

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

Software Version 2.0



## **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: August 2005

Part Number: PAC0366

©2005 Cyclades Corporation

Information in this document is subject to change without notice.

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

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.

# Contents

Before You Begin .....	xxix
Audience .....	xxix
Document Organization .....	xxx
Related Documents .....	xxxi
Typographic and Other Conventions .....	xxxi
Chapter 1: Introduction .....	1
Description .....	2
What's New in KVM/net Plus .....	4
Support for up to Ten Concurrent Users .....	4
In-band Server Access .....	4
Color OSD .....	5
PCMCIA Card Slots .....	6
LED Status .....	6
Access Window for Managing Multiple Server Connections .....	6
Temperature Monitor .....	8
Enhanced Power Management for Cascaded Devices .....	8
Enhanced Syslogging .....	8
Guidelines for Using the KVM/net Plus .....	8
Connectors on the KVM/net Plus .....	9
Types of Ports .....	9
Connectors on the Back .....	11
Power Connector and Power Switch .....	12
KVM Ports .....	12
Management Ports (Console, Ethernet, User 1, User 2) .....	13
AUX Ports .....	15
PCMCIA Card Slots on the Front .....	16
Activity LEDs on the KVM/net Plus .....	16
Activity LEDs on the Management and AUX Ports .....	16
Front Panel Activity LEDs .....	18
AlterPath KVM/net Plus Ordering Options .....	19
Types of Users .....	20

Simultaneous KVM/net Plus Logins .....	21
Simultaneous Server Connections .....	22
Administration Options .....	23
Cyclades Web Manager .....	24
Prerequisites for Using the Web Manager .....	25
TCP Ports .....	26
Cascaded Devices .....	27
Accessing Ports on Cascaded KVM Devices .....	29
KVM/net Plus Port Permissions .....	29
Understanding KVM Port Permissions .....	30
KVM Port Permissions Hierarchy .....	31
Decision 1: Check User's KVM Port Permissions .....	31
Decision 2: Check Group's KVM Port Permissions .....	32
Decision 3: Check Generic User's KVM Port Permissions .....	32
Decision 4: Check User's Default Permissions .....	33
Decision 5: Check Group's Default Permissions .....	33
Decision 6: Check Generic User's Default Permissions .....	34
Server Access: In-band and Out of Band .....	34
Determining the Connection Type and its Supported Functionality .....	36
Administering Users of Connected Servers .....	38
Types of Access to Ports .....	38
Tasks Related to Access to Connected Devices .....	38
Redefining Keyboard Shortcuts (Hot Keys) .....	40
Redefining KVM Connection Hot Keys .....	40
Redefining Sun Keyboard Equivalent Hot Keys .....	40
Summary of Tasks for Redefining Hot Keys .....	41
Packet Filtering on the KVM/net Plus .....	42
Power Management .....	44
Options for Managing Power .....	44
Controlling Power Through the Web Manager IPDU	
Power Management Forms .....	45
Controlling Power While Connected to KVM Ports .....	45
Setting Up and Configuring Power Management .....	46
Security .....	47
Encryption .....	47
Authentication .....	48
Choosing Among Authentication Methods .....	48
Tools for Specifying Authentication Methods .....	51
Notifications, Alarms, and Data Buffering .....	52
Syslog Servers .....	52

Prerequisites for Logging to Syslog Servers .....	52
Facility Numbers for Syslog Messages .....	53
Example of Using Facility Numbers .....	53
Configuring Logging and Alarms .....	53
VPN and the KVM/net Plus .....	54
Considerations When Choosing Whether to Enable DHCP .....	55
Monitoring Temperatures .....	56
KVM Terminator Usage and Types .....	58
KVM Expander .....	59
KVM Expander Features .....	60
KVM Expander Models and Components .....	61
Ports on the KVM Expander .....	62
LEDs on the KVM Expander .....	63
Power Outlets on the KVM Expander .....	63
Cascading a KVM Expander .....	64
Adding the KVM Expander to the KVM/net Plus Unit's List of Cascaded Devices .....	66
Upgrading the KVM Expander Microcontroller Code .....	66
User Access .....	67
AlterPath KVM RP .....	68
Connectors on the Back of the KVM RP .....	68
<b>Chapter 2: Installing the KVM/net Plus.....</b>	<b>71</b>
Shipping Box Contents AlterPath KVM/net Plus .....	73
Setting Up the KVM/net Plus .....	75
Making an Ethernet Connection .....	79
Connecting Servers to the KVM Ports .....	80
Making a Direct Connection for Network Configuration .....	84
Powering On the KVM/net Plus and Connected Devices .....	85
Performing Basic Network Configuration .....	86
Configuring Basic Networking Using the wiz Command .....	87
Configuring Basic Networking Using the OSD .....	90
Completing Configuration Using the Web Manager .....	99
Changing Default Passwords .....	100
Enabling Access to the Web Manager without Making a Direct Connection .....	102
Preconfiguring the KVM/net Plus for Remote Installation .....	105
Additional Configuration Tasks .....	106
Avoiding Conflicting Mouse Settings .....	107

Avoiding Internet Explorer Conflicts .....	110
<b>Chapter 3: Advanced Installation Procedures .....</b>	<b>113</b>
Installing PCMCIA Cards in the Front Card Slots .....	114
Connecting an External Modem .....	116
Connecting AlterPath PMs to the KVM/net Plus .....	117
Installing the AlterPath KVM Expander .....	119
Shipping Box Contents KVM Expander .....	120
Setting Up the KVM Expander .....	122
Powering On the KVM Expander and Connected Devices .....	125
Connecting Cascaded KVM Units to the Primary KVM/net Plus .....	126
Installing the AlterPath KVM RP .....	129
Shipping Box Contents KVM RP .....	130
Options for Accessing the RP .....	131
Supplying Power to the RP .....	132
<b>Chapter 4: Web Manager for Administrators .....</b>	<b>133</b>
Common Tasks .....	134
Common Features of Administrators' Windows .....	136
Administrators' Control Buttons, Logout Button, and KVM/net Plus Information .....	136
Obtaining More Information .....	137
Logging Into the Web Manager and Saving Changes .....	138
Administrative Modes .....	141
Wizard Mode .....	141
Procedures in Wizard Mode .....	142
Steps in Wizard Mode .....	142
Step 1: Network Settings [Wizard] .....	142
Step 2: Access [Wizard] .....	144
Step 3: System Log [Wizard] .....	149
Expert Mode .....	151
Overview of Menus and Forms in Expert Mode .....	152
Access .....	153
Connect to Server .....	153
IPDU Power Management .....	154
Outlets Manager .....	155
View IPDUs Info .....	156
Users Manager .....	157

Configuration .....	159
Software Upgrade .....	160
Configuration .....	162
KVM .....	163
General .....	164
General .....	164
Enabling Direct Access to KVM Ports .....	165
Redefining KVM Connection Keyboard Shortcuts (Hot Keys) .....	166
Specifying Authentication for KVM Port Logins .....	167
Local User and IP Users .....	168
Configuring Individual KVM Ports .....	172
Configuring Cascaded KVM Units .....	177
Users & Groups .....	181
Security .....	189
Configuring an Authentication Method .....	191
Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices .....	194
Configuring In-band (RDP) Servers .....	203
Prerequisites for In-band Access to RDP Servers .....	204
Network .....	209
Host Settings .....	211
Syslog .....	214
Configuring a Modem (PCMCIA) Card .....	216
Services .....	220
IP Filtering .....	221
VPN .....	238
SNMP .....	242
Host Tables .....	246
Static Routes .....	248
AUX Ports .....	250
System .....	253
Time/Date .....	254
Boot Configuration .....	256
Viewing System Information .....	260
General .....	260
Port Status .....	261
Temperature Sensor .....	263
Management .....	267
Backup Configuration .....	268
Firmware Upgrade .....	272

