Q>             | Quit command - closes the port session and takes you back to the KVM Main Menu.                                                                                                                                                       |
| <Ctrl-K> <P>             | Port command - initiates a power control session.                                                                                                                                                                                     |
| <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 command - resets the keyboard and mouse interface if either of these becomes unavailable after adding a new server to the KVM/net.<br><b>Caution:</b> Causes the keyboard and mouse to stop working on some servers. |

You can change or modify the escape key sequences in the User Configuration (Main Menu > Configure > User Configuration). See User Configuration section.

There is also a set of escape key sequences for the RP switch. These are invoked by pressing Scroll Lock twice in quick succession, followed immediately by the command character.

**Note:** *You cannot modify the RP escape key sequences.*

The RP switch escape sequences are shown in the following table:

### 3: KVM/net Configuration

| <i>Key Sequence</i>                         | <i>Action</i>                                                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------|
| <Scroll Lock> <Scroll Lock><br><L>          | RP Switch to Local command - switches the AlterPath KVM RP video display to the local computer.   |
| <Scroll Lock> <Scroll Lock><br><R>          | RP Switch to Remote command - switches the AlterPath KVM RP video display to the remote computer. |
| <Scroll Lock> <Scroll Lock><br><N>          | RP Beep On - switches the beeper on when switching between devices (local-remote).                |
| <Scroll Lock> <Scroll Lock><br><F>          | RP Beep Off - switches the beeper off when switching between devices (local-remote).              |
| <Scroll Lock> <Scroll Lock><br><Esc>        | Microcontroller Reset - resets the RP local microcontroller.                                      |
| <Scroll Lock> <Scroll Lock><br><up arrow>   | Increase Brightness - increases the video brightness                                              |
| <Scroll Lock> <Scroll Lock><br><down arrow> | Decrease Brightness - dims or decreases the video brightness.                                     |

## Sun Key Emulation Using a Non-Sun USB Keyboard

Using the OSD, you can configure a PS/2 keyboard to emulate the Sun unique keyboard actions. The table below summarizes the keys.

| <i>PS/2 Keyboard Key</i> | <i>Mapped Sun Key Equivalent</i> |
|--------------------------|----------------------------------|
| <b>F2</b>                | Again                            |
| <b>F3</b>                | Props                            |
| <b>F4</b>                | Undo                             |
| <b>F5</b>                | Front                            |
| <b>F6</b>                | Copy                             |
| <b>F7</b>                | Open                             |
| <b>F8</b>                | Paste                            |
| <b>F9</b>                | Find                             |
| <b>F10</b>               | Cut                              |
| <b>F11</b>               | Help                             |
| <b>F12</b>               | Mute                             |
| * [numpad]               | Compose                          |
| + [numpad]               | Vol+                             |
| - [numpad]               | Vol-                             |

## KVM OSD 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:

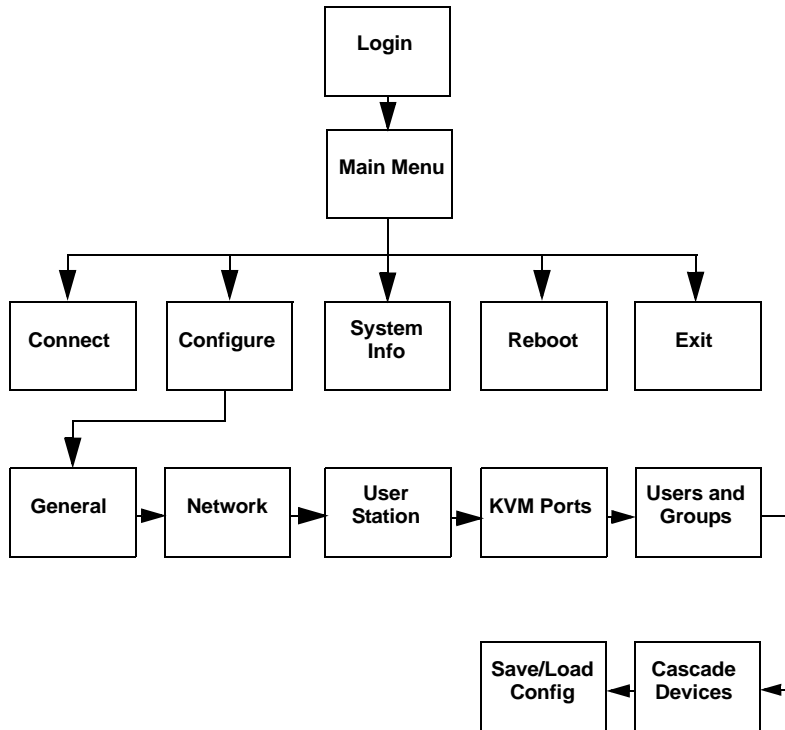


Figure 3.1 - KVM GUI Structure (top three levels only)

**Note:** 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**

In most cases, changes take effect as soon as you make them and press <Enter>. However, the changes will be forgotten if you reboot. Therefore, be sure to go the Save/Config menu to save all your changes after you finish with your configuration (see Figure 3.1 - KVM GUI Structure (top three levels only)).

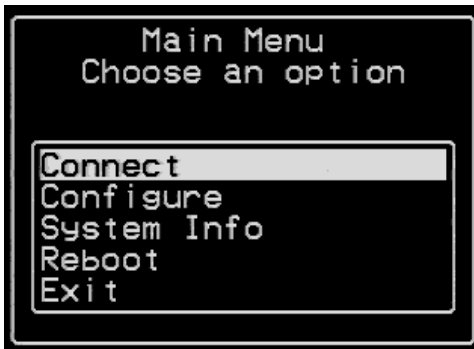
Press <Esc> to return to the last main menu.

## OSD Main Menu

The OSD Main Menu provides three selections:

| <i>Menu Selection</i> | <i>Select the menu item to:</i>                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Connect</b>        | 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. |
| <b>Configure</b>      | View the Configuration Menu.                                                                                                                           |
| <b>System Info</b>    | View the system information pertaining to the KVM version that you are using.                                                                          |
| <b>Reboot</b>         | Reboot the KVM/net Switch.                                                                                                                             |
| <b>Exit</b>           | Close the OSD session.                                                                                                                                 |

The actual menu as viewed from the OSD:



**Note:** *The WMI counterparts of these functions are discussed in Chapter 5, KVM/net Operation*

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

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

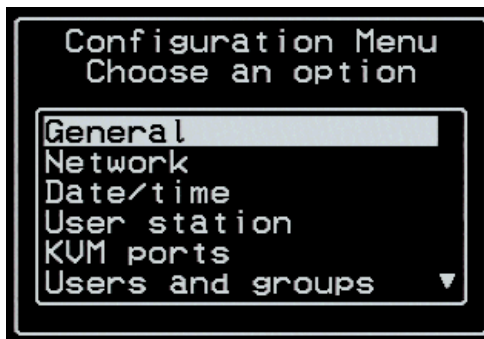


## Configuration Menu

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

| <i>Menu Selection</i>   | <i>Select the menu item to:</i>                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>          | Configure authentication type, authentication servers, syslog facility, Escape Sequence, and Sun Keyboard.                                             |
| <b>Network</b>          | Configure DHCP and/or IP address,                                                                                                                      |
| <b>Date/Time</b>        | Enable/disable NTP; manually configure the system date and time.                                                                                       |
| <b>User Station</b>     | Configure the work station's idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current workstation. |
| <b>KVM Ports</b>        | Activate ports, name servers, and configure power outlets.                                                                                             |
| <b>Users and Groups</b> | Configure local users and groups, set up user passwords, and update the User Access List.                                                              |
| <b>Cascade Devices</b>  | Add, edit or delete devices in connection with cascading.                                                                                              |
| <b>Syslog</b>           | Configure the address of the syslog server.                                                                                                            |
| <b>Save/Load Config</b> | Save or load configuration, and restore configuration to factory default values.                                                                       |
| <b>Exit</b>             | 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:

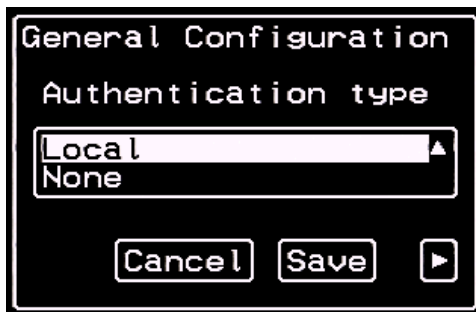
| <i>Menu Selection</i>      | <i>Select the menu item to:</i>                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Type</b> | Assign the authentication type. (Select from: None, Local, Radius, TacacsPlus, Kerberos, LDAP, and Windows NT/2K/2K3.) |
| <b>Syslog Facility</b>     | Define the number which the target syslog server will use as a message identifier. Values are from 0 through 7.        |
| <b>Escape Sequence</b>     | Configure the escape sequence (default is ^K).                                                                         |
| <b>Sun Keyboard</b>        | Enable your keyboard to simulate the Sun keyboard.                                                                     |
| <b>IP Security Level</b>   | Disable or enable IP security to extend to the keyboard/mouse or keyboard/video/mouse.                                 |
| <b>3DES</b>                | Disable or enable 3DES encryption.                                                                                     |
| <b>Direct Access</b>       | Enable direct access to a port from the Login screen.                                                                  |
| <b>TCP Port Viewer</b>     | Assign your own TCP Port Viewer address or range or addresses, and override the default address.                       |

**Note:** *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/net 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.

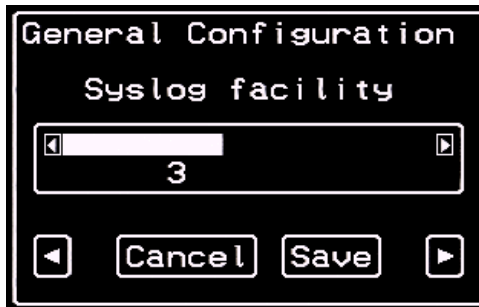
**Note:** *The type of dialog windows that appear depend on the type of authentication that you define in the Authentication Type window.*

### Syslog Facility

(Configure > General > Authentication Type > Syslog Facility)

Assigning a Facility Number allows the syslog server to identify and determine how to handle messages generated by devices connected to the KVM ports. In other words, the Facility Number serves as an identifier for messages generated by events relating to the KVM ports.

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

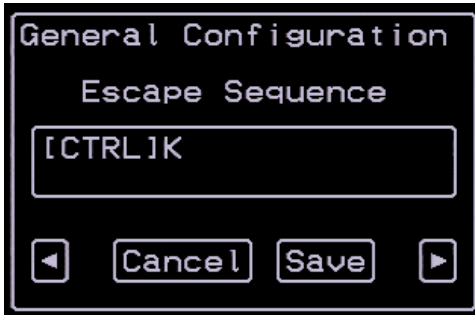


2. From the Syslog Facility window, enter the value (0 through 7) that you wish to use as a message identifier for events relating to the KVM ports.
3. Tab to the next button to configure the **Escape Sequence**.

### 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.

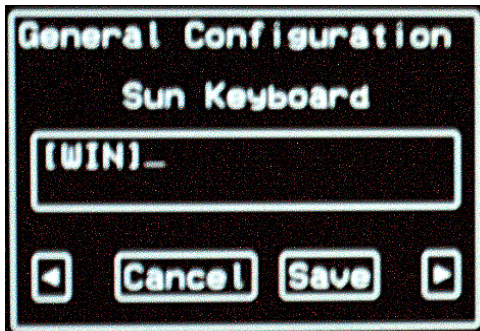


1. From the Escape Sequence window, enter the key sequence for the escape function, or to change the default escape sequence (Ctrl-K).
2. Tab to the Save button and then press <Enter> to save your configuration.

### 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/net.



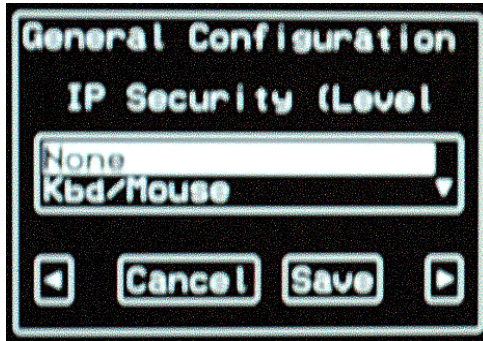
1. From the Sun Keyboard window, enter the keyboard type that you are using (default: WIN).
2. Tab to the forward button to configure the IP Security.

## IP Security

**Note:** This function pertains to the setup of KVM over IP. For more information, see “Security” on page 4 - 41.

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

The IP Security Level window allows you to select the level of IP security to include keyboard and mouse, OR keyboard, video and mouse, OR none.



1. From the IP Security window, select the IP security level (None, Keyboard/Mouse, or Keyboard/Video/Mouse).
2. Tab to the forward button to configure 3DES.

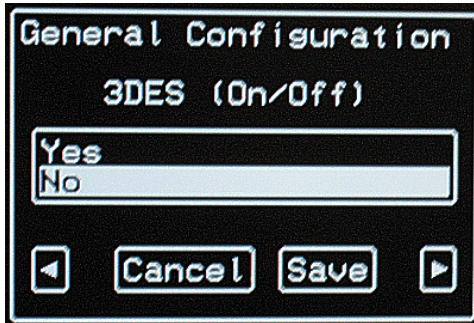
## 3DES

**Note:** This function pertains to the setup of KVM over IP. For more information, see “Security” on page 4 - 41.

(Configure > General > Authentication Type > Syslog Facility > Escape Sequence > Sun Keyboard > IP Security Level > 3DES)

### 3: KVM/net Configuration

The 3DES window allows you to enable or disable 3DES encryption for your IP security. (The system uses RC4 if 3DES is not selected.)



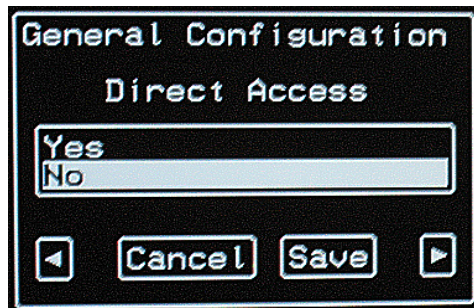
1. From the 3DES window, select **Yes** or **No** to enable or disable 3DES.
2. Tab to the forward button to configure Direct Access.

#### Direct Access

**Note:** *This function pertains to the setup of KVM over IP. For more information, see “Direct Access to a Port” on page 4 - 4.*

(Configure > General > Authentication Type > Syslog Facility > Escape Sequence > Sun Keyboard > IP Security Level > 3DES > Direct Access)

Enabling Direct Access allows you to access a port directly from the Login screen of the KVM web interface through the addition of a Port field.



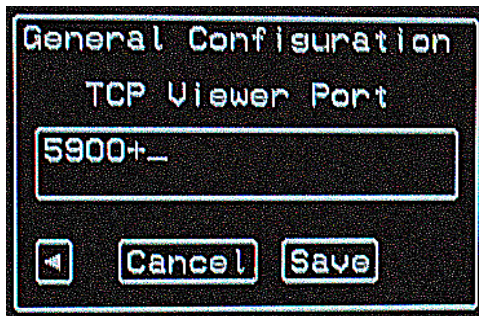
1. From the Direct Access window, select **Yes** or **No** to enable or disable Direct Access.
2. Tab to the forward button to configure the TCP Viewer Port address(es).

## TCP Viewer Port

**Note:** *This function pertains to the setup of KVM over IP. For more information, see “Configuring the TCP Viewer Port Address“ on page 4 - 29.*

(Configure > General > Authentication Type > Syslog Facility > Escape Sequence > Sun Keyboard > IP Security Level > 3DES > Direct Access > TCP Viewer Port)

Except for ports 1 through 1024, the TCP Viewer Port allows you to assign your own TCP port address (or range of addresses) other than the default 5900+.



**WARNING!** *Do not use ports 1 through 1024 to assign ports. These are privileged ports, reserved for system and server software, such as web server, DNS, etc. Using any of these ports to assign your own port address can cause a connection failure or prevent the KVM Viewer from working.*

1. From the TCP Viewer Port window, type in the desired TCP Port Address. 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. Tab to the **Save** button to complete General Configuration.

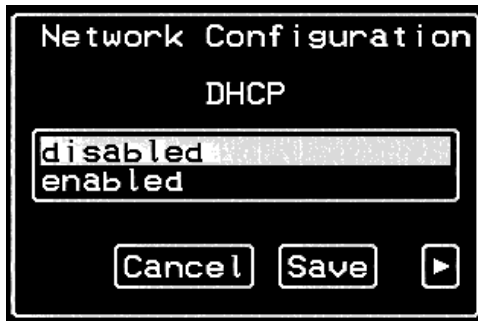
## Network Configuration

The Network Configuration screens allow you to configure the KVM/net 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.



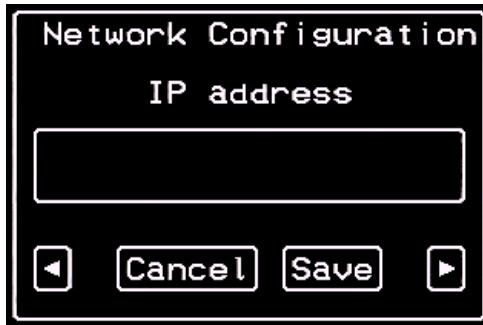
1. From the DHCP dialog window, select from: Disabled, Enabled, or Save.
2. Tab to the next button and press <Enter> to configure the **IP address**.



### IP Address

(Configure > Network > DHCP > IP Address)

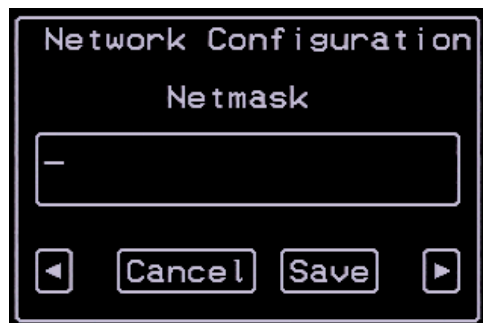
If DHCP is disabled, continue on to the IP Address window and the rest of the Network Configuration windows.