Microcode Upgrade .....	276
Microcode Reset .....	279
Active Sessions .....	280
Reboot .....	282
<b>Chapter 5: Web Manager for Regular Users .....</b>	<b>283</b>
Web Manager for Regular Users .....	284
Prerequisites for Logging in to the Web Manager .....	286
Power Management for Regular Users .....	288
Power Control of Any Device Plugged Into a PM on the KVM/net Plus .....	288
Changing Your KVM/net Plus Password .....	289
<b>Chapter 6: Accessing Connected Devices .....</b>	<b>291</b>
Who Can Access Connected Devices .....	292
Server Connections: What You See .....	293
Viewing KVM Connections .....	294
Viewing In-band Connections .....	296
Prerequisites for Accessing Servers With In-band Connections .....	296
Prerequisites for Accessing Servers With KVM Connections .....	297
Web Manager Login Screen .....	297
Login Screen: Direct Logins Not Enabled .....	299
Connect to Server Drop-down List .....	300
Servers and Connection Types in the Connect to Server Drop-down List .....	300
Port Numbers of Cascaded KVM Devices in the Connect to Server Drop-down List .....	301
Login Screen: Direct Logins Enabled, Only IP Address Entered .....	301
Login Screen: Direct Logins Enabled, IP Address and Port Entered .....	302
Connecting to Servers Remotely Through the Web Manager .....	304
Managing Multiple Server Connections with the Access Window .....	308
Adjusting Screen Brightness and Contrast .....	312
Sharing a Server Connection .....	315
Connecting to Servers Locally Through the OSD .....	320
Controlling Local KVM Port Connections Through the OSD .....	322
Hot Keys for Local .....	323
Hot Keys for Emulating Sun Keyboard Keys .....	324
Cycling Between Servers .....	326



Resetting the Keyboard and Mouse .....	328
Controlling Power of a KVM-connected Server .....	329
Closing a Local KVM Connection .....	330
Sharing KVM Port Connections .....	330
AlterPath Viewer Settings .....	332
Recommended Settings .....	332
Options Menu .....	333
Setting the Viewer Options .....	334
Connection Menu .....	335
Power Management .....	336
Modem Connections .....	339
<b>Chapter 7: On Screen Display .....</b>	<b>345</b>
Navigating the OSD .....	346
Basic Navigation Keys .....	346
Common Navigation Actions .....	347
Logging In Through the OSD .....	347
OSD Main Menu .....	348
Connection Menu .....	349
Power Management Menu .....	350
Configure Menu Overview .....	351
Understanding OSD Configuration Screen Series .....	354
General Configuration Screens [OSD] .....	355
Network Configuration Menu Options [OSD] .....	358
Network Configuration Screens [OSD] .....	359
SNMP Configuration Screens [OSD] .....	362
VPN Configuration Screens [OSD] .....	366
IP Filtering Configuration Screens .....	370
Hosts Configuration Screens [OSD] .....	377
Static Routes Configuration Screens .....	378
Date/time Configuration Screens .....	381
User Station Screens .....	382
KVM Ports Screens .....	385
AUX Ports Screens .....	387
Cascade Devices .....	390
Users and Groups Screens .....	393
Syslog Screens .....	400
PCMCIA Screens .....	400
Authentication Screens .....	404

Save/Load Configuration Screens .....	411
System Info Menu .....	414
Reboot .....	415
Controlling the OSD Through the AlterPath KVM RP .....	416
<b>Appendix A: Troubleshooting .....</b>	<b>419</b>
Replacing a Boot Image .....	420
Downloading a New Software Version .....	422
Changing the Boot Image .....	423
Changing the Boot Image with bootconf .....	423
Changing the Boot Image in U-Boot Monitor Mode .....	424
<b>Appendix B: Technical Specifications.....</b>	<b>429</b>
<b>Glossary .....</b>	<b>431</b>
<b>Index .....</b>	<b>439</b>

# List of Figures

<b>Figure 1-1:</b>	KVM/net Plus Front and Back.....	2
<b>Figure 1-2:</b>	OSD Main Menu.....	5
<b>Figure 1-3:</b>	Access Pop-up Window with Two Active Port Connections .....	7
<b>Figure 1-4:</b>	Show Connections Link on the Connect to Server form .....	7
<b>Figure 1-5:</b>	KVM/net Plus Back Panel .....	11
<b>Figure 1-6:</b>	Power Connector and KVM Server Ports on the Left Rear .....	12
<b>Figure 1-7:</b>	KVM Ports on the Center Rear.....	12
<b>Figure 1-8:</b>	Management Ports .....	13
<b>Figure 1-9:</b>	AUX Ports.....	15
<b>Figure 1-10:</b>	PCMCIA Card Slots on Front of the AlterPath KVM/net Plus .....	16
<b>Figure 1-11:</b>	LEDs on the KVM/net Plus Management Ports.....	17
<b>Figure 1-12:</b>	Activity LEDs on the Front of the KVM/net Plus .....	19
<b>Figure 1-13:</b>	Simultaneous Administrator Login Prompt.....	21
<b>Figure 1-14:</b>	Cascaded KVM Devices from an KVM/net Plus .....	27
<b>Figure 1-15:</b>	Connecting an AlterPath PM to the KVM/net Plus.....	44
<b>Figure 1-16:</b>	KVM/net Plus VPN Example .....	54
<b>Figure 1-17:</b>	KVM Expander Back Panel Components .....	61
<b>Figure 1-18:</b>	Ports on the KVM Expander Back Panel.....	62
<b>Figure 1-19:</b>	Connecting a KVM Expander to the KVM/net Plus ...	64
<b>Figure 1-20:</b>	Devices Form on KVM/net Plus Web Manager .....	66
<b>Figure 1-21:</b>	Microcode Update Form on KVM/net Plus Web Manager .....	67
<b>Figure 1-22:</b>	KVM RP Front.....	68
<b>Figure 1-23:</b>	KVM RP Back Panel .....	68
<b>Figure 2-1:</b>	KVM/net Plus and Brackets for Front Mounting .....	75
<b>Figure 2-2:</b>	KVM/net Plus and Brackets for Back Mounting.....	76

<b>Figure 2-3:</b>	Rack Mounting Holes on the KVM/net Plus .....	76
<b>Figure 2-4:</b>	Right Bracket for Back Mounting the KVM/net Plus ..	77
<b>Figure 2-5:</b>	Right Bracket for Front Mounting the KVM/net Plus ..	77
<b>Figure 2-6:</b>	Left Bracket for Front Mounting the KVM/net Plus ...	77
<b>Figure 2-7:</b>	Left bracket for Back Mounting the KVM/net Plus ....	78
<b>Figure 3-1:</b>	PCMCIA Card Slots on the KVM/net Plus Front Panel .....	114
<b>Figure 4-1:</b>	Example Window in Wizard Mode.....	141
<b>Figure 5-1:</b>	Cyclades KVM/net Plus Web Manager .....	285
<b>Figure 6-1:</b>	AlterPath Viewer for KVM Connections.....	294
<b>Figure 6-2:</b>	Access Window.....	295
<b>Figure 6-3:</b>	ActiveX Viewer for In-band Connections .....	296
<b>Figure 6-4:</b>	Web Manager Login Screen Without KVM Direct Logins Enabled .....	299
<b>Figure 6-5:</b>	Connect To Server Drop-down List.....	300
<b>Figure 6-6:</b>	Example: Web Manager with Direct Logins Enabled, IP Address and Port Entered.....	303
<b>Figure 6-7:</b>	Access Pop-up Window with Two Active Port Connections .....	308
<b>Figure 6-8:</b>	Connection Options for Users with Read Only Permission.....	316
<b>Figure 6-9:</b>	Connection Options for Users with Read-Write or Read-Write-Power Permissions .....	316
<b>Figure 6-10:</b>	AlterPath Viewer Options Screen .....	334
<b>Figure 7-1:</b>	OSD Main Menu.....	348
<b>Figure 7-2:</b>	First, Middle, and Last Screens in Configuration Series.....	354
<b>Figure 7-3:</b>	User Station Configuration Screens.....	383
<b>Figure 7-4:</b>	KVM Ports Configuration Screens .....	386
<b>Figure 7-5:</b>	AUX Ports Configuration Screens.....	387
<b>Figure 7-6:</b>	Cascade Devices Configuration Screens .....	390
<b>Figure 7-7:</b>	Users and Groups Configuration Screens .....	394
<b>Figure 7-8:</b>	Syslog Configuration Server Screen.....	400
<b>Figure 7-9:</b>	PCMCIA Configuration Screens .....	401
<b>Figure 7-10:</b>	Authentication Options and Screens.....	405
<b>Figure 7-11:</b>	Save/Load Config Configuration Screens .....	412

# List of Tables

<b>Table ii-1:</b>	Typographic Conventions .....	xxxi
<b>Table ii-2:</b>	Other Terms and Conventions .....	xxxii
<b>Table 1-1:</b>	Port Types.....	9
<b>Table 1-2:</b>	Management Port LED Status Definitions.....	17
<b>Table 1-3:</b>	Model Numbers and Configuration Options .....	19
<b>Table 1-4:</b>	User Types, Responsibilities, and Default Password .....	20
<b>Table 1-5:</b>	Server Connection Types Available on the KVM/net Plus.....	22
<b>Table 1-6:</b>	Administration Options .....	23
<b>Table 1-7:</b>	Supported Browsers .....	25
<b>Table 1-8:</b>	Tasks: Configuring TCP Port Numbers .....	26
<b>Table 1-9:</b>	Connectors and Ports for Cascading KVM Units .....	28
<b>Table 1-10:</b>	Default Port Access Permissions.....	29
<b>Table 1-11:</b>	Tools for Setting KVM Port Permissions.....	31
<b>Table 1-12:</b>	In-band and Out of Band Connections .....	34
<b>Table 1-13:</b>	Available Functionality During KVM and In-band Connections .....	36
<b>Table 1-14:</b>	Tasks for Redefining Hot Keys .....	41
<b>Table 1-15:</b>	Levels of IP Filtering.....	42
<b>Table 1-16:</b>	Tasks: General Power Management Set Up .....	46
<b>Table 1-17:</b>	Tasks: KVM-connected Power Management.....	47
<b>Table 1-18:</b>	Supported Authentication Types for KVM/net Plus and Port Types.....	48
<b>Table 1-19:</b>	Tasks: Specifying Authentication Methods.....	51
<b>Table 1-20:</b>	Temperature Graph Parameters .....	56
<b>Table 1-21:</b>	AlterPath KVM Terminators .....	58
<b>Table 1-22:</b>	KVM Expander Model Numbers and Port Options .....	61
<b>Table 1-23:</b>	KVM Expander Port Types .....	62
<b>Table 1-24:</b>	Maximum Number of Supported Servers .....	65

<b>Table 1-25:</b>	KVM RP Port Types .....	69
<b>Table 2-1:</b>	Shipping Box Contents, Part Numbers, and Description .....	73
<b>Table 2-2:</b>	OSD Equivalents for Common Actions .....	90
<b>Table 3-1:</b>	KVM Expander Shipping Box Contents, Part Numbers, and Description .....	120
<b>Table 3-2:</b>	KVM RP Shipping Box Contents, Part Numbers, and Description .....	130
<b>Table 4-1:</b>	Network Forms.....	209
<b>Table 4-2:</b>	Host Settings Configuration Fields .....	212
<b>Table 4-6:</b>	Add/Modify Static Routes Fields .....	249
<b>Table 4-7:</b>	PPP Fields for Configuring the AUX Port.....	252
<b>Table 4-8:</b>	Boot Configuration Fields and Options .....	258
<b>Table 4-9:</b>	Port Status Information .....	262
<b>Table 5-1:</b>	Power Management Tasks Available to Regular Users	288
<b>Table 6-1:</b>	Web Manager Login Screen Options .....	297
<b>Table 6-2:</b>	Tasks Available During KVM Connections.....	309
<b>Table 6-3:</b>	Access Window Brightness and Contrast Arrows .....	313
<b>Table 6-4:</b>	Connection Option According to Port Access Permissions .....	315
<b>Table 6-5:</b>	Power Status Icons .....	319
<b>Table 6-6:</b>	Tasks Available While Connected to KVM Ports Through the OSD .....	322
<b>Table 6-7:</b>	Default Local Keyboard Shortcuts Through the OSD	323
<b>Table 6-8:</b>	Default Sun Key Emulation Hot Keys .....	324
<b>Table 6-9:</b>	AlterPath Viewer>Options>Viewer Options Menu .....	334
<b>Table 6-10:</b>	Tasks for Configuring and Making Dial Up Connections (User).....	340
<b>Table 7-1:</b>	Basic Navigation Keys .....	346
<b>Table 7-2:</b>	OSD Equivalents for Common Actions .....	347
<b>Table 7-3:</b>	OSD Main Menu Items .....	348
<b>Table 7-4:</b>	Configuration Menu Items .....	352
<b>Table 7-5:</b>	General Configuration Screens [OSD].....	355
<b>Table 7-6:</b>	Network Configuration Screens [OSD] .....	360
<b>Table 7-7:</b>	SNMP Configuration Screens [OSD] .....	364

<b>Table 7-8:</b>	VPN Configuration Screens [OSD] .....	367
<b>Table 7-9:</b>	IP Filtering Configuration Screens [OSD] .....	372
<b>Table 7-10:</b>	Hosts Configuration Screens [OSD] .....	378
<b>Table 7-11:</b>	Static Routes Screens [OSD].....	379
<b>Table 7-12:</b>	User Station Configuration Screens .....	383
<b>Table 7-13:</b>	KVM Port Configuration Screens .....	386
<b>Table 7-14:</b>	KVM Ports Configuration Screens .....	388
<b>Table 7-15:</b>	Cascade Devices Configuration Screens.....	391
<b>Table 7-16:</b>	Local Users Configuration Screens.....	395
<b>Table 7-17:</b>	Local Groups Configuration Screens .....	396
<b>Table 7-18:</b>	User Access List KVM Port Permissions Configuration Screens .....	398
<b>Table 7-19:</b>	OSD Configuration Screens for a PCMCIA Modem Card.....	402
<b>Table 7-20:</b>	Authentication Configuration Screens for KVM/net Plus Logins.....	406
<b>Table 7-21:</b>	Common Configuration Screens for Kerberos and LDAP Authentication Servers .....	406
<b>Table 7-22:</b>	Unique LDAP Authentication Server Configuration Screens .....	408
<b>Table 7-23:</b>	Configuration Screens for the Radius or TACACS+ Authentication Servers .....	409
<b>Table 7-24:</b>	Smb (NTLM) Configuration Screens.....	409
<b>Table 7-25:</b>	NIS Configuration Screens.....	410
<b>Table 7-26:</b>	Save/Load Configuration Screens .....	412
<b>Table 7-27:</b>	System Information Example.....	414
<b>Table A-1:</b>	Boot Partitions, Formats, and Contents.....	421
<b>Table B-1:</b>	Technical Specifications.....	429





# List of Procedures

▼ To Mount the KVM/net Plus .....	76
▼ To Make an Ethernet Connection .....	79
▼ To Prepare to Connect Servers to the KVM/net Plus .....	81
▼ To Connect Computers to KVM Ports .....	82
▼ To Connect to the Console Port.....	84
▼ To Connect to the User 1 Management Port .....	85
▼ To Power On the KVM/net Plus.....	85
▼ To Power On Connected Devices.....	85
▼ To Log Into the KVM/net Plus Through the Console .....	87
▼ To Change the Password Through the Console.....	87
▼ To Use the wiz Command to Configure Network Parameters .....	88
▼ To Apply and Confirm the Network Parameters Defined Using the wiz Command.....	89
▼ To Log Into the OSD .....	91
▼ To Change a Password Using the OSD .....	92
▼ To Configure Network Parameters Using the OSD .....	94
▼ To Set the Time and Date Using the OSD.....	97
▼ Changing admin's Default Password [Web Manager] .....	100
▼ Changing the Root Password [Command Line] .....	100
▼ Changing Default Passwords [OSD] .....	101
▼ To Use the Default IP Address to Access the Web Manager .....	102
▼ To Use a Dynamic IP Address to Access the Web Manager .....	103
▼ To Preconfigure the KVM/net Plus .....	105
▼ To Set Up a Preconfigured KVM/net Plus .....	106
▼ To Prevent Mouse Conflicts [Windows XP/Windows 2003] .....	107
▼ To Prevent Mouse Conflicts [Windows 2000 / ME] .....	108
▼ To Prevent Mouse Conflicts [Windows 95/98/NT] .....	108
▼ To Prevent Mouse Conflicts [Linux].....	109
▼ To Modify IE Security Settings.....	110