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

### Netmask

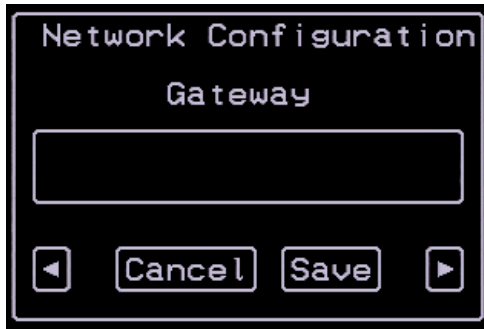
(Configure > Network > DHCP > IP Address > Netmask)



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

### Gateway

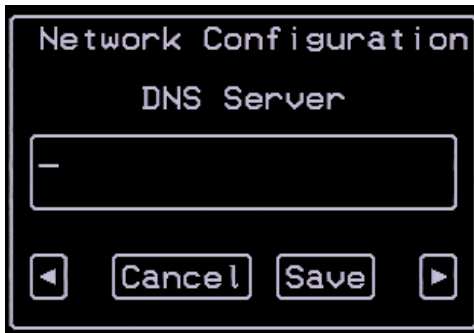
(Configure > Network > DHCP > IP Address > Netmask > Gateway)



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

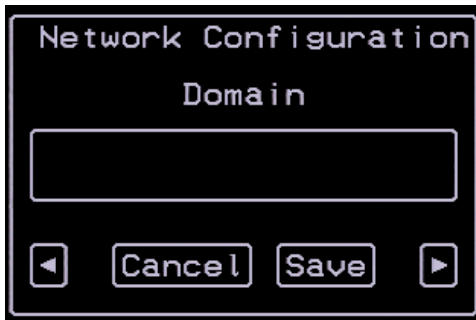
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server)



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

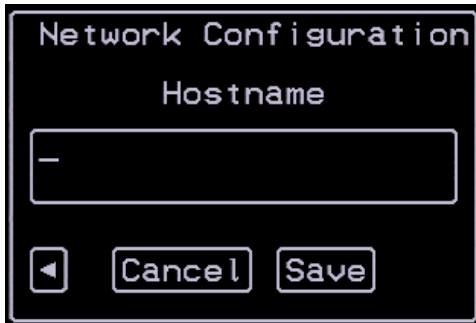
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server > Domain Name)



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

### Hostname

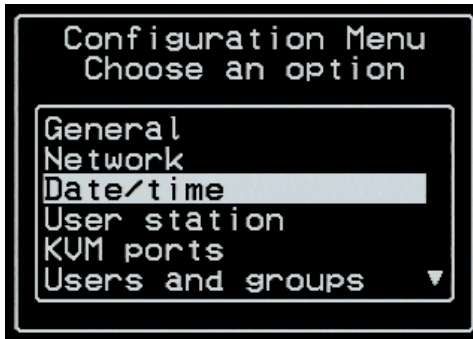
(Configure > Network > DHCP > IP Address > Netmask > Gateway > DNS Server > Domain Name > Hostname).



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:

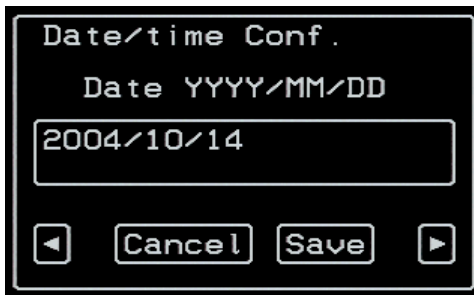


2. Tab to the **Save** button and press <Enter> to complete the procedure.

### Entering the Date and Time Manually

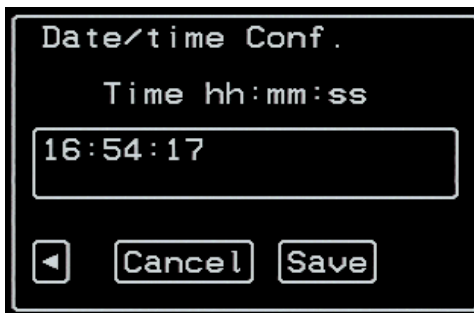
1. From the NTP window, select **disabled** and press <Enter>.

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>.

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

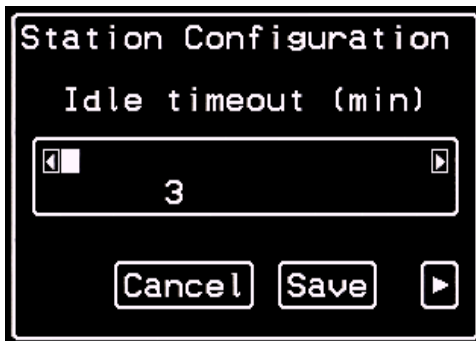
The keyboard escape sequences for the following commands

- 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.

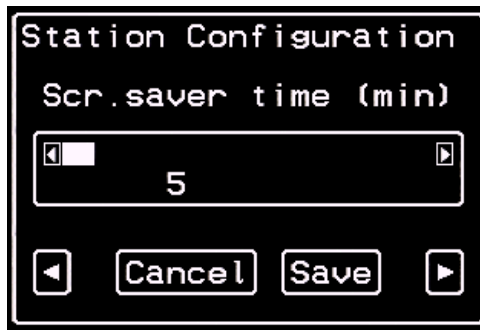
**Note:** A setting of “0” disables the timeout.

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. 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.

**Note:** A setting of “0” disables the screen saver.

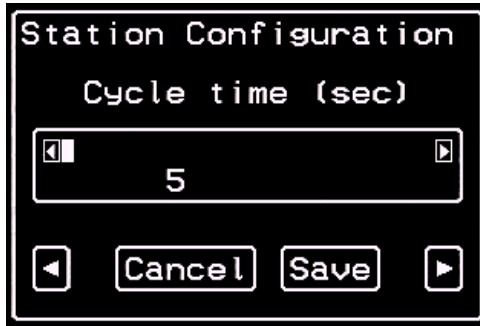
2. Tab to the next button and press <Enter> to configure the **Cycle Time**.

### Cycle Time

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

### 3: KVM/net Configuration

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**.

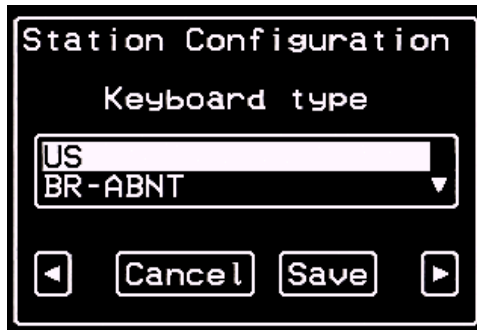
#### **Keyboard Type**

(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/net box. The types of keyboard to choose from are:

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

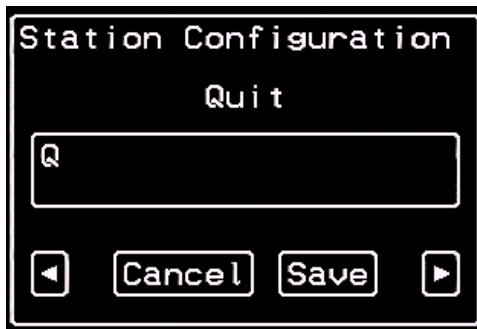




### Quit

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

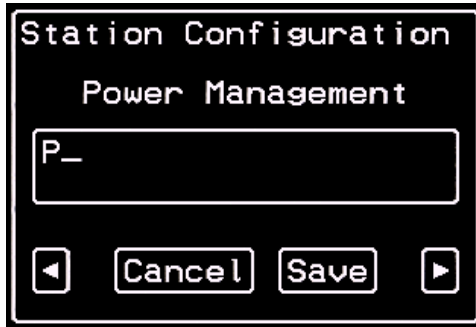
The Quit window allows you to define (or change the default value of) the key sequence for the quit command.



### Power Management

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

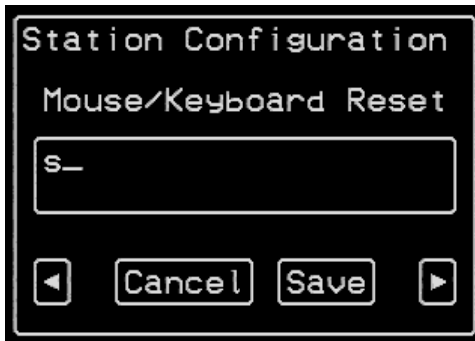
The Power Management screen defines the key sequence for the “Power Management” command. The default key sequence (^KP) displays an OSD menu which allows you to switch ON or OFF the remote server.



### Mouse/Keyboard Sync

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

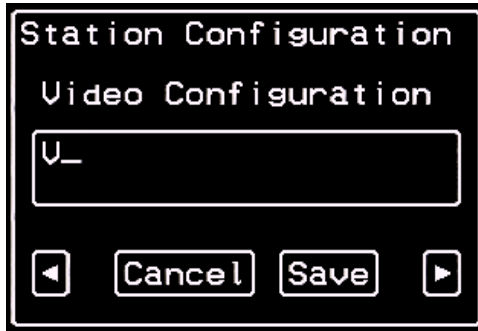
The Mouse/Keyboard Reset defines the key sequence for the mouse and keyboard synchronization command.



### Video Configuration

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

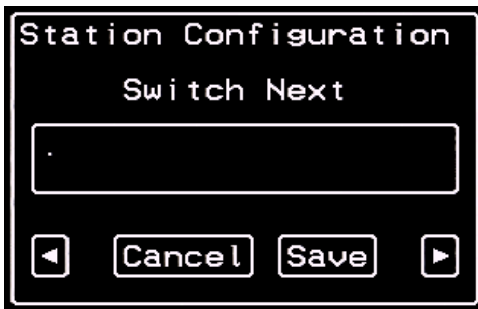
The Video Configuration window defines the key sequence for displaying the video configuration command.



### Switch Next

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

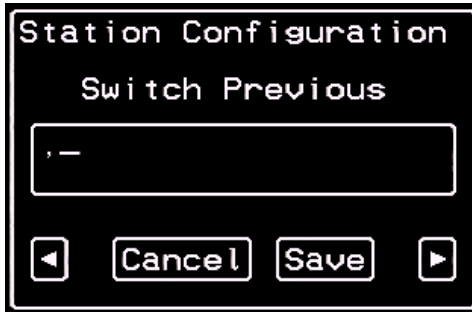
The Switch Next window allows you to define or change the default key sequence for the switch next command. This command allows the user to switch to the next port or server while using the OSD.



### 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)

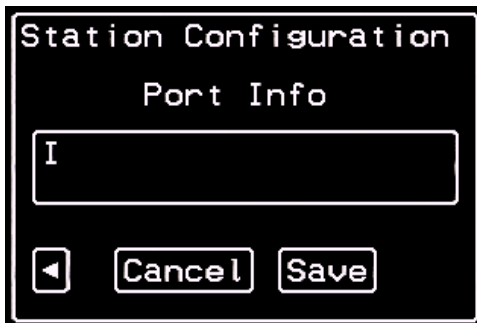
The Switch Previous window allows you to define or change the default key sequence for the switch previous command. This command allows the user to switch to the previous port or server while using the OSD.



### 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

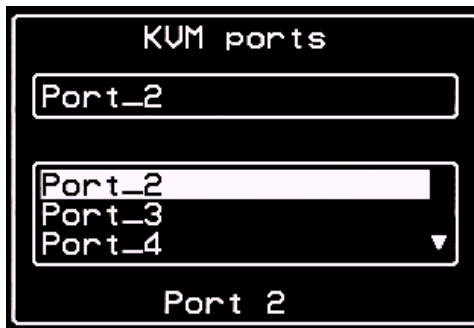
(Configure > KVM Ports)

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.

To select a KVM Port:

1. Go to the KVM Ports window:

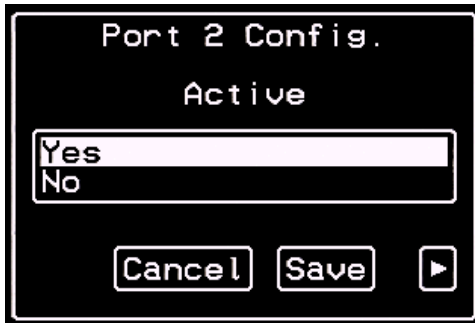


2. From the resulting window, enter or select the port you wish to configure
3. Press <Enter>

NOTE: 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)

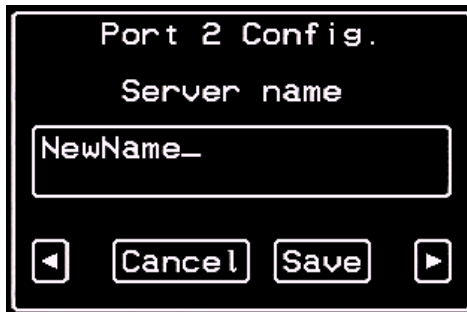


From the **Active** window, select **Yes** or **No** to activate or disable the currently selected port.

Tab to the next button to configure the **Server Name**.

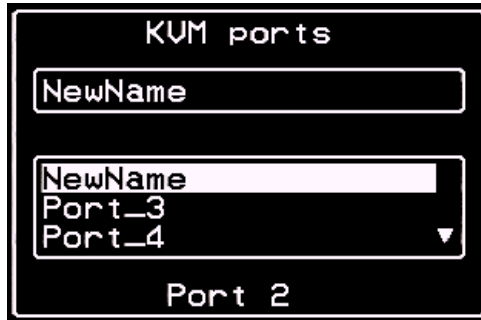
### Server Name

(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 **Server Name**.  
- OR -  
To verify the new server name, tab to the **Save** button and press <Enter>.

The system displays the KVM Ports selection window:

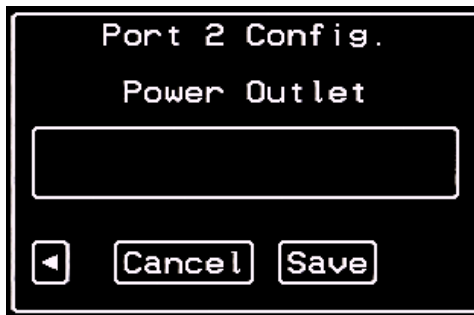


3. Type in the server name in the search box, as necessary.

### 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.

**Notes:** *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 4 - Operating through a Web Browser.

### 3: KVM/net Configuration

2. From the menu to the left of the Configuration screen, select **AUX Port**.  
  
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.

**Note:** *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

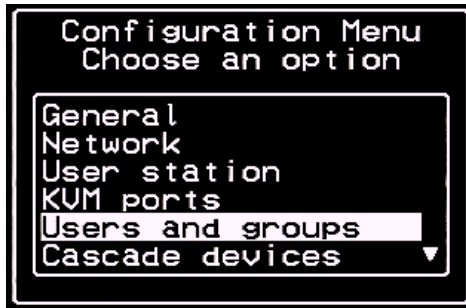
The Users and Groups option of the Configuration Menu allows you to configure the following:

- 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

**Note:** *To understand how the hierarchy of permissions work when creating user permissions between groups and the generic user, refer to “**Hierarchy of Permissions**” on page 4 - 2.*

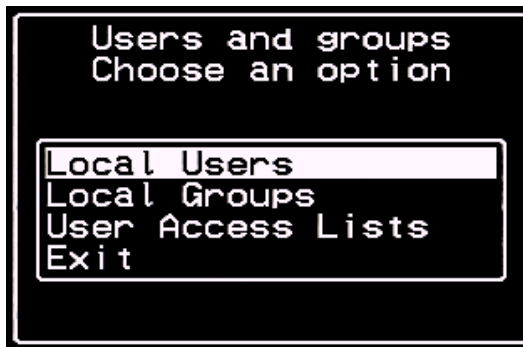
The Users and Groups option of the Configuration Menu:





### 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.

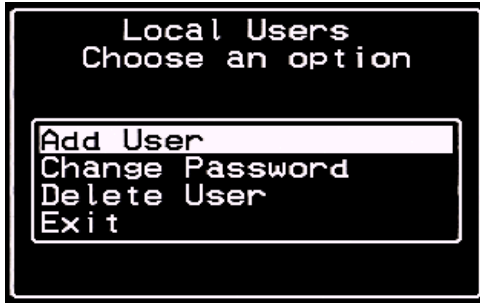
### Adding a User

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

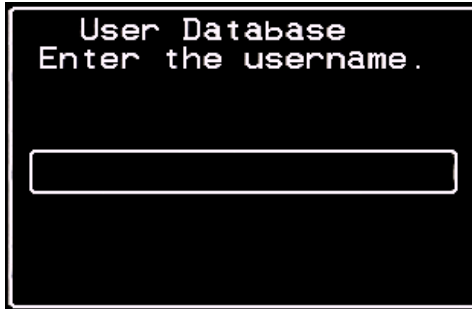
To Add a User follow the steps below:

### 3: KVM/net Configuration

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:



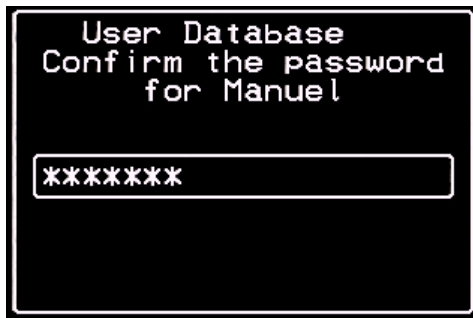
3. Press <Enter> when done.

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



4. From the resulting window, enter 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:



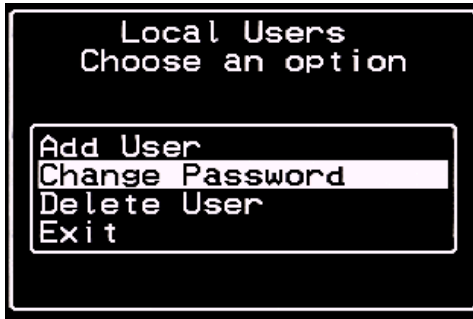
6. Click on **OK** to complete the procedure.

### Changing the User, Admin, or Root Password

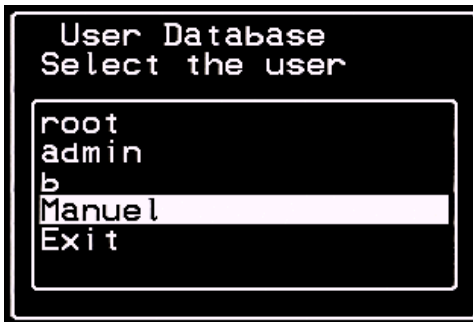
(Configure > Users and Groups > Local Users > Change Password)

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

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

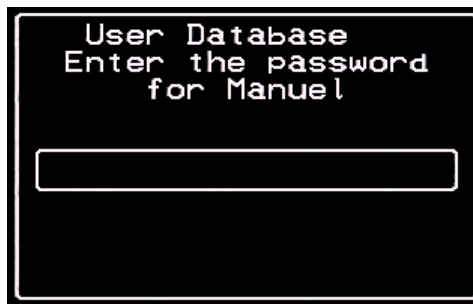


The system displays the **Select the User** window.



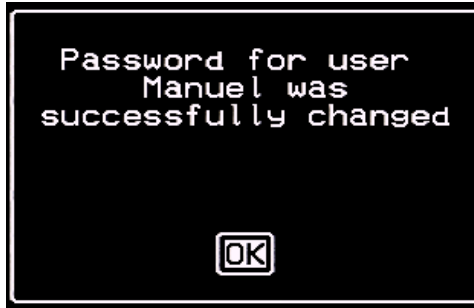
2. From the resulting window, select the user whose password you want to change, and then press <Enter>.

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:



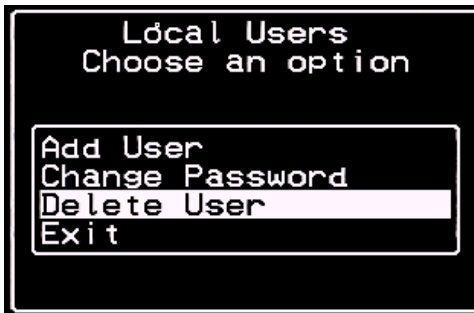
5. Select **OK** to complete the procedure.