- ▼ To Install a PCMCIA Card in the Front Card Slot ..... 114
- ▼ To Remove a PCMCIA Card from the Front Card Slot ..... 115
- ▼ To Connect an External Modem to an AUX Port ..... 116
- ▼ To Connect a PM to the AUX 1 Port..... 117
- ▼ To Connect Multiple PMs to the KVM/net Plus ..... 118
- ▼ To Mount the KVM Expander..... 122
- ▼ To Power On the KVM Expander ..... 125
- ▼ To Power On Devices Daisy Chained to the KVM Expander's  
Power Outlet ..... 125
- ▼ To Power On KVM-connected Devices ..... 125
- ▼ To Connect a Secondary KVM, KVM/net, or KVM/net Plus to  
the Primary KVM/net Plus ..... 127
- ▼ To Connect a KVM Expander to the Primary KVM/net Plus ..... 128
- ▼ To Connect the RP to the KVM/net Plus ..... 131
- ▼ To Connect the RP to a Dedicated Keyboard, Monitor, and Mouse ..... 131
- ▼ To Connect the RP to the Local Work Station ..... 132
- ▼ To Power On the KVM RP..... 132
- ▼ To Log Into the Web Manager as Admin..... 138
- ▼ To Save Configuration Changes..... 140
- ▼ To Change Network Settings [Wizard] ..... 143
- ▼ To Add a User [Wizard] ..... 145
- ▼ To Delete a User [Wizard]..... 147
- ▼ To Change a Password [Wizard] ..... 147
- ▼ To Add a Syslog Server [Wizard] ..... 150
- ▼ To Delete a Syslog Server [Wizard]..... 150
- ▼ To View Status, Lock, Unlock, and Cycle Power Outlets ..... 156
- ▼ To View and Reset IPDU Information ..... 157
- ▼ To Configure Users to Manage Specific Power Outlets..... 158
- ▼ To Specify or Change the Alias of an IPDU ..... 159
- ▼ To Configure Creation of Alarms and Syslog Files for IPDUs..... 160
- ▼ To Upgrade Firmware on an AlterPath PM..... 161
- ▼ To Enable Direct Access to KVM Ports..... 165
- ▼ To Redefine KVM Session Keyboard Shortcuts ..... 166
- ▼ To Specify an Authentication Method for KVM Port Logins ..... 167
- ▼ To Configure Local User 1 and User 2 Sessions ..... 171

▼ To Configure IP User (KVM Over IP) Sessions .....	172
▼ To Configure a KVM Port for Power Management .....	174
▼ To Specify or Change the Alias for a KVM Port .....	176
▼ To Enable or Disable a KVM Port .....	176
▼ To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net Plus .....	178
▼ To Edit the Configuration of a Cascaded KVM Unit .....	179
▼ To Delete the Configuration of a Cascaded KVM Unit .....	181
▼ To Add a User [Expert] .....	182
▼ To Delete a User or Group [Expert] .....	184
▼ To Change a User's Password [Expert].....	184
▼ To Add a Group.....	184
▼ To Modify a Group.....	185
▼ To Select Users and Groups for Assigning KVM Port Access .....	185
▼ To Assign KVM Port Access to a User or Group .....	186
▼ To Configure Encryption on Port Connections [Expert].....	190
▼ To Configure an Authentication Method for KVM/net Plus Logins.....	192
▼ To Configure an Authentication Method for Logins Through KVM Ports.....	193
▼ To Identify a Kerberos Authentication Server .....	195
▼ To Identify an LDAP Authentication Server.....	197
▼ To Configure an SMB(NTLM) Authentication Server .....	199
▼ To Configure a NIS Authentication Server .....	200
▼ To Identify a RADIUS Authentication Server .....	201
▼ To Identify a TACACS+ Authentication Server .....	202
▼ To Add or Modify an In-band (RDP) Server .....	205
▼ To Delete an In-band (RDP) Server .....	208
▼ To Configure Host Settings [Expert].....	212
▼ To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert] .....	215
▼ To Configure a Modem Card.....	216
▼ To Eject a PCMCIA Card From the Card Slot.....	219
▼ To Select the Daemons Used for Incoming Connections.....	221
▼ To Add a Chain.....	229
▼ To Edit a Chain.....	229

- ▼ To Edit a Rule for IP Filtering..... 230
- ▼ To Add a Packet Filtering Rule ..... 231
- ▼ To Add a Chain for IP Filtering..... 231
- ▼ To Edit A Chain for IP Filtering..... 233
- ▼ To Add a Rule for IP Filtering..... 233
- ▼ To Configure VPN..... 239
- ▼ To Configure SNMP..... 243
- ▼ To Configure Hosts ..... 246
- ▼ To Add, Edit, or Delete a Static Route ..... 248
- ▼ To Configure the AUX 1 Port for Use With a PM..... 251
- ▼ To Configure the AUX 2 Port for Use With an External Modem..... 251
- ▼ To Set the KVM/net Plus' Date and Time Manually ..... 254
- ▼ To Set The Time and Date With NTP ..... 255
- ▼ To Set the Time and Date to the KVM/net Plus' Local GMT ..... 255
- ▼ To Configure KVM/net Plus Boot..... 259
- ▼ To View General Information for Your KVM/net Plus ..... 260
- ▼ To View Port Status..... 261
- ▼ To Monitor the Temperature of Your KVM/net Plus..... 263
- ▼ To Back Up or Retrieve KVM/net Plus Configuration Data..... 270
- ▼ To Find the Cyclades Pathname for Firmware or Microcode Upgrades . 274
- ▼ To Upgrade Firmware ..... 275
- ▼ To Download Microcode From an FTP Server ..... 278
- ▼ To Reset the Microcode After Upgrade ..... 279
- ▼ To View Active Sessions Information..... 280
- ▼ To Kill an Active Session..... 281
- ▼ To Reboot the KVM/net Plus From a Remote Location ..... 282
- ▼ To Log Into the KVM/net Plus Web Manager as a Regular User..... 286
- ▼ To Change Your KVM/net Plus Password..... 289
- ▼ To Connect to Servers Through The Web Manager's  
Connect To Server Form ..... 304
- ▼ To Connect to a KVM Port Through the Web Manager Login Screen... 306
- ▼ To View Connected Port Information ..... 310
- ▼ To Connect to Another Port Using the Current AlterPath Viewer  
and Access Window Tab ..... 310
- ▼ To Cycle Between Ports ..... 311

▼ To Stop Cycling Between Ports.....	311
▼ To Connect to the Previous or Next Authorized Port Without Opening a New AlterPath Viewer .....	312
▼ To Adjust Screen Brightness and Contrast.....	313
▼ To Reset Your Keyboard and Mouse .....	314
▼ To Refresh the Information Displayed on the Access Window .....	314
▼ To Resume Your Port Connection After an Idle Timeout.....	315
▼ To Quit the Port Connection.....	315
▼ To Share a Server Connection .....	317
▼ To Power On, Power Off, or Reboot the Connected Server [KVM].....	318
▼ To Connect to Servers Through the OSD Connection Menu .....	321
▼ To Return to the Connection Menu After Connecting to a Port.....	325
▼ To View Connected Port Information .....	325
▼ To Initiate Cycle by Server.....	326
▼ To Connect to the Next Authorized Server from the Current Server .....	327
▼ To Connect to the Previous Authorized Server from the Current Server .....	327
▼ To Adjust Screen Brightness and Contrast.....	327
▼ To Reset the Keyboard and Mouse.....	328
▼ To Power On, Power Off, or Reboot the Connected Server.....	329
▼ To Close a KVM Connection .....	330
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets.....	337
▼ To Configure a PPP Connection on a Remote Computer .....	340
▼ To Make a PPP Connection From a Remote Computer .....	342
▼ To Set Up a Terminal Emulator Dial Up Connection .....	342
▼ To Dial Into the KVM/net Plus Using a Terminal Emulator .....	343
▼ To Log In to the KVM/net Plus Through the OSD .....	348
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets.....	350
▼ To Access System Information.....	415
▼ To reboot the KVM/net Plus .....	415
▼ To Use the AlterPath KVM RP to Access the KVM/net Plus .....	416
▼ To Switch the RP Video Display from the OSD to the Local Computer .....	417
▼ To Switch the RP Video Display from the Local Computer to the OSD .....	417

- ▼ To Turn the Beeper On or Off When Switching Between the  
Local and the Remote Work Stations ..... 418
- ▼ To Boot from an Alternate Image With bootconf ..... 423
- ▼ To Boot in U-Boot Monitor Mode ..... 425
- ▼ To Boot from an Alternate Image in U-Boot Monitor Mode ..... 425
- ▼ To Boot in Single User Mode from U-Boot Monitor Mode..... 426
- ▼ To Replace a Boot Image From a Network Boot in U-Boot  
Monitor Mode ..... 426
- ▼ To Restore the KVM/net Plus Configuration to the Factory Default..... 427

# Before You Begin

This installation, administration, and user's guide provides background information and procedures for installing, configuring, and administering the Cyclades™ AlterPath™ family of KVM products including:

- AlterPath KVM/net Plus
- AlterPath KVM Expander
- AlterPath KVM RP
- AlterPath KVM Terminators

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

## Audience

This manual is intended for installers and system administrators of the KVM/net Plus and for users who may be authorized to connect to devices and to manage power through the KVM/net Plus.

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

# Document Organization

This document contains the following chapters:

---

<b>Chapter 1: Introduction</b>	Defines and explains the overall product features and uses of AlterPath KVM/net Plus.
<b>Chapter 2: Installing the KVM/net Plus</b>	Explains the procedures for installing the KVM/net Plus and setting up its basic configuration.
<b>Chapter 3: Advanced Installation Procedures</b>	Explains the procedures for installing the KVM Expander and the KVM RP in addition to explaining how to install PCMCIA cards, an external modem, an AlterPath PM and how to cascade KVM units to the KVM/net Plus.
<b>Chapter 4: Web Manager for Administrators</b>	Explains how to use the Web Manager, highlighting such procedures as how to configure the KVM/net Plus, add or delete users, define user access, add or delete server connections, and other topics pertaining to KVM/net Plus administration.
<b>Chapter 5: Web Manager for Regular Users</b>	Presents the procedures for connecting to a port and other operations related to using the web user interface.
<b>Chapter 6: Accessing Connected Devices</b>	Explains how to connect to KVM ports and in-band servers and how to use the AlterPath Viewer and control KVM connection sessions.
<b>Chapter 7: On Screen Display</b>	Describes how to use the On Screen display for local connections to the User 1 port.
<b>Appendix A: Troubleshooting</b>	Explains how to troubleshoot common KVM/net Plus issues.
<b>Appendix B: Technical Specifications</b>	List the technical specifications for the KVM/net Plus.
<b>Glossary</b>	Glossary of terms and acronyms used in the manual.

---



## Related Documents

The following document for the Cyclades AlterPath KVM/net Plus is shipped with the product.

- *AlterPath KVM/net Plus QuickStart Guide* (hard-copy)

The following manuals for Cyclades AlterPath products mentioned in this guide are on the Documentation CD shipped with the product and they are also available at: <http://www.cyclades.com/support/downloads.php>.

- *AlterPath PM User Guide*
- *AlterPath Manager E2000 Manual*
- *AlterPath KVM/net Installation, Configuration, and Users Guide*
- *AlterPath KVM Installation, Configuration, and Users Guide*

Updated versions of this document will be posted on the downloads section of the Cyclades website in the “AlterPath KVM/net Plus” section when Cyclades releases new versions of the software.

A printed version of this document can be ordered under part number KVM0000-U02 through your Cyclades sales representative.

## Typographic and Other Conventions

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

**Table ii-1:** Typographic Conventions

Typeface	Meaning	Example
<a href="#">Links</a>	Hypertext links or URLs	Go to: <a href="http://www.cyclades.com">http://www.cyclades.com</a>
<i>Emphasis</i>	Titles, emphasized or new words or terms	See the <i>AlterPath KVM/net Plus Quick Start</i> .
Filename or Command	Names of commands, files, and directories; onscreen computer output.	Edit the <code>pslave.conf</code> file.

**Table ii-1:** Typographic Conventions

<b>Typeface</b>	<b>Meaning</b>	<b>Example</b>
<b>User type</b>	What you type in an example, compared to what the computer displays	[kvm #] <b>ifconfig eth0</b>

The following table describes other terms and conventions.

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

<b>Term or Convention</b>	<b>Meaning</b>	<b>Examples</b>
Hot keys	When hot keys are shown, a plus (+) appears between two keys that must be pressed at the same time, and a space appears between two keys that must be pressed sequentially.	Ctrl+k p entered while the user is connected to a KVM port brings up an IPDU power management screen. Ctrl and k must be pressed at the same time followed by p.
Navigation shortcuts	Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager forms or OSD screens.	Go to Configuration>KVM>General >IP Users in Expert mode.

# Chapter 1

## Introduction

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

## Description

The KVM/net Plus is a 1U rack-mountable device that serves as a single access point for administering and using servers and other devices through in-band and out-of-band access methods.

The following figure shows the front and back of the KVM/net Plus.



**Figure 1-1:** KVM/net Plus Front and Back

You can use the two PCMCIA card slots in the front for optional v.90 modem or secondary Ethernet PCMCIA cards.

You use the KVM ports on the left and middle back of the KVM/net Plus to connect servers. You can use the AUX ports on the right back to connect AlterPath PM IPDUs or an optional external modem. You use the management ports on the right back to connect to the KVM/net Plus and to its connected devices.

Depending on the model, the KVM/net Plus comes with either 16 or 32 KVM ports to connect from 16 to 32 servers with KVM connections.

The KVM/net Plus can be used to manage power of up to 128 devices when the devices are plugged into up to 32 daisy-chained AlterPath PM intelligent power distribution units that are connected to the AUX 1 port on the KVM/net Plus.

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

For extended local administration, administrators can connect the Cyclades AlterPath KVM Expander (purchased separately) to the KVM/net Plus with a CAT5 cable of up to 500 feet in length.

---

**Note:** The 500-foot limit includes the distance of the User 2 from the KVM/net Plus and the distance of the most remote system connected to a KVM port.

---

Secondary KVM units such as the Cyclades AlterPath KVM Expander or an AlterPath KVM can be cascaded for extended KVM server connections. A maximum of 32 secondary KVM devices can be cascaded from the primary KVM/net Plus extending the number of KVM ports to a maximum of 1024.

If multiple KVM/net Plus units are installed in multiple remote locations, a Cyclades AlterPath Manager (purchased separately) can manage all the KVM/net Plus units together with other Cyclades products and their connected devices through a single IP address.

Access to the KVM/net Plus for administration is separate from access to connected devices. Only the KVM/net Plus administrator can configure access to the KVM/net Plus and to the connected devices.

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

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

The KVM/net Plus administrator can further control access by controlling which ports are assigned to each user name.

The KVM/net Plus administrator can configure event logging, alarms, and notifications, set up encryption, and data buffering.

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

## What's New in KVM/net Plus

The KVM/net Plus supports the following new features:

- “Support for up to Ten Concurrent Users” on page 4
- “In-band Server Access” on page 4
- “Color OSD” on page 5
- “PCMCIA Card Slots” on page 6
- “LED Status” on page 6
- “Access Window for Managing Multiple Server Connections” on page 6
- “Temperature Monitor” on page 8
- “Enhanced Power Management for Cascaded Devices” on page 8
- “Enhanced Syslogging” on page 8

### ***Support for up to Ten Concurrent Users***

KVM/net Plus supports up to ten concurrent server connections including two local user connections and eight remote IP connections:

- Up to four KVM connections are allowed depending on the number of IP modules installed.
- Up to eight in-band connections are allowed; however, the number of allowable in-band connections decreases by one for each KVM connection being made.

See “Simultaneous Server Connections” on page 22 for more details about each type of user connection.

### ***In-band Server Access***

KVM/net Plus offers in-band connections to Windows Terminal Servers that have RDP enabled. With valid IP addresses, administrators can configure as many in-band connections as they can out-of-band KVM connections without using cables, a KVM port, or a KVM Terminator. However, if desired, dual KVM and in-band access can be configured for each Windows Terminal Server.

KVM/net Plus users can make up to eight server connections at once over the Ethernet or dial up (remote) in addition to making up to two simultaneous local KVM connections. Up to four of the remote connections can be KVM,

while the rest can be in-band, adding up to eight total remote connections. The following list describes the types and number of connections available to the KVM/net Plus:

- Up to eight in-band (RDP) connections OR
- Up to four KVM over IP connections plus the number of in-band connections that add up to eight when added to the number of active KVM over IP connections AND
- Local User 1 and Local User 2 connected, independently of KVM over IP and/or in-band connections

In-band connections have faster control response times than KVM connections, and there is no need to synchronize the keyboard and mouse.

The following links offer more detailed information on in-band connections:

- See “Server Access: In-band and Out of Band” on page 34 for a description of in-band and out-of-band server access.
- See “Configuring In-band (RDP) Servers” on page 203 for instructions on configuring RDP servers for in-band access.
- See Chapter 5. “Web Manager for Regular Users” on page 283 for instructions on making in-band server connections.

## Color OSD

In KVM/net Plus, the OSD uses multiple colors to enhance its usability. A selected option is highlighted in green.