### Deleting a User

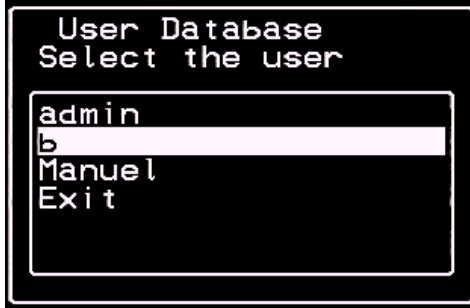
(Configure > Users and Groups > Local Users > Delete User)

To delete a user, follow the steps below:

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



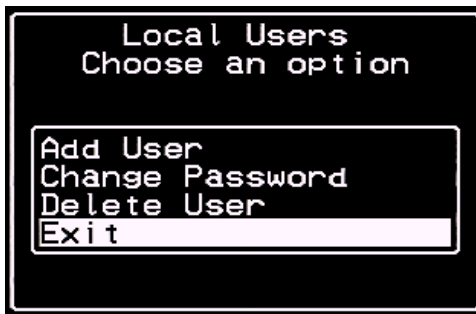
The system displays the **Select the User** window as shown:



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>.

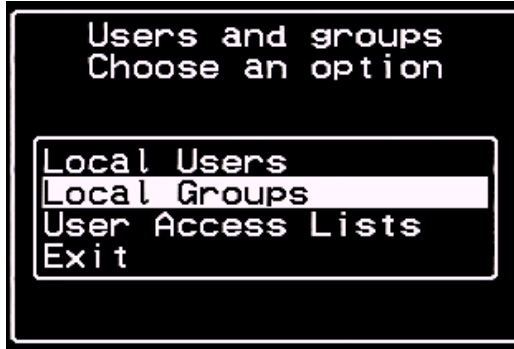


### **Local Groups**

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:

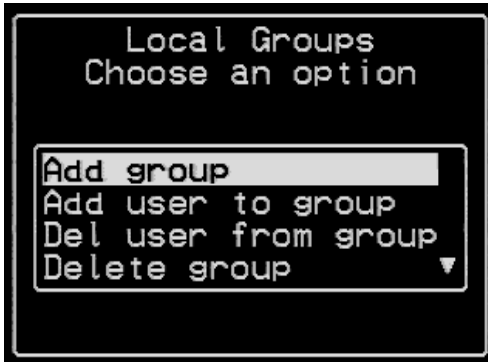


### Adding a Group

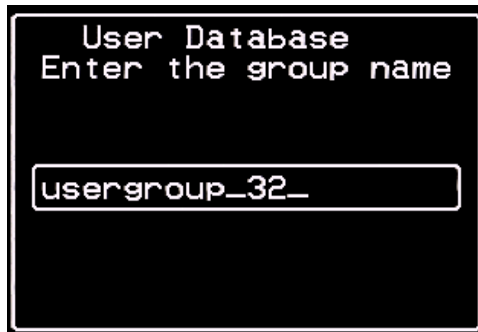
(Configure > User and Groups > Local Groups > Add Group)

To add a user group, follow the steps below:

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



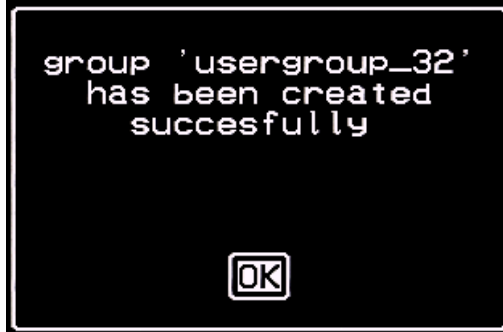
The system displays the Enter the Group Name window as shown:



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.

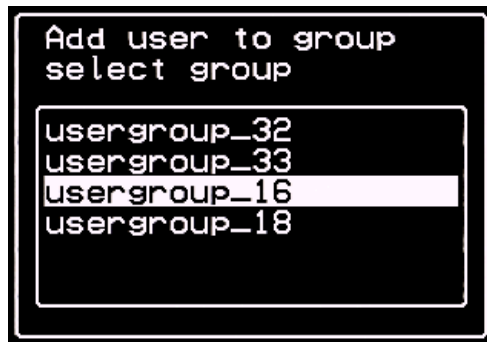
### **Adding a User to a Group**

(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>.

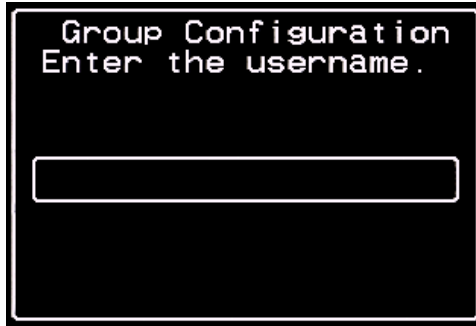
The system displays the Add User to Group - Select Group window as shown:



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

### 3: KVM/net Configuration

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. (To enter multiple users, use a comma to separate each username.)
4. Press <Enter>.

The system displays the following message:



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

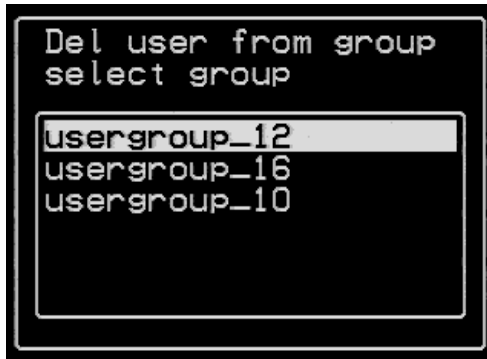
#### **Deleting a User from a Group**

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

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

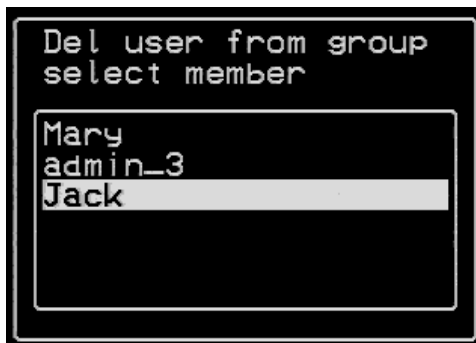
1. From the Local Groups Menu, select **Delete User from Group** and press <Enter>.

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:



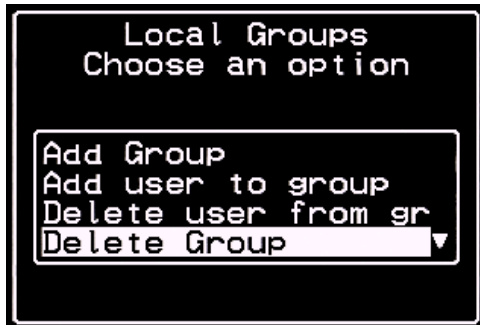
4. Click on **OK** to complete the procedure.

### Deleting a Group

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

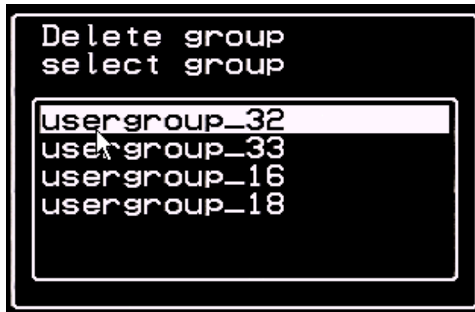
To delete a user group, follow the steps below:

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)

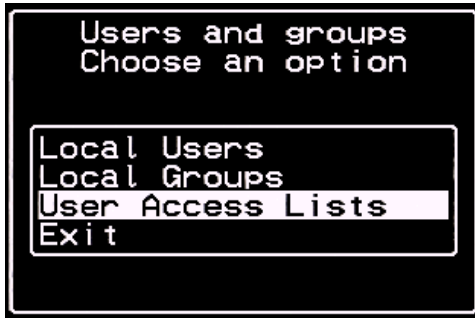
The User Access Lists Menu allows you to add, edit, or delete users from the user access list. The User Access List is a database that defines all KVM users, the ports to which they have access, and the types of permissions that they have.

#### **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.

### 3: KVM/net Configuration

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

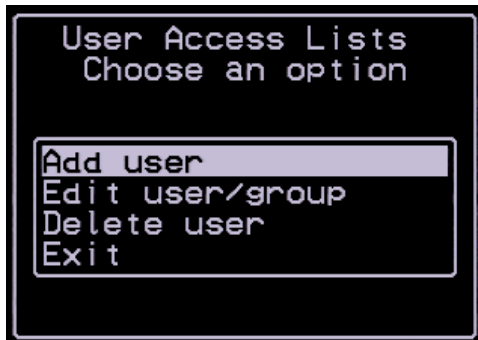


#### Adding a User to the User Access List

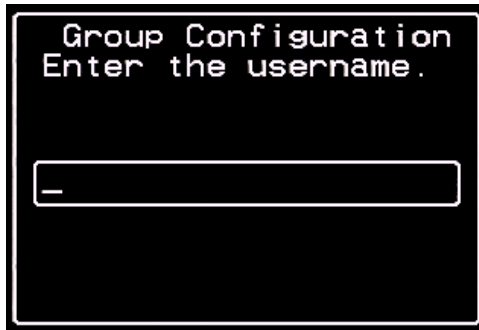
(Configure > Users and Groups > User Access List > Add User)

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>.

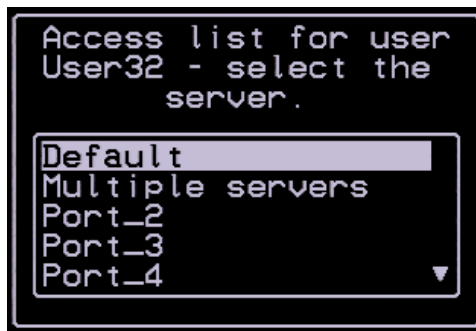


The system displays the **Group Configuration - Enter the Username** window as shown:



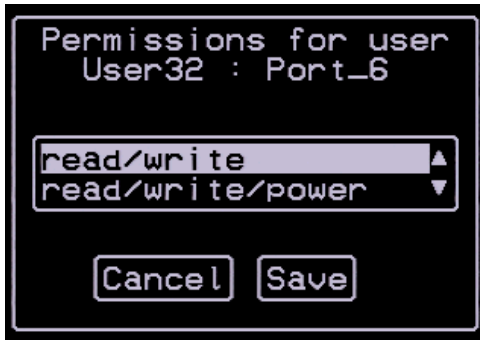
2. Type in the username of the user that you wish to add, and then press <Enter>.

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>.

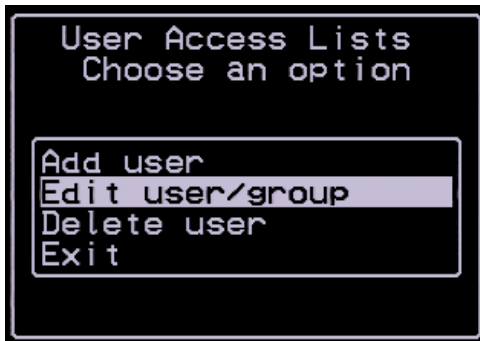
The system displays the Permission for User window as shown:



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)



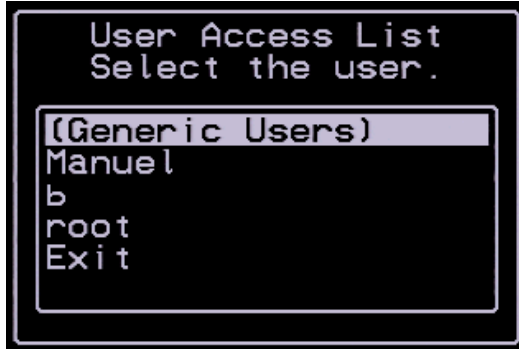
### Editing the Generic User

To edit the generic user, follow the steps below:

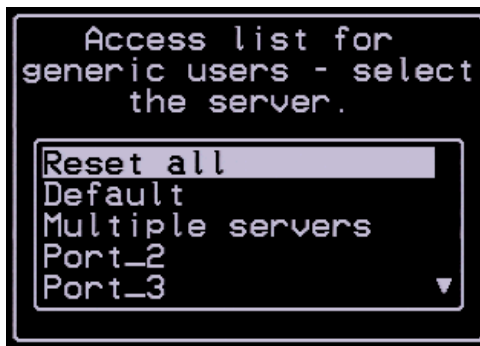
1. From the User Access List - Select the User window, select (**Generic Users**) and press <Enter>.



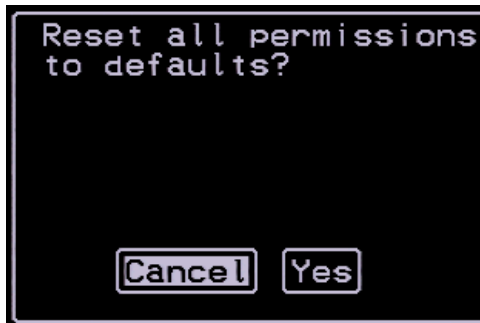
The system displays the **User Access List - Select the User** window:



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:

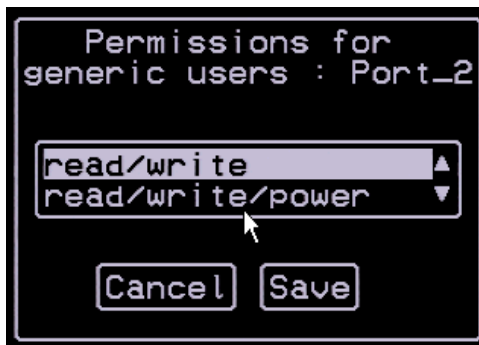


If you select Multiple Servers, the system displays the following window:



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.

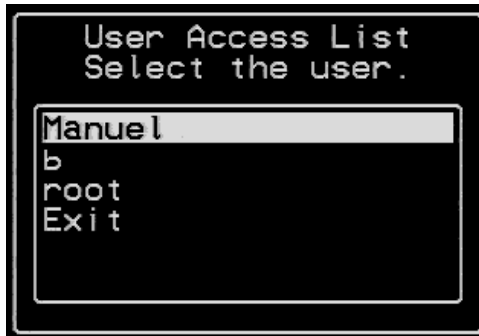
### **Deleting a User from the User Access List**

(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:



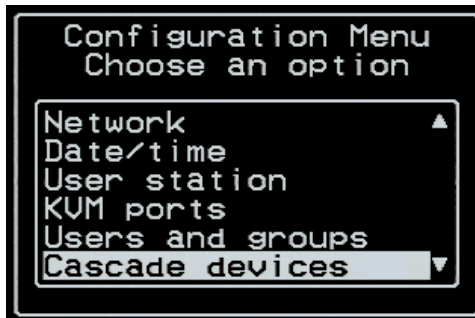
2. From the resulting window, select from the list the user you wish to delete from the User Access List and then press <Enter>.

The system displays a message to confirm your deletion.

## Cascade Devices

(Configure > Cascade Devices)

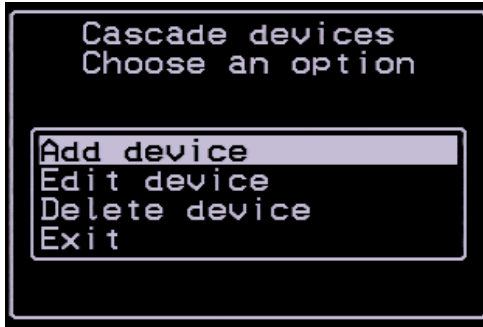
The Cascade Devices option of the Configuration Menu allows you to configure a secondary KVM to be cascaded to the KVM/net switch to increase the number of supportable ports. The secondary device may be another KVM/net switch, a KVM switch or a KVM expander.



### **Cascade Devices Menu**

(Configure > Cascade Devices > Add Device)

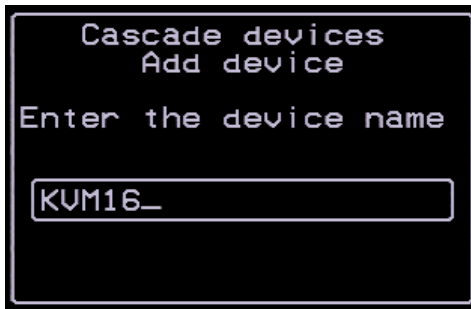
The Cascade Devices Menu provides four options:



### **Adding a Secondary Device**

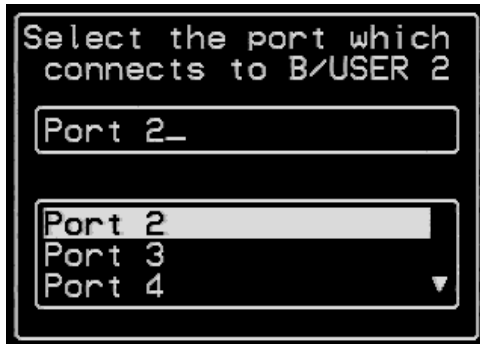
To add a secondary device to be cascaded to the KVM/net switch, follow the steps below:

1. From the Cascade Devices Menu, select Add Device and press <Enter>. The system displays the Add Device - Enter the Device Name window:



2. From the resulting window, select the device type and press <Enter>.

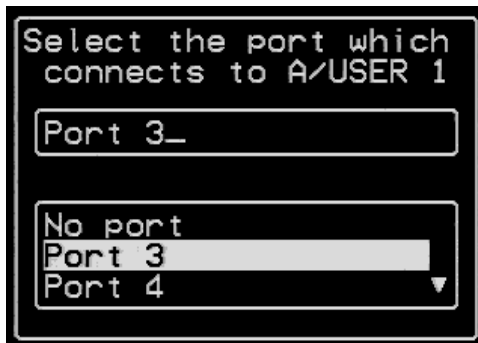
The system displays the Port Selection for USER 2 window:



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

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

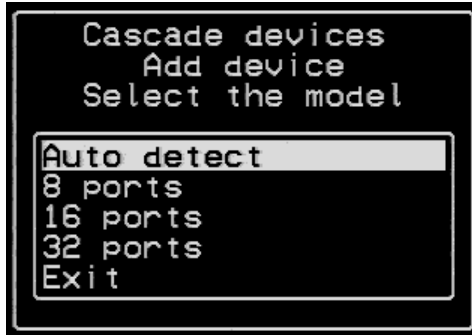
The system displays the Port Selection for USER 1 window:



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

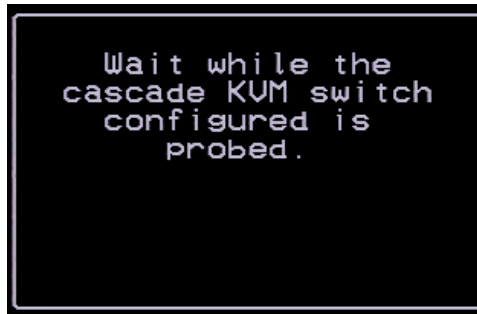
### 3: KVM/net Configuration

The system displays the Device Model Selection window:



5. From the resulting window, select the model or select **Auto Detect** and press <Enter>.

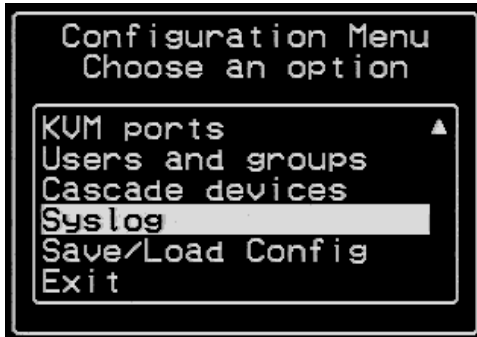
Auto Detect automatically detects and selects the model that is already connected. During auto detection, the system displays the following message:



## Syslog

(Configure > Syslog)

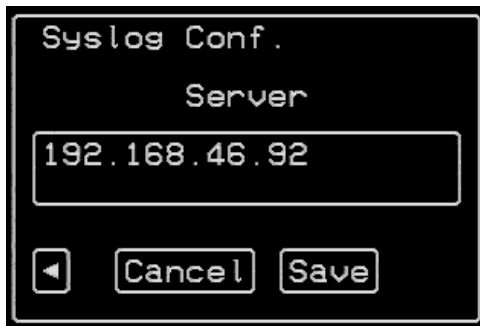
The Syslog option of the Configuration Menu allows you to define the syslog server address.



To configure the Syslog IP address:

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

The system displays the Syslog Sever window:



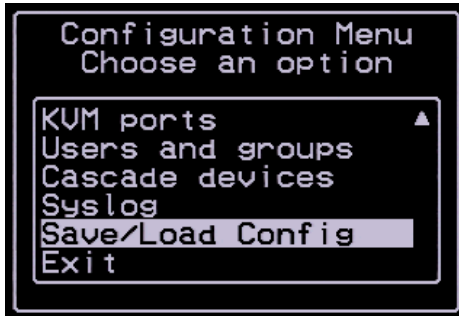
2. From the resulting window, enter the address of the syslog server. Tab to the **Save** button and press <Enter> to complete Syslog configuration.

### Save/Load Config

(Configure > Save/Load Config)

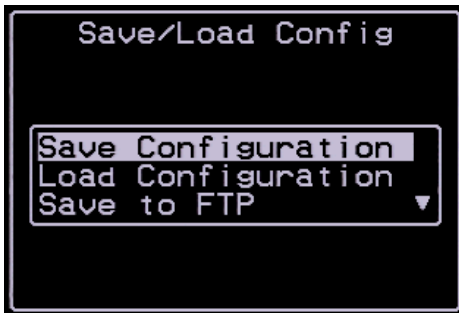
### 3: KVM/net Configuration

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.



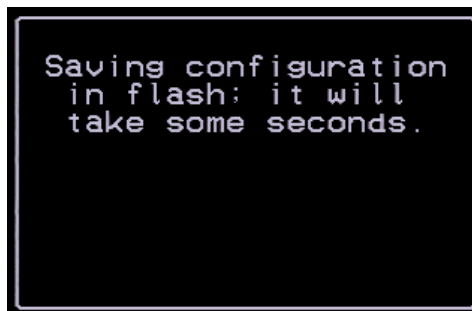
#### **Saving Your Configuration**

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



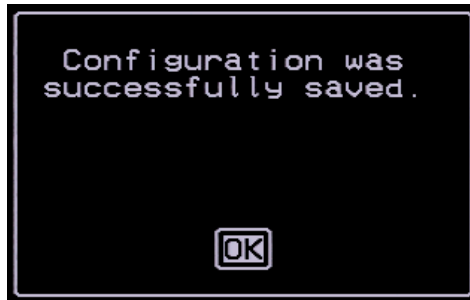
1. From the Save/Load Config window, select Save Config and press <Enter>.

The system displays the following message:





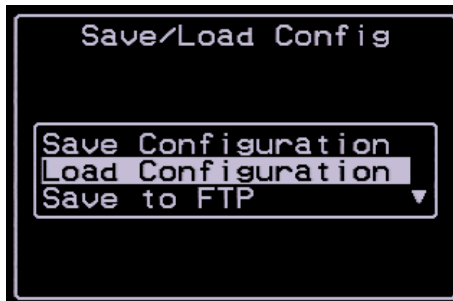
The following message follows:



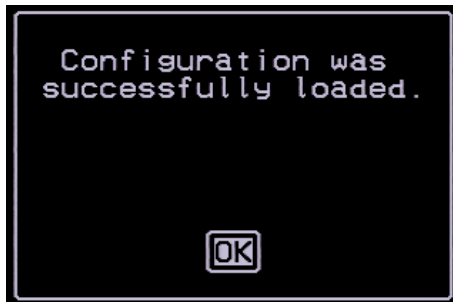
2. Click on **OK** to complete the procedure.

### **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:



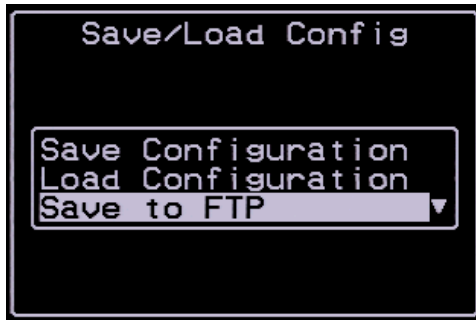
### 3: KVM/net Configuration

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>.

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.

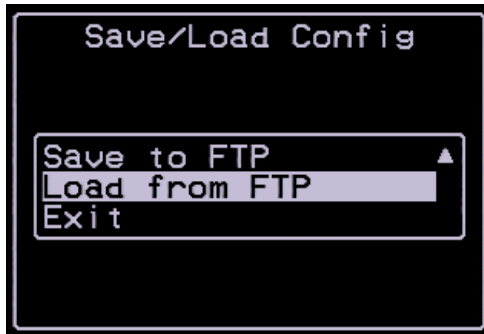
### 3: KVM/net Configuration

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 next button and press <Enter>.

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



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

The system displays the Load from FTP Server - Password.



### 3: KVM/net Configuration

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
- KVM Hardware (FPGAs) and Firmware
- 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: 2.0.7
Alt. Boot: no code
SYS FPGA: 0x43
MUX FPGA: 0x5b

3. Memory
RAM: 128 Mbytes
Flash: 16 Mbytes
RAM usage: 17%
RAMDISK usage: 100%

4. CPU
Clock: 48 MHz

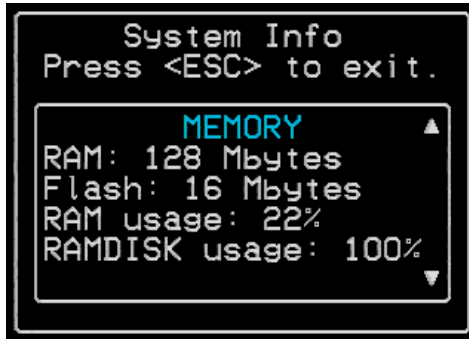
5. Time
Mon Jul 19 2004 12:35:12 PDT
up 10 min