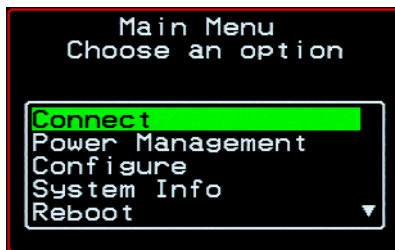


Figure 1-2: OSD Main Menu

## ***PCMCIA Card Slots***

Two PCMCIA card slots on the front of the KVM/net Plus support the optional connection of a modem card. The PCMCIA Management page allows you to configure a local user to login through an installed and configured modem card. In addition, when using PPP, you can enable callback.

The following links offer more detailed information on PCMCIA connections:

- See “PCMCIA Card Slots on the Front” on page 16 for more background information on the PCMCIA card slots.
- See “To Install a PCMCIA Card in the Front Card Slot” on page 114 for installation instructions.
- See “To Configure a Modem Card” on page 216 for configuration instructions.
- See “Modem Connections” on page 339 for instructions using the modem card to connect to the KVM/net Plus.

## ***LED Status***

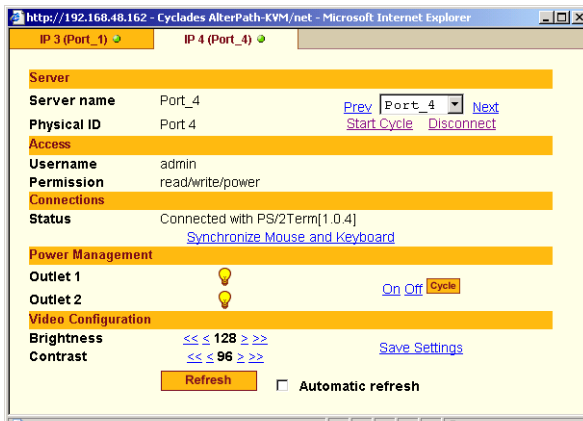
The LEDs (light emitting diodes) on the KVM/net Plus offer information on Ethernet activity, KVM and AUX port data flow, and the number of users accessing KVM ports over IP. See “Activity LEDs on the KVM/net Plus” on page 16 for a complete description of each LED.

## ***Access Window for Managing Multiple Server Connections***

Each time a user connects to a KVM port through the Web Manager, a new AlterPath Viewer is launched, and so is the Access Window, which is a separate pop-up window that contains four tabs—one for each active KVM connection. The tabs of the Access Window dynamically change status information and viewer event messages as the connection information changes.



As displayed in the following figure, users can cycle servers, control power, and set the brightness and contrast of their AlterPath Viewer all from one window.



**Figure 1-3:** Access Pop-up Window with Two Active Port Connections

A user can launch the access window without being connected to a KVM port by clicking the “Show Connections” link at the bottom of the Connect to Server form.



**Figure 1-4:** Show Connections Link on the Connect to Server form

For more information about the Access window, see “Managing Multiple Server Connections with the Access Window” on page 308.

## ***Temperature Monitor***

KVM/net Plus supports monitoring of three temperature sensors in the following locations:

- Power supply
- Fan
- FPGA (field programmable gate array)

Administrators and regular users with KVM/net Plus administration permissions can monitor the three temperature sensors on the KVM/net Plus with a graph displayed by the Web Manager.

For more information, see “Monitoring Temperatures” on page 56.

## ***Enhanced Power Management for Cascaded Devices***

The KVM/net Plus supports power management on devices connected to the AUX ports of cascaded KVM units. See “Power Management” on page 44 for more details.

## ***Enhanced Syslogging***

The KVM/net Plus supports configuring a syslog server to accept and store syslog messages from the AUX and KVM ports. See “Notifications, Alarms, and Data Buffering” on page 52 for more information.

## **Guidelines for Using the KVM/net Plus**

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

Troubleshooting in the event of network failure can be done using one of the two direct-connect methods, or by using the Web Manager through a dial-up connection to an external modem connected to the AUX 2 port or an optional PCMCIA card.

Optional: see “Installing PCMCIA Cards in the Front Card Slots” on page 114 for instructions on how to install PCMCIA cards. Also see “Modem

Connections” on page 339 for instructions on how to configure dial-up connections.

See “Accessing Connected Devices” on page 291 for instructions on how users without KVM/net Plus administration privileges can access computers and AlterPath PMs that are connected to the KVM/net Plus.

## Connectors on the KVM/net Plus

The following sections describe the connectors on the back and front of the KVM/net Plus, including ports, card slots, and plugs.

### *Types of Ports*

The KVM/net Plus’ ports include KVM ports, which support server connections, AUX ports, and management ports including the User 1, User 2, Console, and Ethernet ports, as described in the following table.

**Table 1-1:** Port Types

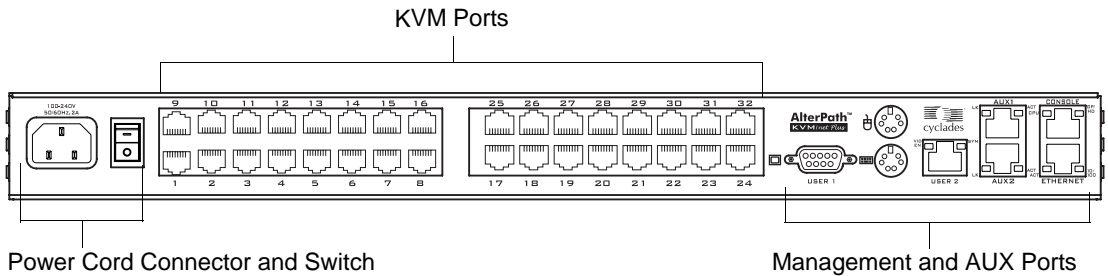
<b>Port Type</b>	<b>Connection Information</b>	<b>Where Documented</b>
KVM	Connect an RJ-45 CAT5 cable to a Terminator, which is connected to a PC with a USB or a PS/2 connector or a Sun server with a USB connector.	<ul style="list-style-type: none"> <li>• “KVM Ports” on page 12</li> <li>• “To Connect Computers to KVM Ports” on page 82</li> </ul>
AUX 1	Connect an RJ-45 cable to an: <ul style="list-style-type: none"> <li>• AlterPath PM intelligent power distribution unit (IPDU)</li> </ul> or <ul style="list-style-type: none"> <li>• external modem.</li> </ul>	<ul style="list-style-type: none"> <li>• “AUX Ports” on page 15</li> <li>• “To Connect a PM to the AUX 1 Port” on page 117</li> <li>• “To Connect an External Modem to an AUX Port” on page 116</li> </ul>
AUX 2	Connect an RJ-45 cable to an: <ul style="list-style-type: none"> <li>• external modem</li> <li>• CSU/DSU device</li> </ul>	<ul style="list-style-type: none"> <li>• “AUX Ports” on page 15</li> <li>• “To Connect an External Modem to an AUX Port” on page 116</li> </ul>

**Table 1-1: Port Types (Continued)**

Port Type	Connection Information	Where Documented
Console	Connect a CAT5 to DB-9 cable to a COM port on a computer.	<ul style="list-style-type: none"> <li>• “Management Ports (Console, Ethernet, User 1, User 2)” on page 13</li> <li>• “To Connect to the Console Port” on page 84</li> </ul>
Ethernet	Connect an Ethernet cable to the local area network (LAN).	<ul style="list-style-type: none"> <li>• “Management Ports (Console, Ethernet, User 1, User 2)” on page 13</li> <li>• “To Make an Ethernet Connection” on page 79</li> </ul>
User 1 [PS/2 and VGA]	Connect a keyboard, video, mouse cable to a local station’s keyboard, monitor, and mouse.	<ul style="list-style-type: none"> <li>• “Management Ports (Console, Ethernet, User 1, User 2)” on page 13</li> <li>• “To Connect to the User 1 Management Port” on page 85</li> </ul>
User 2	Connect an RJ-45 cable of up to 500 feet to an AlterPath KVM RP. The KVM RP can be ordered separately. <b>Note:</b> The 500-foot limit includes the distance of the User 2 from the KVM/net Plus and the distance of the most remote system connected to a KVM port.	<ul style="list-style-type: none"> <li>• “Management Ports (Console, Ethernet, User 1, User 2)” on page 13</li> <li>• “AlterPath KVM RP” on page 68</li> <li>• “To Connect the RP to the KVM/net Plus” on page 131</li> </ul>

## Connectors on the Back

The back of the KVM/net Plus has KVM and management ports, a power cord connector, a power switch, and AUX ports as illustrated in the following figure.