6. User1 connection
Int. uC, V1.0.4

7. User2 connection
RP main, V1.0.4
RP local, V1.0.4
```

### System Info Window

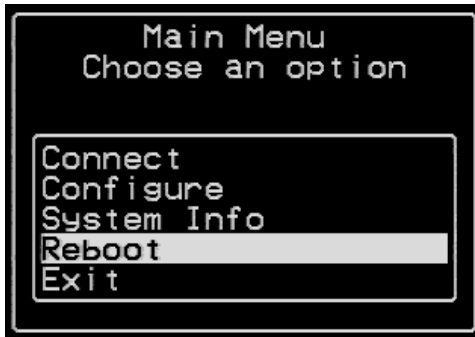
Below is an example of the System Info window. Use the up and down arrow keys of the scroll bar to view the information.



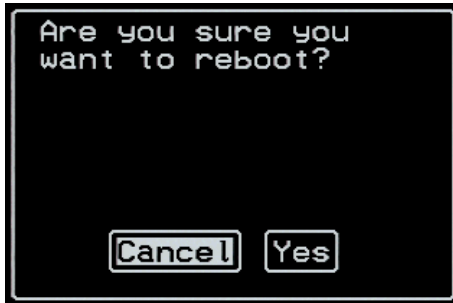


## Reboot

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



The system will display the following message:



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

### *3: KVM/net Configuration*

# Chapter 4

## KVM/net Web Configuration

---

This chapter presents the procedures for configuring the KVM/net using the web interface. It is organized as follows:

- Overview
- Logging In
- KVM/net 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/net and its users, as well as to those users who are granted administrative access to configure and operate the KVM/net.

The KVM/net 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.

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

## 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, <b>passwd</b> , and follow system prompt. Then type in <b>saveconf</b> to save password.           |
| admin            | WMI and OSD                   | root user<br>admin user      | From WMI, go to: Configuration > KVM > Users & Groups.<br>From OSD, go to Configure > Users and Groups > Local Users > Change Password. |
| Regular User     | OSD                           | root user<br>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

**Note: 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/net web interface by typing in the KVM/net server's IP address (e.g., `http://192.168.160.10`) in the browser's address (URL) field.

**Note:** To determine the IP address, log on to the console as root. Then enter the command: **ifconfig**  
For more information about IP addresses, see *About the KVM/net IP Address* on page 2 - 7.

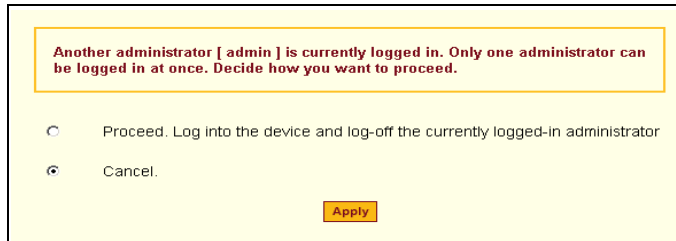
The system brings up the AlterPath KVM/net Login page:



2. Log in as **admin** and type in the password: **cyclades**  
The system brings up the KVM/net web management page.

## 4: Web Configuration

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.

Apply

3. 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  
admin

password  
●●●●●●●●

port  
Port\_16

GO

1. From the port field, enter the port alias or the port number using the following format: **Port\_[number]**  
*Example: Port\_4*
2. Click on GO.  
The system connects you to the port.

## KVM/net Web Management Interface

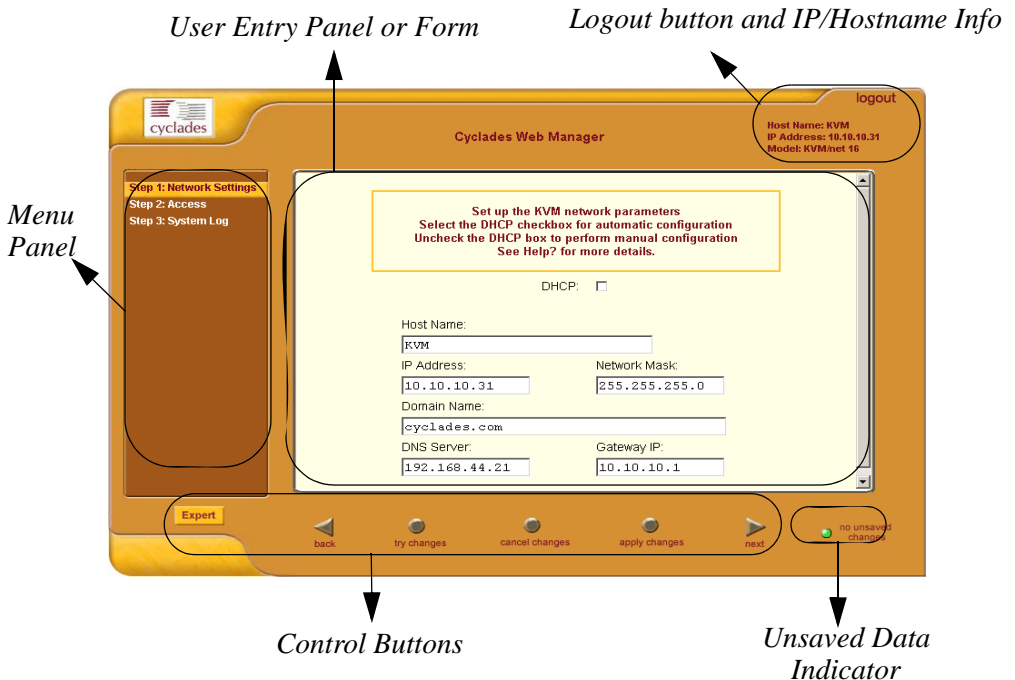
You can use the KVM/net web management interface in two modes:

- 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/net and users in the quickest possible way. When you log on to KVM/net 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.



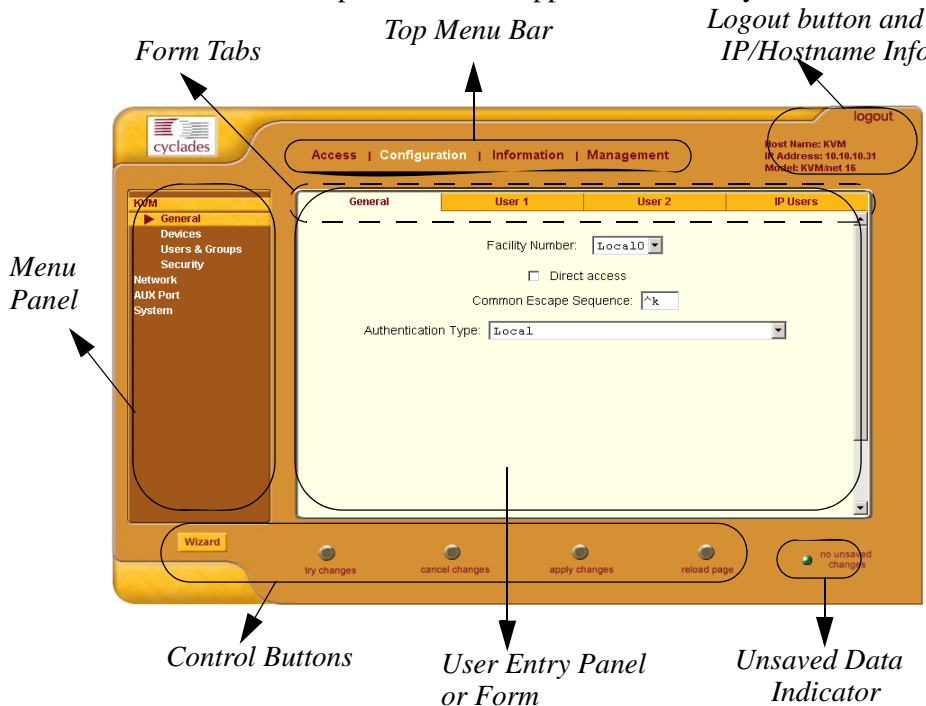
## 4: Web Configuration

Shown in the previous page is a *typical* configuration window of the KVM/net web interface in Wizard Mode. The user entry panel or form varies depending on the selected menu item. The KVM/net 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/net screen in Expert Mode. One main difference between the two modes is that in the Expert Mode you will notice the addition of 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.

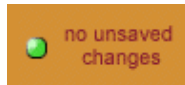
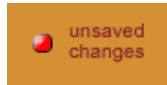
### Button Functions

The control buttons located at the bottom of the KVM/net 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/net 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/net 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/net 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/net for networking. To configure the network settings for the KVM/net, 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. On the left, a sidebar contains three steps: 'Step 1: Network Settings' (highlighted), 'Step 2: Access', and 'Step 3: System Log'. Below the sidebar is an 'Expert' button. The main content area is titled 'Set up the KVM network parameters' and includes instructions: 'Select the DHCP checkbox for automatic configuration', 'Uncheck the DHCP box to perform manual configuration', and 'See Help? for more details.'. Below this is a 'DHCP' checkbox which is currently unchecked. The form contains several input fields: 'Host Name' (containing 'KVM'), 'IP Address' (containing '10.10.10.31'), 'Network Mask' (containing '255.255.255.0'), 'Domain Name' (containing 'cyclades.com'), 'DNS Server' (containing '192.168.44.21'), and 'Gateway IP' (containing '10.10.10.1'). At the bottom, there are navigation buttons: 'back', 'try changes', 'cancel changes', 'apply changes', and 'next'. A status indicator shows 'no unsaved changes'.

3. Type in the network information in the corresponding entry fields, and then select **apply changes**.

**Caution:** *If you change the IP address and then click on **apply changes**, you will need to reconnect to the WMI.*

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 **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**.

The User List box, by default, initially contains two user types that cannot be deleted:

- Admin
- Generic User

The Admin is the super user of the KVM/net web management interface.

The Generic User, by itself, is not a system user. It simply defines the default access permissions for all generic users. Any user that you add from the Access form automatically inherits the configured access permissions of the Generic User.

**Note:** To configure the Generic User, switch to Expert Mode, and go to: **Configuration > KVM > Users and Groups**.

To add a non-generic user, or to change a generic user to a non-generic user (or vice versa), use the Users and Groups form as well.

### 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 <b>Regular User</b> or an <b>Admin</b> .                                                 |
| Shell             | Optional. The default shell the user will get when they ssh or telnet into the KVM/net. Choices are: <b>sh</b> or <b>bash</b> . |
| 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.

**Note:** 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).

## 4: Web Configuration

### To Delete a User

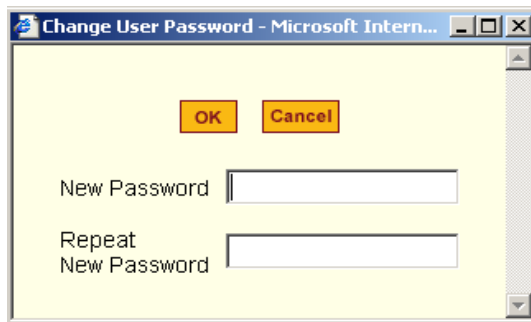
1. From the users list box of the Access form, select the user that you want to delete.
2. Click on the **Delete** button
3. Click on the **apply changes** button.

### To Change a User's Password

**Note:** *It is recommended that you change your admin password as soon as you begin configuring the KVM/net 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

You can send syslog messages to one or more syslog servers that you select. The System Log form is used to add syslog servers to or delete syslog servers from your server list. Select **Step 3: System Log** from the main menu.

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

The system brings up the System Log form:

### To Add a Syslog Server

The Facility Number serves as an identifier for messages generated by the KVM/net relating to the AUX port (*i.e.*, power strips and other such devices connected to this port). This number allows the syslog server to identify and determine how to handle messages generated by the AUX port (*e.g.*, PM events).

**Note:** To assign the Facility Number for messages relating to the KVM ports, use the **General** form (Expert Mode: **Configuration** > **General**).

1. From the **Facility Number** dropdown list, select the facility number.
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.

## 4: Web Configuration

3. Select **apply changes** to save your configuration.

### To Delete a Syslog Server

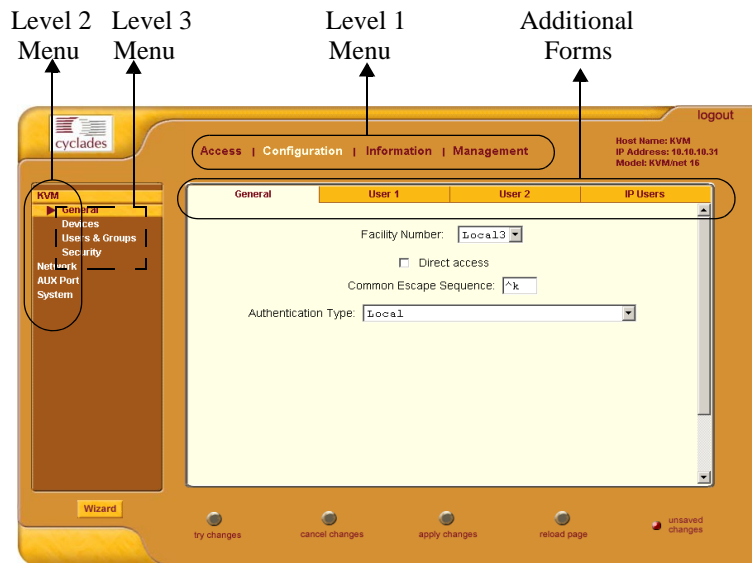
1. From the Syslog Server list box, select the syslog server that you want to delete, and then select **Delete**. (Repeat this step for as many servers you need to delete.)
2. Select **apply changes** to save your configuration.

## Configuring in Expert Mode

This section presents the procedures for configuring the KVM/net web interface in Expert Mode. The Expert Mode adds a top menu bar to support a wider array of menu choices, and allow the admin user to configure the KVM/net beyond the capabilities of the basic wizard mode.

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.

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

## 4: Web Configuration

| <i>Menu Selection</i>         | <i>Form Name</i>                 |
|-------------------------------|----------------------------------|
| > <b>General</b>              | <b>This is a form by itself.</b> |
| > <b>Port Status</b>          | <b>This is a form by itself.</b> |
| <b>Management</b>             |                                  |
| > <b>Backup Configuration</b> | <b>This is a form by itself.</b> |
| > <b>Firmware Upgrade</b>     | <i>This is a form by itself.</i> |
| > <b>Microcode Upgrade</b>    | <i>This is a form by itself.</i> |
| > <b>Microcode Reset</b>      | <i>This is a form by itself.</i> |
| > <b>Active Sessions</b>      | <i>This is a form by itself.</i> |
| > <b>Reboot</b>               | <i>This is a form by itself.</i> |

**Note:** 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.

### Connect to Server

The first selection, **Connect to Server**, is designed for the KVM/net regular user and is discussed in more detail in **Chapter 5 KVM/net Operation**.

| <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 IPDU's 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/net 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 cause the AlterPath PM to sound an alarm or send a notification message. |
| Software Upgrade      | Upgrade Software on the AlterPath PM IPDU.                                                                                                                                                                                                     |

### 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:

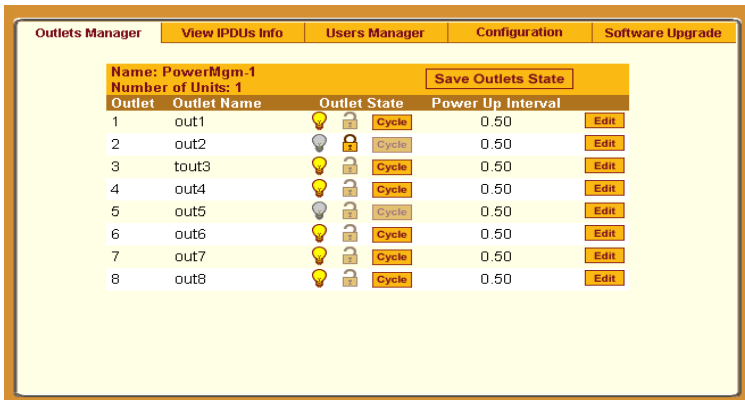
## 4: Web Configuration



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

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 2 has been switched off and locked.



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 the maximum current and the maximum temperature attained by the IPDU.

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:

| Serial Port 4: General Information                                                                                      |                         |                              |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------|
| <input type="button" value="Clear Max Detected Current"/> <input type="button" value="Clear Max Detected Temperature"/> |                         |                              |
| 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

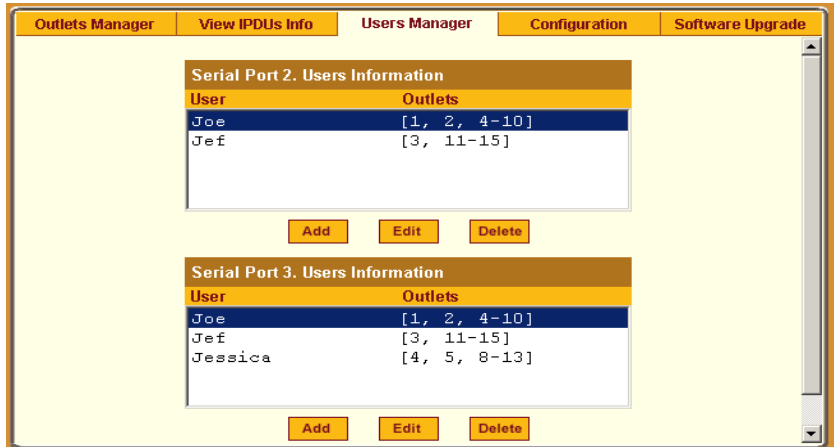
The Users Management form of Power Management allows you to assign users to selected outlets for each KVM port and vice versa.

## 4: Web Configuration

### 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:

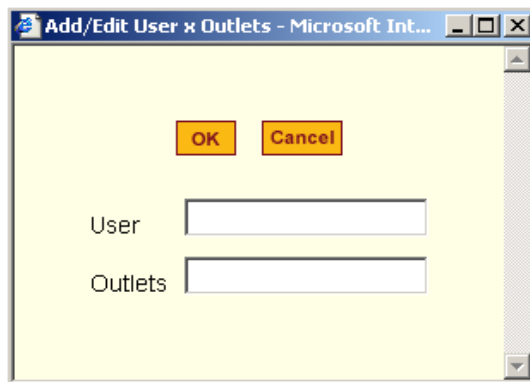


2. To edit an assigned user, select the user you wish to edit from the Serial Port view table and then select the **Edit** button that corresponds to the table.

- 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 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.

**Caution:** *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).*

**Caution:** *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.

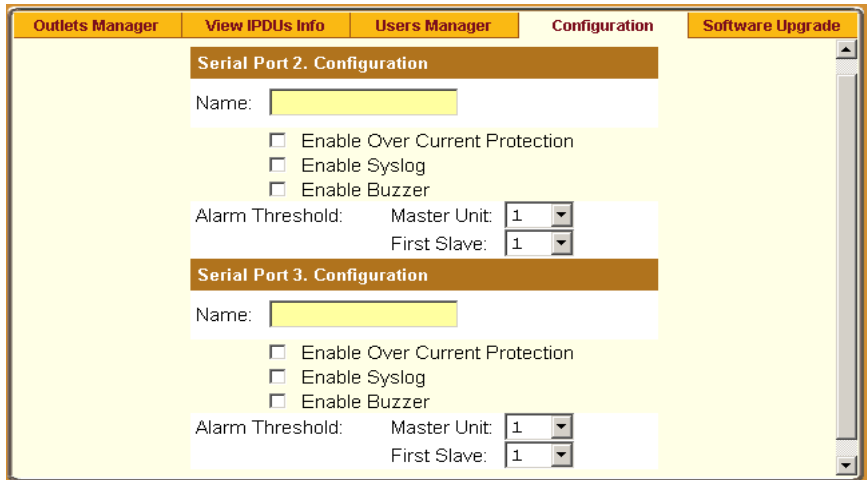
## ***Power Management > Configuration***

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:

## 4: Web Configuration



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:" text input field, three checkboxes for "Enable Over Current Protection", "Enable Syslog", and "Enable Buzzer", and two "Alarm Threshold:" fields: "Master Unit:" with a dropdown menu set to "1" and "First Slave:" with a dropdown menu 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**

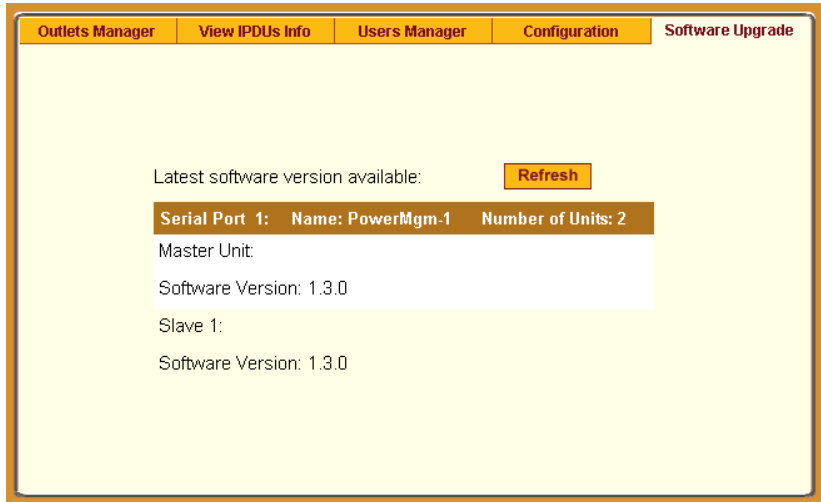
The **Software Upgrade** form of Power Management allows you to upgrade the Power Management software for a selected serial port. The first line of the form shows the **latest software version available**. The presence of an **Upgrade** button indicates that a new software version for that master or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





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.

**Note:** *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

## 4: Web Configuration

### **KVM**

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

| <i>Form Name</i> | <i>Use this form to:</i>                                                                                                                     |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| General          | Define the Facility Number ( <i>i.e.</i> , the message identifier for events relating to KVM ports), 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/net 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/net 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/net Main Menu.                                                                                                                                                                                                           |
| <Ctrl-K> and then <P>   | Port command - initiates a power control session.                                                                                                                                                                                                                                                  |
| <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      | <b>Video command - controls screen brightness and contrast.</b>                                                                                                                                                                                                                                    |
| Ctrl-K, and then S      | Keyboard and Mouse Reset command - resets the keyboard and mouse if either one stops responding after adding a new server to the KVM/net.<br><br><i>Note: Use with caution. This can cause some servers to lock up. On a Linux server command line, try using the command:<br/><b>xset m 0</b></i> |

1. To configure the KVM/net 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:

## 4: Web Configuration



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

| <i>Field Name</i>      | <i>Definition</i>                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Facility Number        | The Facility Number serves as an identifier for messages generated by the KVM/net relating to the KVM ports. It allows the syslog server to identify messages coming from the KVM ports and determine how to handle this specific group of messages.<br><br><i>Note: To assign the Facility Number for messages relating to the AUX port, you must use the <b>Step 3: Syslog form (Wizard Mode)</b>.</i> |
| 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.                                                                                                                                                                                                                                                                                                        |

- Click on apply changes to save your configuration.

- 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:

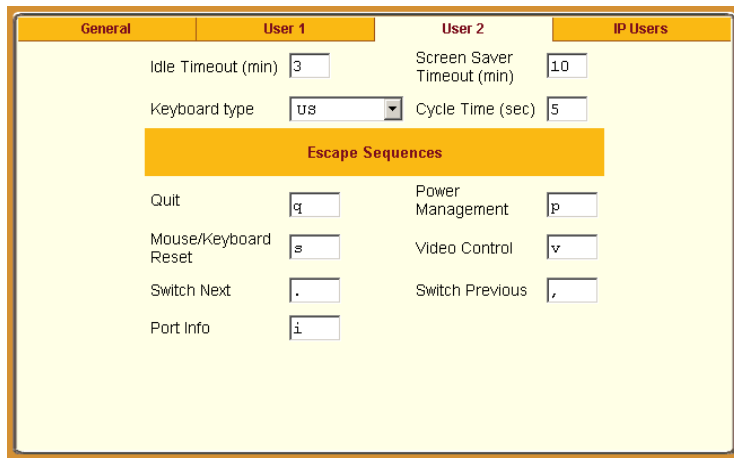
| <i>Field Name</i>    | <i>Definition</i>                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------|
| Idle Timeout         | The time (in minutes) it takes the system to timeout after it remains idle (0 disables Idle Timeout).                    |
| Screen Save Timeout  | The time (in minutes) it takes for the screen saver to activate after the system remains idle (0 disables Screen Saver). |
| 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 Reset | Key sequence for resetting the mouse and keyboard.                                                                       |
| Video Control        | Key sequence for video control.                                                                                          |
| Switch Next          | Key sequence for switching to the next screen.                                                                           |

#### 4: Web Configuration

| <i>Field Name</i> | <i>Definition</i>                                      |
|-------------------|--------------------------------------------------------|
| Switch Previous   | Key sequence for switching to the previous screen.     |
| Port Info         | Key sequence for invoking the Port Information screen. |

6. 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:



| General                 | User 1                                              | User 2                                                     | IP Users |
|-------------------------|-----------------------------------------------------|------------------------------------------------------------|----------|
|                         | Idle Timeout (min) <input type="text" value="3"/>   | Screen Saver Timeout (min) <input type="text" value="10"/> |          |
|                         | Keyboard type <input type="text" value="US"/>       | Cycle Time (sec) <input type="text" value="5"/>            |          |
| <b>Escape Sequences</b> |                                                     |                                                            |          |
|                         | Quit <input type="text" value="q"/>                 | Power Management <input type="text" value="p"/>            |          |
|                         | Mouse/Keyboard Reset <input type="text" value="e"/> | Video Control <input type="text" value="v"/>               |          |
|                         | Switch Next <input type="text" value="."/>          | Switch Previous <input type="text" value=","/>             |          |
|                         | Port Info <input type="text" value="i"/>            |                                                            |          |

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 page. At the top, there are four tabs: 'General', 'User 1', 'User 2', and 'IP Users'. The 'IP Users' tab is selected. Below the tabs, there is a form with the following elements:

- 'Idle Timeout (min)' field with the value '3'.
- 'TCP Viewer Ports' field with the value '5900+'.
- A section titled 'Escape Sequences' containing several rows of controls:
  - 'Quit' with a text box containing 'q'.
  - 'Power Management' with a text box containing 'p'.
  - 'Mouse/Keyboard Reset' with a text box containing 's'.
  - 'Video Control' with a text box containing 'v'.
  - 'Switch Next' with a text box containing '.'.
  - 'Switch Previous' with a text box containing ','.
  - 'Port Info' with a text box containing 'i'.

The **IP Users** form is used to configure the 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 Port Address**

By default, if no addresses are specified, the KVM/net automatically looks for the first available port addresses starting at 5900. If 5900 is not available, the KVM increments the port address until it finds one that it can assign. When an additional port is added, the system automatically assigns the next available port address. To override this default, you can assign your own port address to the KVM/net through the web management interface (**TCP Viewer Ports** field of the **IP Users** tabbed form), or the OSD.

**Caution:** *Do not use TCP ports 1 through 1024 as these ports are privileged ports for system and server software. Using any of these ports to assign your own port address can cause a connection failure.*

To configure the TCP viewer port address from the OSD, follow the procedure below:

1. Log onto the OSD as admin
2. Assign the available TCP port address of your choice using any of the following methods:

## 4: Web Configuration

Use the plus sign (+) to assign a TCP port address range from which to start incrementing (e.g., 5903+).

Use the hyphen (-) to indicate a range of addresses (e.g., 5903-5904)

Use the comma (,) to separate two TCP port addresses. (e.g., 5901,5905)

Combine punctuation, as necessary (e.g., 1901,5903+).

3. 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/net web management interface.
2. Access an output port on the KVM/net.
3. From a console window (or from a telnet or ssh session), log on as root.
4. Enter the command: **ps**

You will see a session near the bottom of the screen labeled: **monitor 1**. There will be some information indicating the user name, the port number and finally, TCP port address. If a second port has been accessed through the WMI, there will be a **monitor 2** session displayed, and it will be followed by similar information including the second TCP port address.

### Devices

The **Devices** form allows you to configure one or more secondary KVM units to a primary KVM/net unit, a process also known as *cascading* or *daisy-chaining*. See page **2 - 10** for examples of cascaded configurations.

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/net for as many allowable tiers or hierarchies. For example, a 2-tier, cascaded configuration can have secondary KVM units connected to a primary KVM/net. The diagram below shows a basic cascaded configuration of a primary KVM/net 32 with all KVM components.

Using the KVM/net 32, 32 primary KVM/net 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/net:**

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

**Note:** In the KVM Expander, **User A** and **User B** are interchangeable.

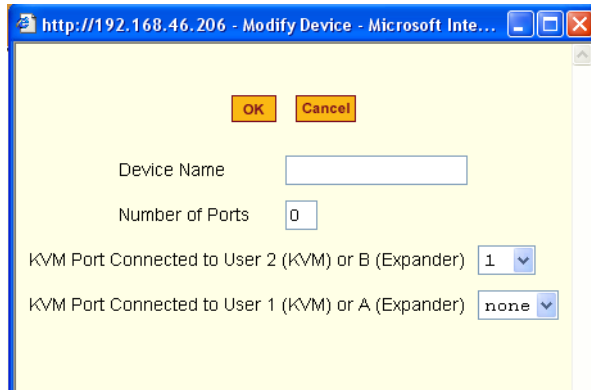
1. From the top menu, select **Configuration**; form the side menu, select **Devices**.

The system brings up the **Devices** configuration form:



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

## 4: Web Configuration



3. 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.                                                                   |
| KVM Port Connected to User 2 | The secondary KVM port to be connected to the User 2 port of the primary KVM/net (or either port A or B of the Expander). |
| Port Connected to User 1     | The secondary KVM port to be connected to the User 1 port of the primary KVM/net (or either port A or B of the Expander). |

4. Select the **OK** button when done.
5. From the configuration window, select **apply changes** to save your configuration.

**Caution:** *You must connect to **USER 2** of the secondary KVM switch to the port to be used for cascading from the primary KVM/net. In a 2-user arrangement, in addition to connecting to **USER 2** of the cascaded KVM switch, use a PS/2 Terminator to connect from a port on the primary KVM/net switch to **USER 1** (local) of the secondary KVM switch.*

### To edit a device configuration:

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

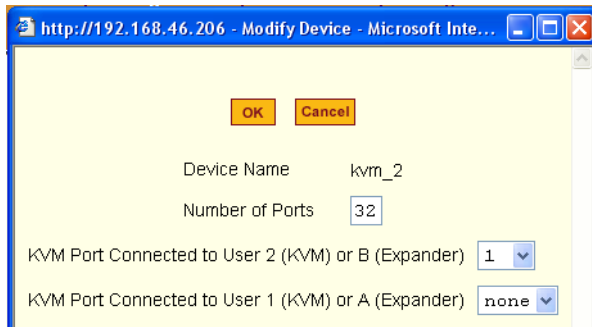
The system brings up the **Devices** configuration form.

- 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 Device** dialog box which is similar to the dialog box used for adding a port.

- From the dialog box, modify the configuration as necessary (see field definition table from the preceding procedure), and then select the **OK** button.



- 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

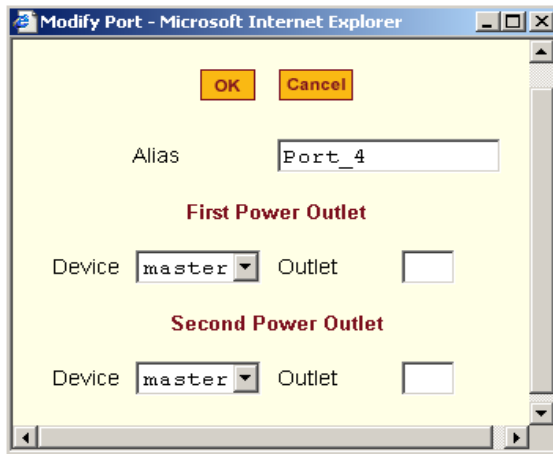
The Ports dialog box is used to modify the power outlet assignments for each port connected to the KVM/net, as well as to enable/disable the ports.

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

The system brings up a list of ports that are available for the (master or cascaded) device selected.



2. Select the port you wish to modify and click the **Modify** button. The system will bring up the Modify Port Dialog box:



3. Enter the Device and Outlet information, as necessary, and then select the **OK** button.
4. 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. Then click the **Ports** button.
2. From the resulting list of ports, select the port to be enabled/disabled, and then select the **Enable** or **Disable** button.

You can repeat this step to enable or disable any additional ports.



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 the default permissions of the Generic User.

**Note:** *The Generic User allows you to set the default permissions for regular users.*

- Set specific KVM/net permissions for a non-generic user.
- Assign or change user passwords.
- Add or delete users from the User Access List.
- Set specific KVM/net permissions by group.

- Add or delete user groups from the Group Access List.

**To set KVM/net 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/net permissions.  
- OR -  
From the **Group List** box, select the group to be configured for KVM/net permissions.
3. Select the corresponding **Set KVM Permissions** button.  
The system displays the Set KVM Permissions form:

## 4: Web Configuration

The screenshot shows a web configuration window titled "KVM Access List for user a". At the top, there is a checkbox labeled "Default Access List" which is currently unchecked. Below it, the "Default Permission" is set to "Full access" in a dropdown menu. A table with two columns, "Device" and "Permissions", is displayed. The table contains one row with "master" in the "Device" column and "-" in the "Permissions" column. At the bottom of the window, there are three buttons: "OK", "Cancel", and "Set permissions for the device". A mouse cursor is pointing at the "Set permissions for the device" button.

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 (this keeps the user as a Generic User). De-selecting the checkbox allows you to re-define the KVM permissions for the current user (and convert the user into a non-generic user). |
| 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**.

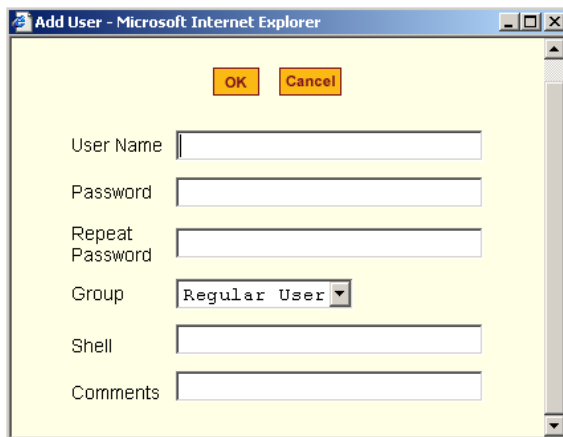


2. To delete a user, select the user to be deleted from the **User List** box  
- OR -  
To delete a group, select the group name to be deleted from the **Group List** box.
3. Select the corresponding **Delete** button.
4. Verify your deletion by checking the list box.
5. Select **apply changes** to save your configuration change.

**To add a user/group to the Access list (to access KVM/net 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:



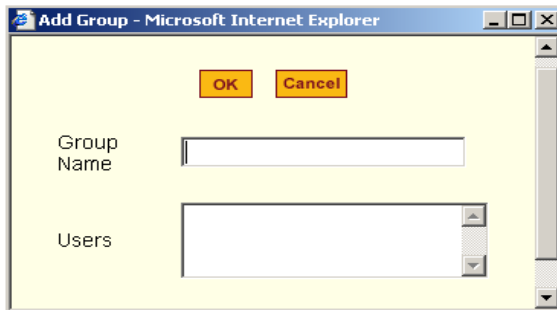
The screenshot shows a web browser window titled "Add User - Microsoft Internet Explorer". The main content area is a yellow dialog box with the following elements:

- 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.

## 4: Web Configuration

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.
3. The system brings up the Change User Password.
4. From the dialog box, type in the new password twice, and then select the **OK** button.
5. From the configuration window, select the **apply changes** button to save your configuration.

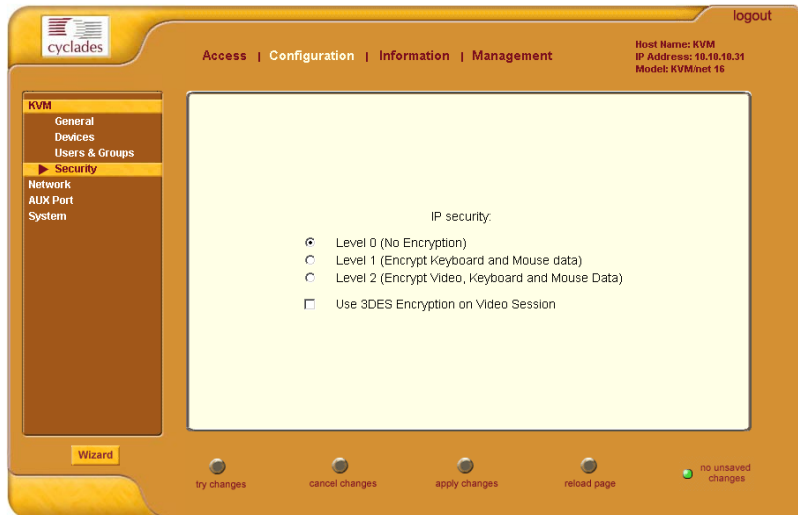
## Security

The IP security feature enables data encryption whenever the KVM/net is accessed through a KVM over IP connection (e.g., whenever a KVM viewer is launched by the WMI). Since the KVM/net can be used over an Ethernet connection and accessed over the internet, you should seriously consider enabling this feature.

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.

**Note:** 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/net 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/net.

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

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

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.

## 4: Web Configuration

The system should add the following fields to your form:

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:

3. 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. |
| Ethernet Port          |                                                                                                                                                          |
| Primary IP             | The 32-bit numeric IP address of the KVM/net 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/net unit on the Internet.                                                                            |
| Secondary Network Mask | The network mask of the secondary IP.                                                                                                                    |
| MTU                    | Maximum Transmission Unit used by the TCP protocol.                                                                                                      |

## 4: Web Configuration

| <i>Field Name</i>    | <i>Definition</i>                                           |
|----------------------|-------------------------------------------------------------|
| DNS Service          |                                                             |
| 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.                  |

4. 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/net-generated syslog messages. The KVM/net 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   | The Facility Number serves as an identifier for messages generated by the KVM/net relating to the AUX port ( <i>i.e.</i> , power strips and other such devices connected to this port). It allows the syslog server to identify and determine how to handle messages generated by events relating to the AUX port ( <i>e.g.</i> , PM events). |
| New Syslog Server | Name of the Syslog Server that you wish to add.                                                                                                                                                                                                                                                                                               |
| Syslog Servers    | List of all Syslog Servers connected to the KVM/net.                                                                                                                                                                                                                                                                                          |

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.

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

The system invokes the Services form.



- Select the service(s) you would use to access devices.
- Select **apply changes** when done.

### **Network > IP Filtering**

**Note:** *If you already understand how IP filtering works, skip this section and proceed to “IP Filtering: To add a chain:” on page 49*

---

*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**.

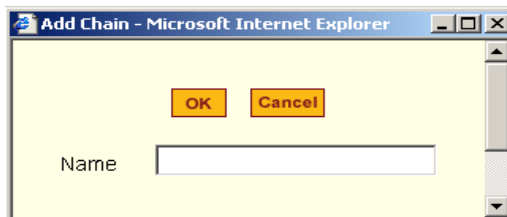
The system brings up the IP Filtering configuration form:



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.)

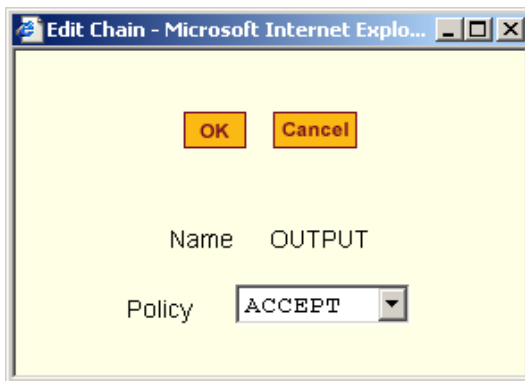
## 4: Web Configuration

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:

**Edit Rules for Chain [INPUT]**

| Packets | Bytes | Target | Source   | Destination | Proto |
|---------|-------|--------|----------|-------------|-------|
| 0       | 0     | DROF   | anywhere | anywhere    | Icmj  |
| 0       | 0     | DROF   | anywhere | anywhere    | Icmj  |

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.

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

## 4: Web Configuration

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

Target  
DROP

Source IP 0.0.0.0 Mask 0.0.0.0  Inverted  
Destination IP 0.0.0.0 Mask 0.0.0.0  Inverted  
Protocol ICMP  Inverted  
Input Interface  Inverted  
Output Interface  Inverted  
Fragments All packets

**ICMP Options Section**  
ICMP Type  
timestamp-request  Inverted

- 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"> <li>- All Packets.</li> <li>- 2nd, 3rd... fragmented packets.</li> <li>- Non-fragmented and 1st fragmented packets.</li> </ul> |

## 4: Web Configuration

| <i>Field Name</i> | <i>Definition</i>                                                                           |
|-------------------|---------------------------------------------------------------------------------------------|
| ICMP Type         | This dropdown list box contains all the ICMP types that may be applied to the current rule. |
| Inverted          | This ICMP option will be applied to all rules except the currently selected rule.           |

### 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. <b>Using tcp flags and appropriate reject type, the packets are matched with the REJECT target.</b> |



| <i>Field Name</i>      | <i>Definition</i>                |
|------------------------|----------------------------------|
| Choices are:           |                                  |
| icmp-net-unreachable   | ICMP network unreachable alias.  |
| icmp-host-unreachable  | ICMP host unreachable alias.     |
| icmp-port-unreachable  | ICMP port unreachable alias.     |
| icmp-proto-unreachable | ICMP protocol unreachable alias. |
| icmp-net-prohibited    | ICMP network prohibited alias.   |
| icmp-host-prohibited   | ICMP host prohibited alias.      |
| echo-reply             | Echo reply alias.                |
| tcp-reset              | TCP RST packet alias.            |

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 > IPsec VPN**

The IP security VPN configuration form allows you to configure one or more VPN connections to other systems or KVM/net 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.

**Note:** *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/net 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/net and the gateway. The gateway machine and the KVM/net 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/net 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/net), or between the KVM/net and the KVM/net 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 leftnexthop (the router which KVM/net sends packets to in order to get them delivered to right). Similarly, you may need to specify rightnexthop (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/net, the IPsec is used to connect the KVM/net 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/net 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

**Caution:** *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:



## 4: Web Configuration

2. To edit a VPN connection, select the VPN connection that you wish to edit from the form, and then select the **Edit** button.

- OR -

To add a VPN Connection, select the **Add** button.

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

The image displays two screenshots of the 'New/Modify Connection' dialog box, which is a web form running in Microsoft Internet Explorer. Both screenshots show the same form structure but with different authentication methods selected.

**Left Screenshot (RSA Public Keys):**

- Buttons: OK, Cancel
- Connection Name:
- Authentication Protocol: ESP
- Authentication Method: RSA Public Keys
- Remote ("Right") section:
  - ID:
  - IP Address:
  - NextHop:
  - Subnet:
  - RSA Key:
- Local ("Left") section:
  - ID:
  - IP Address:
  - NextHop:
  - Subnet:
  - RSA Key:
- Boot Action: Ignore

**Right Screenshot (Shared Secret):**

- Buttons: OK, Cancel
- Connection Name:
- Authentication Protocol: ESP
- Authentication Method: Shared Secret
- Remote ("Right") section:
  - ID:
  - IP Address:
  - NextHop:
  - Subnet:
- Local ("Left") section:
  - ID:
  - IP Address:
  - NextHop:
  - Subnet:
- Boot Action: Ignore
- Pre Shared Secret:

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.

3. 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.                                   |
| 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/net 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/net 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.

**Caution:** *Check the SNMP configuration before gathering information about KVM/net 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/net 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:

The screenshot shows the 'SNMP Daemon Settings' form in the Cyclades web interface. The form includes a message box stating: 'To activate the snmpd services, you should go to the Network Services section.' Below this, the 'System Information Settings' section contains two input fields: 'SysContact' with the value 'cyclades\_Corporation' and 'SysLocation' with the value 'AlterPath\_KVM'. The 'Access Control' section is currently empty. The 'SNMPv1/SNMPv2 Configuration' section features a table with the following columns: 'Community', 'Source', 'OID', and 'Permissi'. The table is currently empty. At the bottom of the form, there are five buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'no unsaved changes'.

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).                                                                                                                                                            |

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


#### 4: Web Configuration

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:

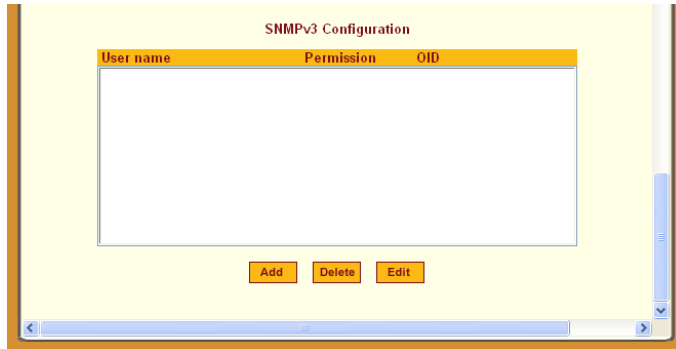


4. Complete the dialog box as follows:

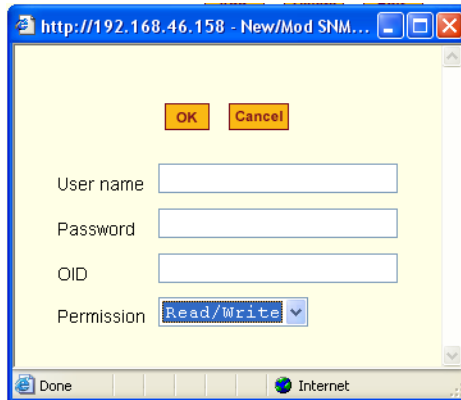
| <i>Field Name</i> | <i>Definition</i>                                                                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.        |
| Source            | The source IP address or range of IP address.                                                                                                                                                                           |
| OID               | Object Identifier.                                                                                                                                                                                                      |
| Permission        | Select the permission type:<br><br>Read Only - Read-only access to the entire MIB except for SNMP configuration objects.<br><br>Read/Write - Read-write access to the entire MIB except for SNMP configuration objects. |



5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form:



6. To Add an SNMP agent using SNMPv3 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.



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:

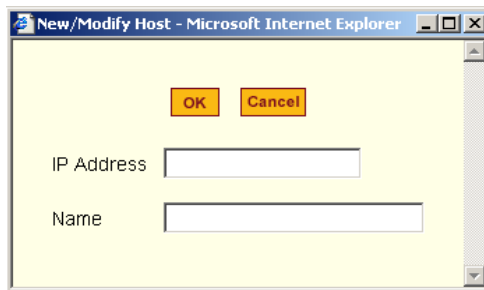


2. To edit host, select the host IP address from the Host Table and then click on the **Edit** button. (If the list is long, use the **Up** and **Down** buttons to go through each item in the list.)

- 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.

**Note:** *Host table entries override DNS server entries.*

## 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:



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

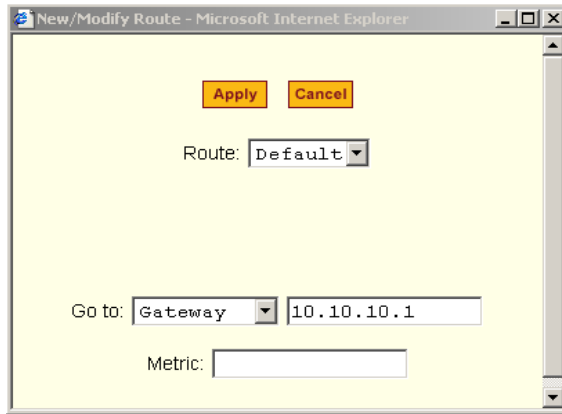
## 4: Web Configuration

- 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:



- Complete the dialog box as follows:

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

- 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/net unit.

**Caution:** *To connect a modem to the KVM/net Aux port, be sure to use the Cyclades RJ-45M to DB-25M straight-through cable (CAB0025).*

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

The system displays 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 shows the Cyclades web configuration interface for the AUX Port. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: KVM, Network, AUX Port (highlighted), and System. The main content area displays the configuration form for the AUX Port. The form includes the following fields and options:

- Profile:** A dropdown menu set to "PPP".
- Baud Rate (Kbps):** A dropdown menu set to "9600".
- Flow Control:** A dropdown menu set to "None".
- Data Size:** A dropdown menu set to "8".
- Parity:** A dropdown menu set to "None".
- Stop Bits:** A dropdown menu set to "1".
- Modern Initialization:** A text area containing the following text:
 

```
TIMEOUT 10
"" \d\1\dATZ
OK\r\n-ATZ-OK\r\n ""
```
- Local IP address:** An empty text input field.
- Remote IP address:** An empty text input field.
- Authentication Required:** A checked checkbox.

At the bottom of the interface, there is a "Wizard" button and several status indicators: "try changes", "cancel changes", "apply changes", "reload page", and "no unsaved changes".

#### 4: Web Configuration

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.<br>For <b>PPP</b> , 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 local IP address.                                                                       |
| Remote IP Address       | The 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/net 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:

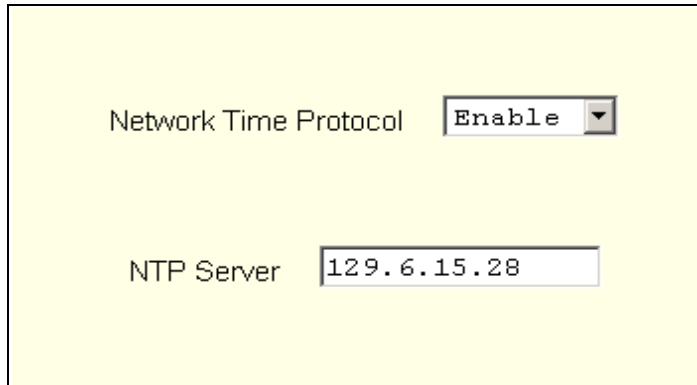
2. If you are not using NTP, complete the date and time fields by selecting the appropriate numbers from the dropdown list boxes.
3. Click on the **apply changes** button to complete the procedure.

### NTP Setting

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

## 4: Web Configuration

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 image 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.

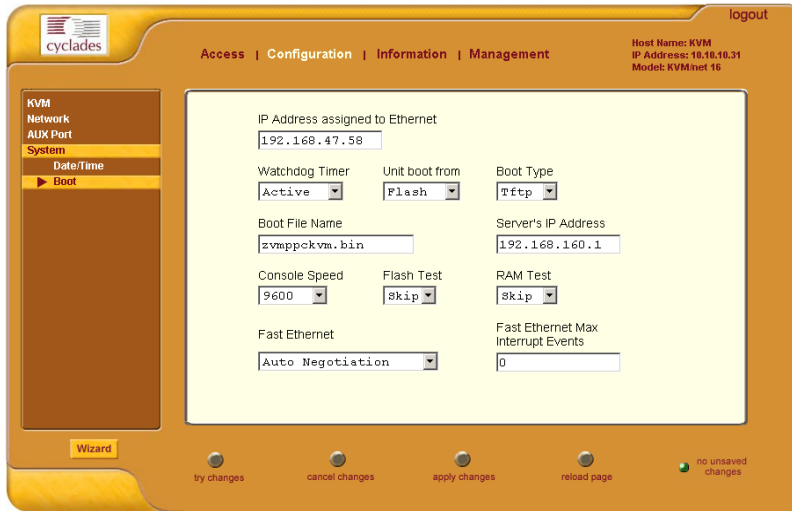
The KVM/net can boot from its internal firmware or from the network. By default, the unit boots from Flash. If you need to boot from the network, install one TFTP or BOOTP server with the firmware to boot from, and then choose **boot from network** and fill in the fields. You may skip Flash test and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

To configure the KVM/net 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     | Usually your KVM/net's IP address                                                          |
| 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                 | The IP address of the TFTP or BOOTP server.                                                |
| 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.   |
| RAM Test                            | Select this to test boot from RAM. You can Skip this test, do a Quick test or a Full test. |
| 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:



## Port Status

Use the Port Status form to view the system status of each KVM/net 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 Upgrade      | Upload firmware from the web to the KVM/net and save the new software version or update.                                                                       |
| Microcode Upgrade     | Update any of the microcontroller microcodes that are stored in the KVM terminator, internal KVM/net switch, KVM RP main, KVM RP local, and KVM Port Expander. |
| Microcode Reset       | Reset any of the microcontroller 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/net 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/net 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 shows a web interface for Backup Configuration. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The left sidebar lists menu items: 'Backup Configuration', '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 row of status indicators: '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/net.
3. Select the **apply changes** button when done. The configuration loaded should run after a reboot.

## Firmware Upgrade

To upgrade your KVM/net firmware, perform the following steps:

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

The system brings up the Firmware Update form:

2. From the Firmware Upgrade 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 Upgrade

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 Upgrade**.

The system brings up the Microcode form:

The screenshot displays the Cyclades web interface for the Microcode Upgrade process. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The left sidebar lists various system management options, with 'Microcode Upgrade' highlighted. The main content area features a 'Target:' label followed by a list of radio buttons: KVM Terminator, KVM Switch (internal), KVM RP Main, KVM RP Local, KVM Port Expander Module, and KVM Video Compression Modules. Below this list are input fields for 'FTP Server', 'User', 'Password', 'Directory', and 'File Name'. An 'Upgrade Now' button is positioned at the bottom of the form. The bottom status bar contains a 'Wizard' button and several status indicators: 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'no unsaved changes'.

2. Complete the input fields as follows:

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

| Field Name | Definition                                               |
|------------|----------------------------------------------------------|
| FTP server | Address of the FTP server used to upgrade 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.

## 4: Web Configuration

3. 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                | <b>System uptime in minutes and seconds (mm:ss).</b>                                                                                                     |
| # Users               | <b>Number of current users.</b>                                                                                                                          |
| User                  | <b>The user who initiated the session.</b>                                                                                                               |
| TTY                   | <b>The name of the serial port.</b>                                                                                                                      |
| From                  | <b>The network machine to which the port is connected.</b>                                                                                               |
| Login@                | <b>The day and time of the last login.</b>                                                                                                               |
| Idle                  | <b>The time when the session or server became inactive.</b>                                                                                              |
| JCPU                  | <b>The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.</b> |
| PCPU                  | <b>The time used by the current process that is named in the What column.</b>                                                                            |
| What                  | <b>The current process attached to the tty.</b>                                                                                                          |

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/net Operation

---

Addressed to the regular user, this chapter presents the procedures and requirements for operating the AlterPath KVM/net, and is organized as follows:

- Logging in
- KVM/net Web Management Interface
- AlterPath Viewer: Connection Menu
- KVM/net Viewer Navigation Keys
- Default Key Sequences
- Changing Your Password
- Connecting to a Server
- Cycling Among Servers
- Remote Operation
- Operating through the Remote Presence (RP)
- Adjusting Screen Brightness and Contrast
- Sharing Server Connection
- Synchronizing Keyboard and Mouse
- Establishing a Power Control Session
- Power Management

For procedures on how to log in and operate the KVM/net as an administrator, refer to **Chapter 3, KVM/net OSD Configuration**.

## Logging In

1. Connect your internet browser to the KVM/net application by typing in the KVM/net server's IP address (*e.g.*, `http://10.0.0.0`) in the browser's address (URL) field as provided to you by your System Administrator.  
The system brings up the AlterPath KVM/net **Login** screen:



2. Log in your User Name and Password as provided to you by your system administrator, and then press <Enter> or select **Go**.  
The system invokes the **Connect** form.
3. If the **Login** screen has been configured to allow direct access to a port, you may enter the port number in the additional **port** field as shown:

**Login**

username  
klimt

password  
\*\*\*\*\*

port  
Port\_16

GO

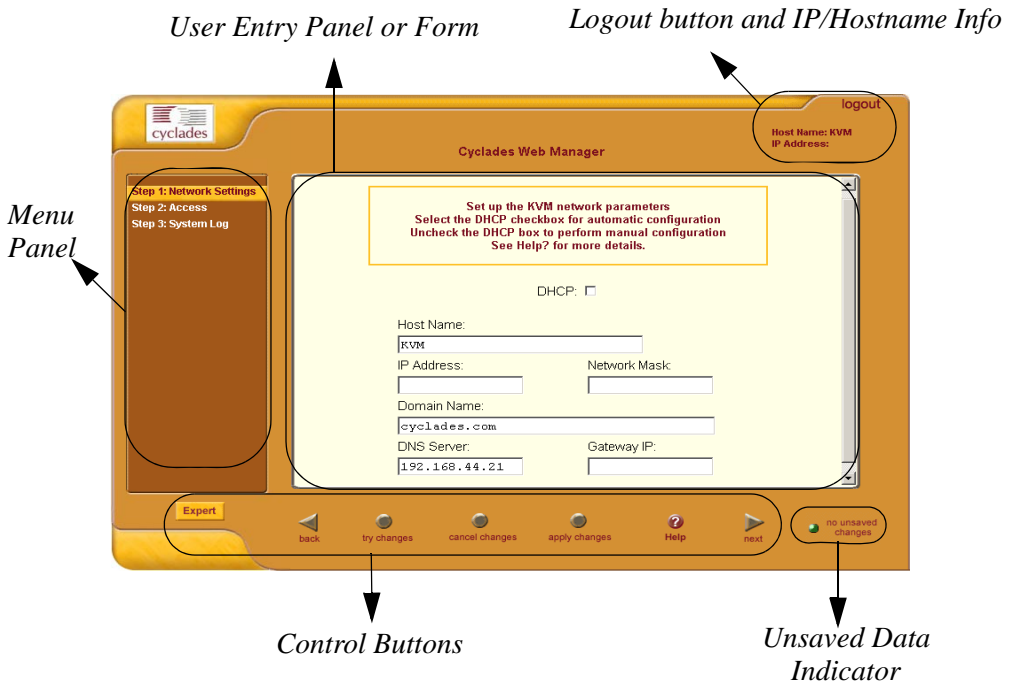
The **port** field accepts either the port alias or the port number using the following format: **port\_[port number]**.

*Example: Port\_8*

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

## KVM/net Web Management Interface

Before continuing, take some time to familiarize yourself with the application's GUI elements. The window shown below is for illustration purposes only; it is not the first window that you will see when you log in to the KVM/net.



The user interface provides you with a main menu and a set of control buttons located at the bottom of the application window. The user entry panel or form changes based on your menu selection.

## 5: KVM/net Operation

When you click the **Connect** button (from the **Connect** form) to connect to a server, the system will launch the AlterPath KVM/net Viewer and connect to the server. The very first time the system invokes the Viewer, it will prompt you to accept a Security Certificate.

Once connected you can connect to another server by typing in <Ctrl-K> and then <Q> to display the **Connection Menu** which will allow you to switch to another server.

### Connecting to a Server

The **Connect** form is used to:

- Launch the KVM/net viewer and connect to a server based on your port selection from the drop down list box.
- Manage the servers from the viewer through the Connection Menu, using the key sequences and navigation keys.

In each case the KVM/net launches a java browser to make the connection.

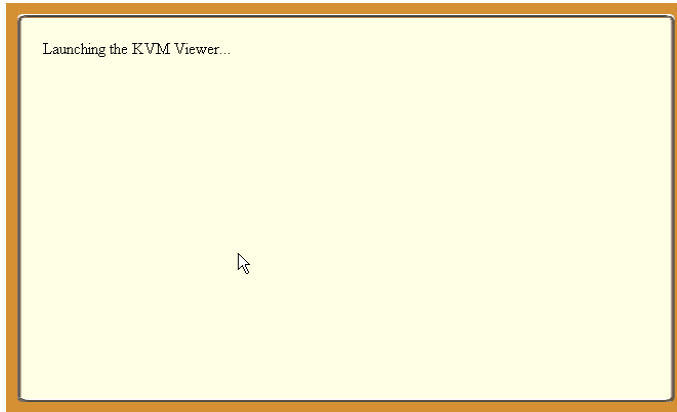
1. From the left menu panel, select **Connect**.

The system invokes the Port Connection form:

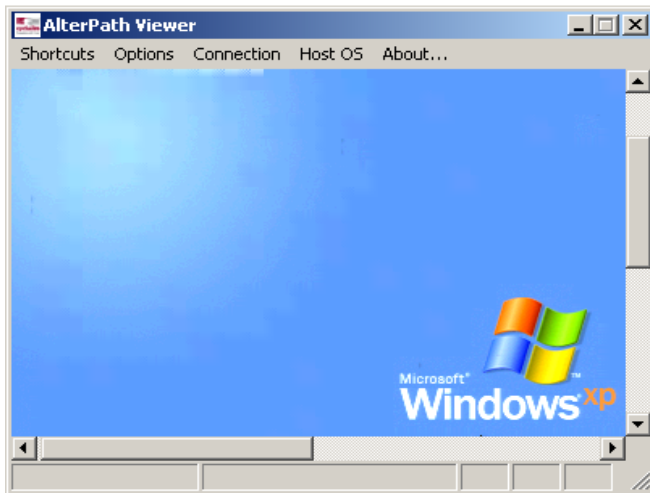


2. From the drop down menu, select the port to which you want to connect.
3. Click on the **Connect** button.

The system prepares to launch the KVM/net viewer:



Once the KVM/net Viewer is launched, you should see the server screen which allows you to view the selected server.



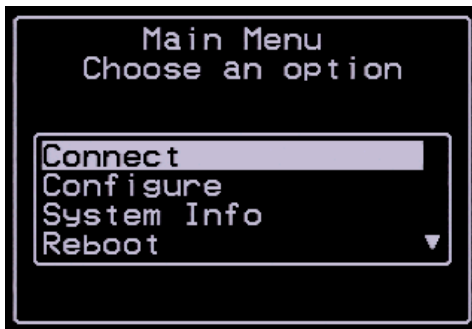
### Connecting to the Server through the OSD

If you are connected as a local user, the system will, instead, display the OSD Login window:



1. From the OSD Login window, enter your username and password as provided to you by the KVM/net administrator.

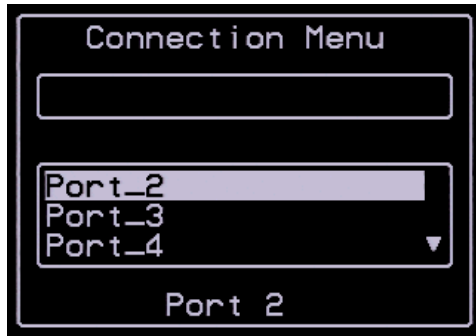
The system displays the OSD Main Menu:



2. From the OSD Main Menu, select **Connect** and press <Enter>.



The system displays the Connection Menu:



3. From the Connection Menu select the port or server you wish to connect to connect by:
  - Entering the first letters of the port name in the quick search box (this field is case-sensitive).
  - OR -
  - Tabbing to the correct port using the scrollable port list box.
4. Press <Enter> to connect to the port.

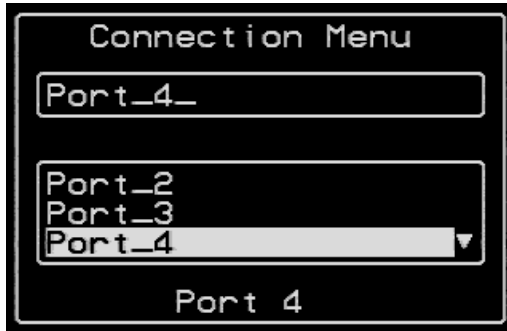
**Note:** *The quick search box of the Connection Menu is designed to speed up the connection process by allowing you to type in the first letters of the port name. Based on your search entry, the port name list box will automatically scroll to the port that matches your entry and highlight it.*

*The search box works for both **User 1** and **User 2** connecting to any KVM port in the master or cascaded KVM units.*

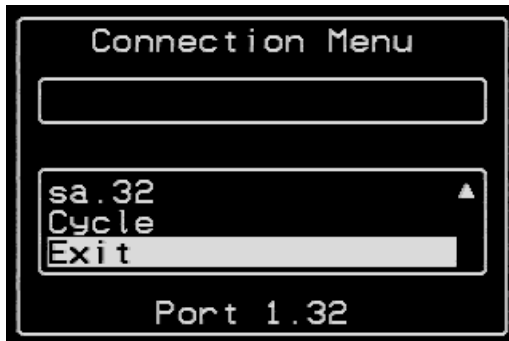
### Returning to the OSD Main Menu

To exit from the Connection Menu and Return to the Main Menu:

1. Press <Ctrl-K> and then <Q> to display the OSD **Connection Menu**:



2. To quit the OSD session from the Connection menu, press <Ctrl-K> and then <Q> to highlight **Exit**. Press <Enter> again.



Refer to the succeeding sections on Overlaying Connection Menu: Navigation Keys and Default Key Sequences to ensure full use of the viewer.

## KVM/net View Settings

For optimized viewing, you can configure the AlterPath viewer from the top menu bar. For a definition of the menu settings, refer to the tables below.

### Recommended Settings

The recommended KVM/net view settings are outlined in the table below.

| <i>Menu</i>              | <i>Select the following option(s):</i>                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------|
| Options                  | Auto Sync Mouse                                                                               |
| Options > Viewer Options | <i>See window below. Settings for the Viewer Options may vary from one system to another.</i> |
| Connection               | T1, No Encryption, High Color                                                                 |
| Host OS                  | Auto/Other                                                                                    |

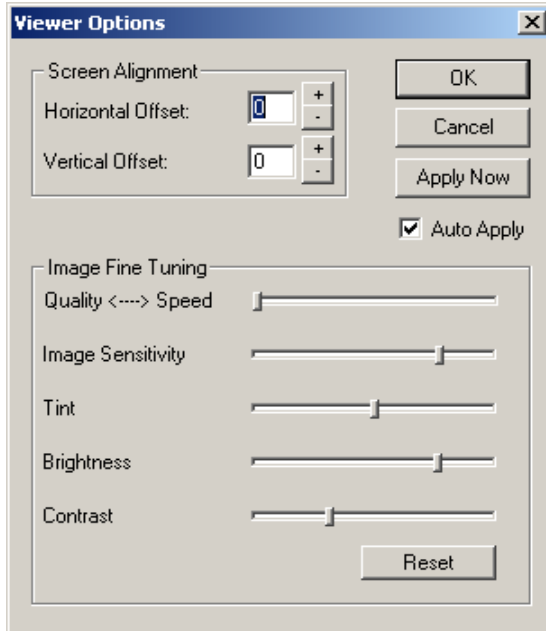
### Options Menu

If you wish to configure the Options settings based on your preferences or requirements, refer to the table below:

| <i>Menu Selection</i>       | <i>Function:</i>                                                                                                                                                                                                    |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Force Screen Refresh        | Forces the viewer to refresh.                                                                                                                                                                                       |
| Force Screen Auto Alignment | Forces the viewer to switch to Auto Alignment mode, which may change the position of the viewer on the screen. (The Screen Alignment is configured from <b>Options &gt; Viewer Options &gt; Screen Alignment</b> .) |
| Toggle Full Screen          | T1, No Encryption, High Color                                                                                                                                                                                       |
| Viewer Options              | Refer to the next section and window diagram.                                                                                                                                                                       |

### Setting the Viewer Options

The Viewer Options window allows you to align or position the viewer window and to fine tune the image. The configuration for these settings may vary from one system to another.



| <i>Field Definition</i> | <i>Function</i>                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Horizontal Offset       | The value of the horizontal coordinate for positioning the AlterPath Viewer on the screen (default = 0).                           |
| Vertical Offset         | The value of the vertical coordinate for positioning the AlterPath viewer on the screen (default = 0).                             |
| Quality <---->Speed     | Move slider to the left to increase image quality; move slider to the right to increase the performance performance of the viewer. |
| Image Sensitivity       | Move slider to the right to increase the image sensitivity.                                                                        |
| Tint                    | Move the slider in either direction to achieve the desired color. For a neutral (white) color, keep the slider in the middle.      |

| <i>Field Definition</i> | <i>Function</i>                                             |
|-------------------------|-------------------------------------------------------------|
| Brightness              | Move the slider to the right to increase screen brightness. |
| Contrast                | Move the slider to the right to increase screen contrast.   |

### Connection Menu

If you wish to configure the Connection settings based on your preferences or requirements, refer to the table below:

| <i>Menu Selection</i>      | <i>Function</i>                                                         |
|----------------------------|-------------------------------------------------------------------------|
| 56K                        | Select this when using a 56K modem to connect to the AlterPath Viewer.  |
| DSL                        | Select this when using DSL.                                             |
| T1                         | Recommended selection for using the KVM viewer from a standard network. |
| Low BW LAN                 | Select this when using a low bandwidth local area network.              |
| LAN                        | Also sets the viewer connection for local area network.                 |
| Auto                       | Sets the connection mode to <i>automatic</i> .                          |
| Encrypt Everything         | Encrypt keyboard, monitor, and mouse.                                   |
| Encrypt Keyboard and Mouse | Encrypt keyboard and mouse only.                                        |
| Encryption Type            | Allows you to select RC4 or Triple DES encryption.                      |
| No Encryption              | Don't encrypt.                                                          |
| High Color                 | Sets the viewer for high screen color resolution.                       |
| Low Color                  | Sets the viewer for low screen color resolution.                        |
| Grey Scale                 | Sets the viewer for grey scale screen color resolution.                 |
| Low Grey Scale             | Sets the viewer for low grey scale screen resolution.                   |

### Host OS

Based on the operating system that you are using to run the AlterPath Viewer, you can configure the Host OS for the following operating systems:

- Windows
- Linux
- Mac OS X
- Solaris
- Auto/Other

### Overlaying Connection Menu: Navigation Keys

Below is a short list of keyboard controls to help you navigate through the KVM Viewer. For the keys to work, make sure 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 ARROW     | Scrolls within a menu.                    |
| BACKSPACE           | Deletes character left to the cursor.     |
| PAGE UP / PAGE DOWN | Skips to the third line.                  |
| END                 | Moves to the end of a menu                |
| HOME                | Moves to the top of a menu                |
| ENTER               | Selects highlighted item; Commits 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/net application.

In KVM/net, the default key sequence (Ctrl-K, Q) for getting out of a particular window while connected to a port is also called *escape sequence*.

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>                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ctrl-K, Q, Esc</b>           | Quit command - closes the port session                                                                                                                                 |
| <b>Ctrl-K</b> and then <b>P</b> | Port command - initiates a power control session.                                                                                                                      |