**Figure 1-5:** KVM/net Plus Back Panel

- On the left are the power connector and power switch and either 16 or 32 KVM ports, which are used for connecting computing systems with KVM connections.

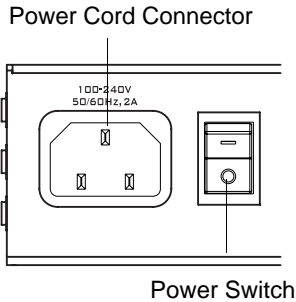
See “Power Connector and Power Switch” on page 12 and “KVM Ports” on page 12.

- On the right are the AUX ports, which are used to connect to PMs or an external modem, and the management ports, which are used for local management of the KVM/net Plus.

See “Management Ports (Console, Ethernet, User 1, User 2)” on page 13 and “AUX Ports” on page 15.

## ***Power Connector and Power Switch***

The following figure shows the power connector and power switch on the left rear of a KVM/net Plus.



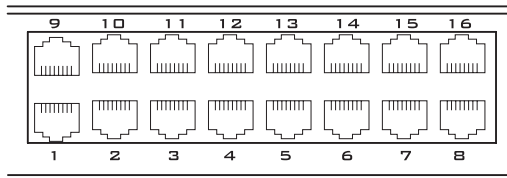
**Figure 1-6:** Power Connector and KVM Server Ports on the Left Rear

The KVM/net Plus is furnished with a power cord used to connect the power connector to a power supply.

See “To Power On the KVM/net Plus” on page 85 for instructions on supplying power to the KVM/net Plus.

## ***KVM Ports***

The following figure shows KVM (keyboard, video, mouse) ports on the center rear of the KVM/net Plus.



**Figure 1-7:** KVM Ports on the Center Rear

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

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

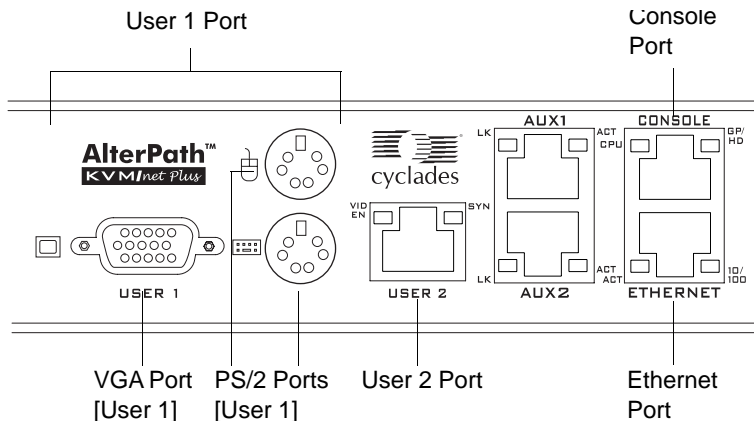
Each connected computing system is identified in the management software by the port number to which it is connected. The administrator can assign a descriptive alias to each port to identify the connected computer. For example, if a Sun E10K server is connected to port 3, the administrator might define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

Customers order one of three Terminator types for connecting each KVM port to a computer. See "KVM Terminator Usage and Types" on page 58 for more details.

See "To Connect Computers to KVM Ports" on page 82 for instructions on connecting servers to KVM ports.

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

The following figure shows the management ports on the right back of the KVM/net Plus.



**Figure 1-8: Management Ports**

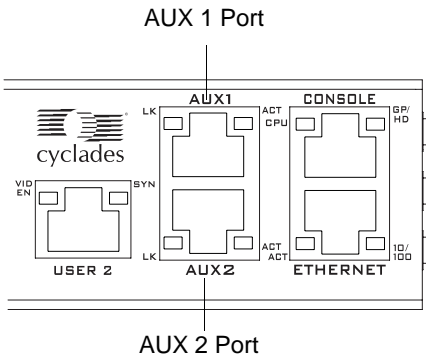
The following list describes the management ports on the right back of the KVM/net Plus.

- **Console** – Its RJ-45 connection can be connected by a CAT5 to DB-9 cable to a COM port on a computer. Administrators can use a terminal emulation program to locally manage and troubleshoot the KVM/net Plus. See “To Connect to the Console Port” on page 84 and “Configuring Basic Networking Using the wiz Command” on page 87 for more details.
- **Ethernet** – Use the Ethernet management port for connecting an Ethernet cable for Intranet and Internet access. See “Making an Ethernet Connection” on page 79 for instructions if needed.
- **User 1** – The User 1 port includes two PS/2 ports and a VGA port, which can be connected to a mouse, keyboard, and monitor. Once a local system is connected to the User 1 port, administrators can use the OSD (On Screen Display) interface to locally manage and use the KVM/net Plus. See “To Connect to the User 1 Management Port” on page 85 and Chapter 7: On Screen Display for more details.
- **User 2** – This port is used for extending the local administration by connecting an RJ-45 cable of up to 500 feet to an AlterPath KVM RP. The RP can be ordered separately. Administrators can use the OSD (On Screen Display) to locally manage and use the KVM/net Plus without being in the same room as the KVM/net Plus. See “Installing the AlterPath KVM RP” on page 129 and “Controlling the OSD Through the AlterPath KVM RP” on page 418 for more details.



## AUX Ports

The following figure shows the AUX ports on the right back of the KVM/net Plus.



**Figure 1-9: AUX Ports**

- **AUX 1** – Its RJ-45 connector can be used for connecting to an optional AlterPath PM IPDU. Up to 32 IPDUs can be daisy-chained for a total of 128 outlets.

See “Power Management” on page 44 for background information on power management and see “Connecting AlterPath PMs to the KVM/net Plus” on page 117 for installation instructions.

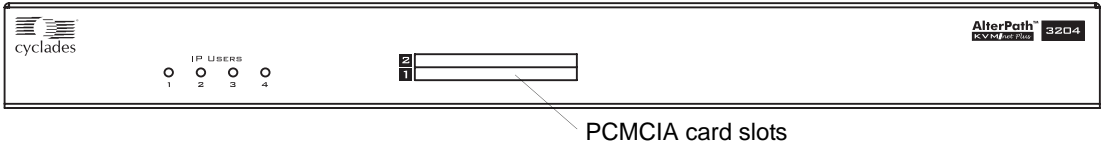
- **AUX 2** – Its RJ-45 connector can be used for connecting to an optional external modem.

See “Connecting an External Modem” on page 116

The user on a remote computer initiates a PPP dial-up session through the modem to access the KVM/net Plus. See “Modem Connections” on page 339 for more details.

## ***PCMCIA Card Slots on the Front***

The front of the KVM/net Plus has PCMCIA card slots that provide additional management options.



**Figure 1-10:**PCMCIA Card Slots on Front of the AlterPath KVM/net Plus

See “Installing PCMCIA Cards in the Front Card Slots” on page 114 for installation instructions.

## **Activity LEDs on the KVM/net Plus**

Activity LEDs (light emitting diodes) are located on the front and back panels of the KVM/net Plus. The following sections explain how these LEDs light up or flash at different intervals to indicate the status of varied KVM/net Plus features:

- “Activity LEDs on the Management and AUX Ports” on page 16
- “Front Panel Activity LEDs” on page 18

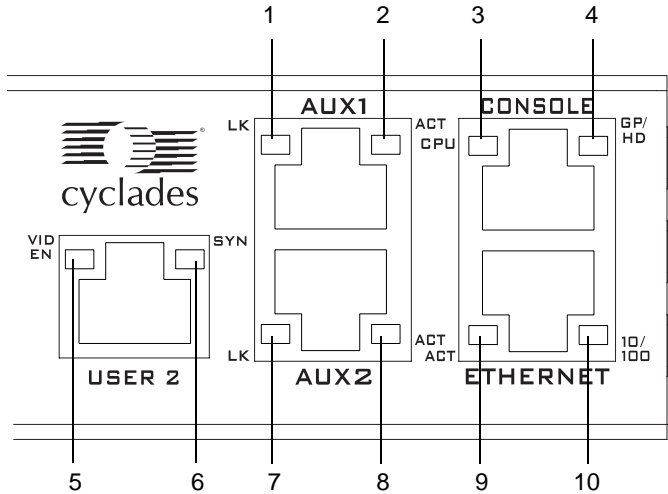
## ***Activity LEDs on the Management and AUX Ports***

The KVM/net Plus unit comes with paired LEDs positioned on each side of the following ports:

- User 2
- AUX 1
- AUX 2
- Ethernet
- Console

The following figure shows the position of the LEDs as they appear on the back of the KVM/net Plus. The LEDs are designed to monitor the interface

connections as described in Table 1-2, “Management Port LED Status Definitions,” on page 17.