| <b>Ctrl-K</b> and then <b>V</b> | Video command - controls screen brightness and contrast.                                                                                                               |
| <b>Ctrl-K</b> and then <b>S</b> | Keyboard and Mouse Synchronization command - resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM/net. |
| <b>Ctrl-K .</b> (period)        | Next Port command - moves from the currently connected port to the next authorized port.                                                                               |
| <b>Ctrl-K ,</b> (comma)         | Previous Port command - returns to the previous port.                                                                                                                  |

## Sun USB Keyboard Emulation

When using a PS/2 keyboard, you can emulate the Sun keyboard by using the configured hot key along with the PS/2 keyboard key. These keys, which are mapped to Sun keys, are summarized below:

Default hot key: <Ctrl> + <Alt>

| <i>PS/2 Keyboard Key</i> | <i>Mapped Sun Key Equivalent</i> |
|--------------------------|----------------------------------|
| <b>F2</b>                | Again                            |
| <b>F3</b>                | Props                            |
| <b>F4</b>                | Undo                             |
| <b>F5</b>                | Front                            |
| <b>F6</b>                | Copy                             |
| <b>F7</b>                | Open                             |
| <b>F8</b>                | Paste                            |
| <b>F9</b>                | Find                             |
| <b>F10</b>               | Cut                              |
| <b>F11</b>               | Help                             |
| <b>F12</b>               | Mute                             |
| * [numpad]               | Compose                          |
| + [numpad]               | Vol +                            |
| - [numpad]               | Vol -                            |

## 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/net
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. Save your new password to Flash by typing in: **saveconf**
8. Close your terminal session.

You may also change your password through the KVM/net configuration interface by referring to **Chapter 3: KVM/net Configuration**.

## Differences in OSD Functions

The Online Screen Display (OSD) which also displays the overlaying menus is accessible to both local and remote users. There are, however, two main differences in the OSD features or functions for each user.

- Only the local user has access to the OSD Login screen.
- Only the local user can cycle between servers using the overlaying Connection Menu. (Consequently, only the local user can use the Ctrl-K keys to cycle)

**Note:** *When the connection is KVM-over-IP, the system response may be slow when using the OSD overlay in the KVM viewer. In most cases, consider using the web management interface instead of the OSD interface.*

## How to Read the Port Numbers

The number enclosed in parenthesis following the port logical number is the physical port number.

*Example:* Server 2 (1)

*Where:* Server 2 = port name  
1 = physical port number

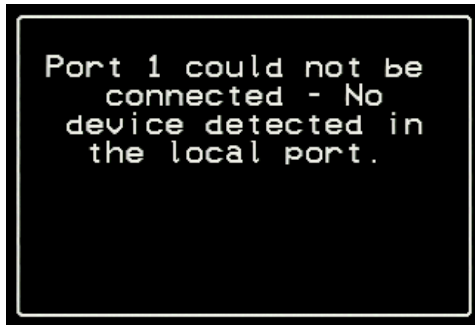
A name and a number connected by a period (.) indicate the slave KVM followed by its physical port.

*Example:* kvm2.4

*Where:* kvm2 = slave name  
4 = physical port on slave kvm2

## Cycling Among Servers

*Cycle* refers to the capability to access or connect from one authorized server to another. This feature is available to the local user only. Through the on-screen display interface, or by using a key sequence, KVM/net provides you immediate access to all connected or authorized servers. Cycling occurs in the order by logical port as they appear in the Server Connection Menu. 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:



There are two types of cycle commands:

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

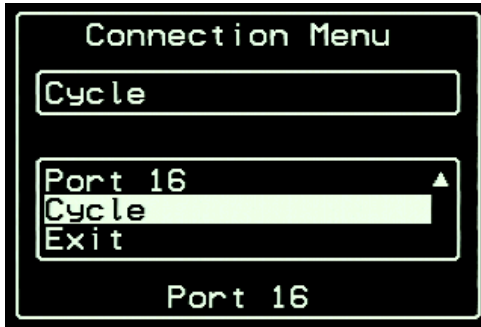
Cycle by Server enables you to view all authorized servers on a continuous basis until all server have been exhausted and then start over again. The cycle does not stop unless you enter the escape sequence (default: **Ctrl-K** and then **Q**) to abort the process and close the session.

### **Cycle by Server**

To initiate Cycle by Server:

1. From the Connection Menu, choose **Cycle** and press **Enter**.

The system brings up the Server Selection Menu:



**Note:** *The Cycle selection is available only to the local (OSD) user, not the WMI user.*

2. Select **Cycle** (you may have to use the **End** key to find Cycle at the bottom of the list) from the Server Connection Menu and then press **Enter**.

The system initiates cycle from the first authorized server.

### **Cycle by Key Sequence**

Cycle by Key Sequence allows you to view or access the next server by entering the Cycle key sequence:

The default Cycle key sequences are:

- **Ctrl-K** and then . (period) for the next port
- **Ctrl-K** and then , (comma) for the previous port.

The cycle by key sequence, like all key sequences, will work only when you are already viewing or accessing a server.

## Using the KVM RP to Extend Operation

You can extend the local distance of your AlterPath KVM/net by using the AlterPath KVM RP. KVM/net supports two concurrent users through any combination of the following:

- One local user at the KVM/net switch.
- One extended user at the AlterPath RP location.
- One remote user over IP.

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

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

### ***Operating through the Remote Presence (RP)***

You can select the keyboard, video, and mouse extended console between a local station and a server connected to the KVM/net 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/net.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + R to switch the local video display to the remote server connected to the KVM/net.
- Use the key sequence [Scroll Lock] + [Scroll Lock] + L to switch the local video display to the local station connected to the KVM RP.

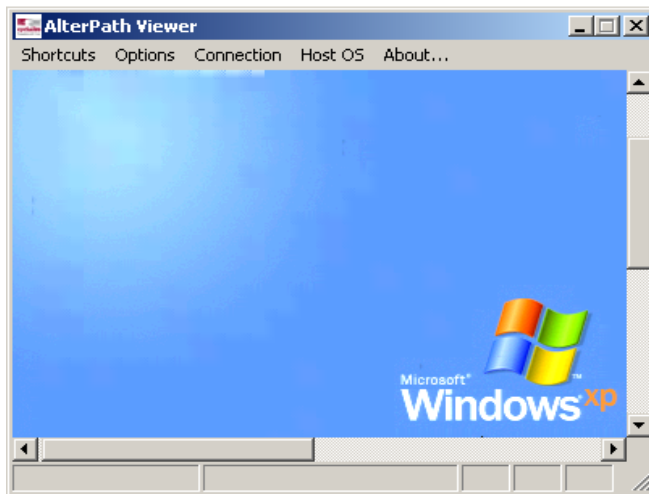
## Finishing your Session

There are three ways to end your AlterPath Viewer session:

- Select **Exit** from the AlterPath Viewer Client
- From either the Viewer Client or from the OSD, press the escape sequence (**Ctrl-K, Q, Esc**)
- Through Idle Timeout

### Method 1: Exiting from the AlterPath Viewer Client

From the menu bar of the AlterPath Viewer, go to: **Shortcuts > Exit Viewer Client**.



### Method 2: Exiting by using the escape sequence.

Press **Ctrl-K** keys followed by **<Q>** and **<Esc>**.

The system will close the session.

### Method 3: Exiting by Idle Timeout

Leaving your system idle will eventually close the session based on the configured idle time. The idle time is set by the KVM/net administrator.

## Adjusting Screen Brightness and Contrast

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

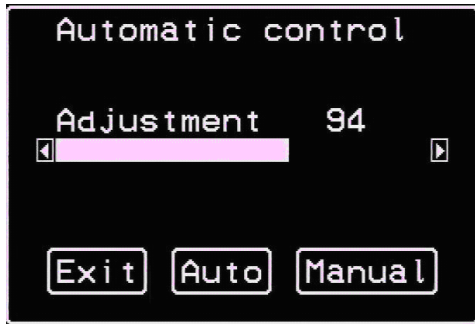
Depending on which window was accessed last, the system will display either one of the following overlaying windows:

- 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.

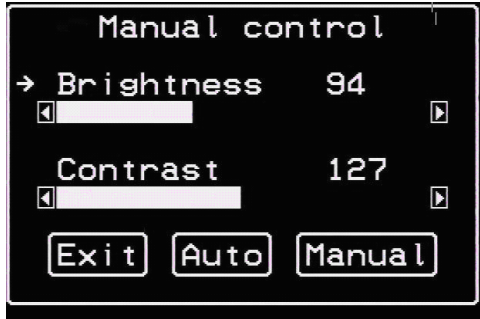
If this setting is not adjusted properly, the video quality will be poor. When the user uses KVM-over-IP, the poor image quality can result to reduced performance.



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/net 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.

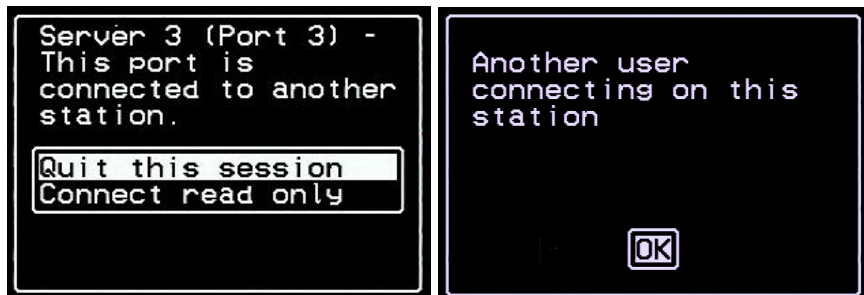
When a user connects to a server that is already in use, the software auto-detects the event and presents a menu to the connecting user. Options available under this menu will vary depending on the connecting user access permissions. Also, a notification is presented to the current user, depending on 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
- Connect read-only: connects the user in read-only mode and notifies the previously connected user of the new connection.

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

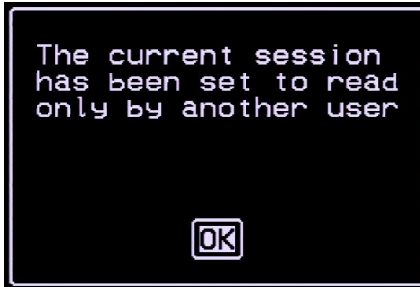
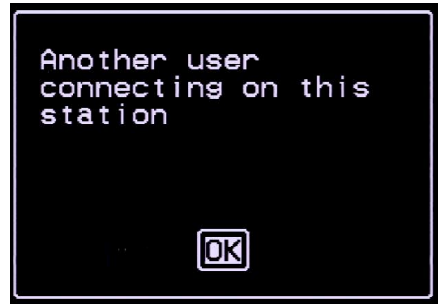
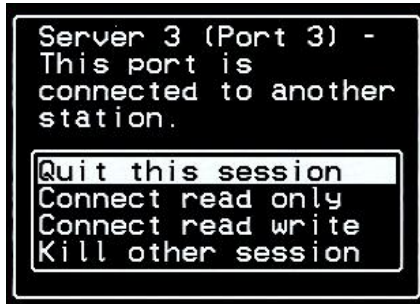


If the connecting user has either read-write, read-write-config, read-write-power or full access permission to the server port, the following additional options are presented in the menu:



- Connect read write: connects the user in read-write mode and the previous user is notified of the event. A previous user who is connected in read-write mode is changed to read-only mode and 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 his or her 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 a escape sequence command)

## Resetting 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 Reset 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** on page 2 - 13.*

## Establishing a Power Control Session

### Power Control by Escape Sequence

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

### Power Control Over IP

If you have Power Manager configured into the KVM/net switch, then you should be able to use the Power Management form of the web interface.

## 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>                                                                                                                                                                                                                                                                         |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Outlets Manager</b>  | Switch on/off and lock/unlock outlets; reboot network devices.                                                                                                                                                                                                                                   |
| <b>View IPDUs Info</b>  | View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.                                                                                                                                                         |
| <b>Users Manager</b>    | <i>For admin user only.</i> This form is used to Add or delete users assigned to specific outlets.                                                                                                                                                                                               |
| <b>Configuration</b>    | <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. |
| <b>Software Upgrade</b> | <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:



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.

2. 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.

The screenshot shows the 'Outlets Manager' window with the following data:

| Outlet | Outlet Name | Outlet State | Power Up Interval |      |      |
|--------|-------------|--------------|-------------------|------|------|
| 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. 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:

| Outlets Manager                           | View IPDUs Info | Users Manager                         | Configuration                | Software Upgrade |
|-------------------------------------------|-----------------|---------------------------------------|------------------------------|------------------|
| <b>Serial Port 4: General Information</b> |                 | <b>Clear Max Detected Current</b>     |                              |                  |
|                                           |                 | <b>Clear Max Detected Temperature</b> |                              |                  |
| Name: PowerMgm-4                          |                 | Syslog: ON                            | Number of Outlets: 8         |                  |
| Number of Units: 1                        |                 | Buzzer: ON                            | Over Current Protection: OFF |                  |
| <b>Master Unit Information:</b>           |                 |                                       |                              |                  |
| 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.

## Chapter 6

# Remote Authentication

---

This section provides some guidelines for configuring remote authentication in the KVM/net 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/net 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/net 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.

**Note: Regarding LDAP:** *The KVM/net 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

### ***Kerberos***

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.

## **LDAP**

### **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.

# Appendix A

# Technical Specifications

---

## Features

### Operating System

- Linux®

### Accessibility

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

### Security

- Local, RADIUS, TACACS+, LDAP, Kerberos, and NTLM (Windows NT LAN Manager) 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)
- Access through Web Management Interface (WMI)
- 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

## *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

ATP4620 AlterPath™ KVM Terminator, Sun USB  
Server-side Unit, Sun USB

ATP4630 AlterPath™ KVM Terminator, PC USB  
Server-side Unit, PC USB

ATP4710 AlterPath™ KVM RP  
Remote User Interface Unit

## Hardware

### CPU

- MPC855T (PowerPC Dual-CPU @48 MHz)

### 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)
- 1 RJ-45 User Interface (CAT5-based)

### Power

- Internal 100-240V~, 50/60 Hz, 0.9A

### Operating Temperature

- 32°F to 122°F (0°C to 50°C)

### Storage Temperature

- -40°F to 185°F (-40°C to 85°C)

### Humidity

- 5% to 90% non-condensating

### Dimensions (WxDxH)

- 17 x 9.5 x 1.75 in (43.18 x 24.13 x 4.45 cm)

### Certification FCC Part 15, A

- EN55022, A (CE)



# 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.

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 key length 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.

## **Baud Rate**

The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per

symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.

- 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.
- Checksum** A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.
- DHCP** Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.
- DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.



- Escape Sequence** A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.
- An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one capability, and thus need some way to tell data from commands.
- Ethernet** A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.
- Flash** Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.
- Flow Control** A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.
- Hot-Swap** Ability to remove and add hardware to a computer system without powering off the system.
- IP Address** A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals. Each address has a network number, an optional sub network number and a host number. The first two numbers are used

for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.

**IP packet filtering**

This is a set of facilities in network equipment that allows the filtering of data packets based on source/destination addresses, protocol, TCP port number and other parameters. Packet filtering is one of the main functions of a firewall.

**IPsec**

Short for *IP Security Protocol*, IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as 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**

A number used by software to separate the local subnet address from the rest of a given Internet protocol address

Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e. 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.

**NTP**

*Network Time Protocol.* A standard for synchronizing your system clock with the "true time", defined as the average of many high-accuracy clocks around the world.

**OSD**

On-Screen Display.

**Packet**

A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is 1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.

**Parity**

In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.

The following lists the available parity parameters and their meanings:

**Odd** - Parity bit set so that there is an odd number of 1 bits

**Even** - Parity bit set so that there is an even number of 1 bits

**None** - Parity bit is ignored, value is indeterminate

**Port**

A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that

run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a port number may be seen as an address of an application within the computer.

**PPP**

*Point-to-Point Protocol*. This protocol is a way to connect your computer to the Internet over telephone lines. PPP is replacing an older protocol, SLIP, as it is more stable and has more error-checking features.

PPP has been a widely-used Internet standard for sending datagrams over a communications link. The PPP standard is described in RFC 1661 by the Point-to-Point Working Group of the Internet Engineering Task Force (IETF). PPP is commonly used when remote computers call an Internet service provider (ISP) or a corporate server that is configured to receive incoming calls.

**RADIUS**

Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

**SMTP**

Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.

**SNMP**

Short for *Simple Network Management Protocol*, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

(Source: Webopedia)

**SNMP Traps**

Notifications or Event Reports are occurrences of Events in a Managed system, sent to a list of managers configured to receive Events for that managed system. These Event Reports are called Traps in SNMP. The Traps provide the value of one or more instances of management information.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

The Trap Definition vary with the SNMP Version (which defines the messaging format), but the information contained in these are essentially identical. The major difference between the two message formats is in identifying the events.

**SSH**

Secure Shell. A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

**Stop Bit**

A bit which signals the end of a unit of transmission on a serial line. A stop bit may be transmitted after the end of each byte or character.

**Subnet Mask**

A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.

**TACACS**

Terminal Access Controller Access Control System.

Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

**TACACS+**

Terminal Access Controller Access Control System Plus. A protocol that provides remote access authentication, authorization, and related accounting and logging services, used by Cisco Systems.

**Telnet**

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console.

**TTY**

1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.

**UDP**

*User Datagram Protocol* uses a special type of packet called