**Figure 1-11:**LEDs on the KVM/net Plus Management Ports

The LED numbers in the table below correspond to the numbers in the previous diagram.

**Table 1-2:** Management Port LED Status Definitions

LED No.	Label	Function	Color/Status
1,7	LK	Monitor RS-232 async port status	<ul style="list-style-type: none"> <li>• Orange – Lights when DTR (data terminal ready) signal is on (when port is open).</li> <li>• Off – Indicates the port is not open.</li> </ul>
2,8	ACT	Monitor RS-232 async activity	<ul style="list-style-type: none"> <li>• Green – Blinks when data is either being received (RX) or transmitted (TX).</li> <li>• Off – Indicates no data activity.</li> </ul>

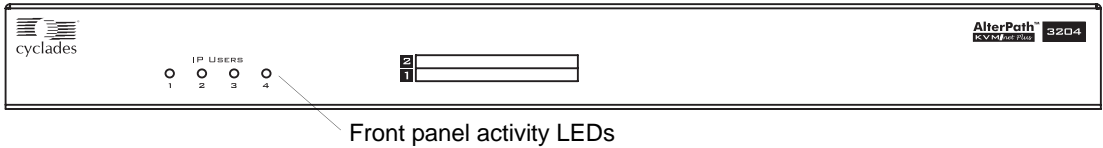
**Table 1-2: Management Port LED Status Definitions (Continued)**

LED No.	Label	Function	Color/Status
3	CPU	Monitor CPU	<ul style="list-style-type: none"> <li>• Green and Orange – Blinks alternating between green and orange when software is operating normally.</li> <li>• Off – During boot up and if software crashes. If the Watchdog timer is active, the KVM/net Plus reboots.</li> </ul>
4	GP/ HD	Monitor compact flash (HD) or other (GP)	Orange – Blinks when data activity occurs in compact flash.
5	VID EN	Monitor KVM CAT5 video interface	Green – Lights when video signal is present.
6	SYN	Monitor KVM CAT5 video interface	Yellow – Lights when KVM input is being transmitted through one or more KVM ports.
9	ACT	Monitor Ethernet line activity	<ul style="list-style-type: none"> <li>• Green – Lights solid when data activity occurs.</li> <li>• Off – Indicates no activity.</li> </ul>
10	10/100	Monitor Ethernet speed and link	<ul style="list-style-type: none"> <li>• Green – Lights when set to operate at 100 Mb/s and there is link.</li> <li>• Orange – Lights when set to operate at 10 Mb/s and there is link.</li> <li>• Off – Indicates no link.</li> </ul>

## ***Front Panel Activity LEDs***

The four activity LEDs on the front panel of the KVM/net Plus light at boot time to indicate the number of KVM over IP (KVM/IP) modules installed on the KVM/net Plus and blink to indicate the number of IP users simultaneously logged into the Web Manager.

The number of IP modules installed indicates the number of IP users that are able to access the Web Manager at one time. The KVM/net Plus is furnished with up to four KVM/IP modules installed; however, the actual number of IP modules depends on the model ordered. See “AlterPath KVM/net Plus Ordering Options” on page 19.



**Figure 1-12:**Activity LEDs on the Front of the KVM/net Plus

**Note:** If a KVM/net Plus is furnished with fewer than four IP modules, one or more of the LEDs does not light. For example, if a KVM/net Plus is furnished with two IP modules, they could be installed in slots 1 and 3. Then LEDs 1 and 3 light when the KVM/net Plus is booted up, and LEDs 1 and 3 blink when a user logs into the Web Manager, while LEDs 2 and 4 never light.

## AlterPath KVM/net Plus Ordering Options

Each AlterPath KVM/net Plus comes with one, two, or four IP module that support one, two, or four connections over the network. The following table shows the model numbers with the various numbers of IP modules and numbers of KVM ports.

**Table 1-3:** Model Numbers and Configuration Options

Model Number	Part Number	IP Modules	KVM Ports
1601	ATP1601	1	16
1602	ATP1602	2	16
1604	ATP1604	4	16
3201	ATP3201	1	32
3202	ATP3202	2	32
3204	ATP3404	4	32

## Types of Users

The KVM/net Plus supports three types of users:

- Predefined administrators who can administer the KVM/net Plus and its connected devices
- Optionally added users who can act as administrators of the KVM/net Plus and its connected devices
- Optionally added users who can act as administrators of connected devices or regular users.

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

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

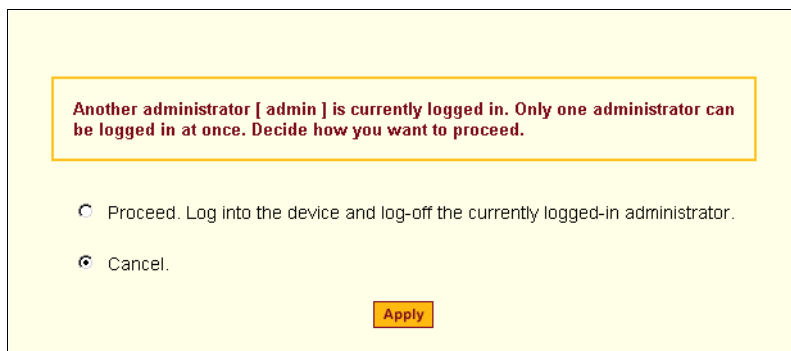
User Name	Responsibilities	Default Password
root	Cannot be deleted. Only console logins allowed. Runs the <code>wiz</code> command to do initial network configuration, as described in “Configuring Basic Networking Using the <code>wiz</code> Command” on page 87. Access Privileges: Full Read/Write/Delete.	cyclades
admin	Cannot be deleted. Has all access: through the Web Manager in Wizard and Expert mode, and through the OSD. Has full access to every function of the Web Manager. Access Privileges: Full Read/Write/Delete.	cyclades

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

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

## Simultaneous KVM/net Plus Logins

Only one KVM/net Plus administrator can be logged in at a time. If a second administrative user attempts to log into the Web Manager, the following prompt appears offering a choice of cancelling the attempt to log in or terminating the other administrator’s login session.

**Figure 1-13:** Simultaneous Administrator Login Prompt

## Simultaneous Server Connections

The KVM/net Plus supports a maximum of 10 concurrent server connections. Up to two local connections are always supported. However, the number of simultaneous IP user connections depends on the number of IP modules installed on the KVM/net Plus. The types of user connections that can be made are explained below:

- Local users include:
  - One local user at the KVM/net Plus (User 1).
  - One extended user at the AlterPath KVM RP location (User 2).
- IP users include:
  - KVM – The KVM/net Plus supports up to four concurrent KVM over IP connections depending on the number of IP cards installed in the specific unit. The KVM/net Plus can come with one IP card, two, IP cards, or four IP cards installed.
  - In-band – KVM/net Plus supports up to eight concurrent in-band connections depending on the number of KVM connections being made. Since the maximum total IP connections is eight, if four KVM connections are being made at one time, only four in-band connections can be made at that time.

Table 1-5 lists the number of users who can simultaneously connect to servers with various connection methods based on the number of IP modules installed in the KVM unit.

**Table 1-5: Server Connection Types Available on the KVM/net Plus**

<b>Users</b>	<b>One Active IP Module</b>	<b>Two Active IP Modules</b>	<b>Four Active IP Modules</b>
<b>Local KVM</b>	2	2	2
<b>KVM over IP</b>	1	2	4
<b>In-band</b>	7	6	4
<b>Total</b>	10	10	10

See “AlterPath KVM/net Plus Ordering Options” on page 19 for a table that shows the number of IP modules in each KVM/net Plus model.



# Administration Options

The following sections summarize the KVM/net Plus administration options:

- “Cyclades Web Manager” on page 23
- “On-Screen Display” on page 23
- “Linux Commands and KVM/net Plus-specific Commands” on page 24

The administrator options require different types of log in credentials. For more information on which types of users can perform administrative tasks and access administrative options, see “Types of Users” on page 20.

**Table 1-6:** Administration Options

<b>Cyclades Web Manager</b>	<p>The Web Manager is the primary means of configuring the KVM/net Plus and administering its connected devices.</p> <ul style="list-style-type: none"> <li>• See “Prerequisites for Using the Web Manager” on page 25 for an introduction that includes prerequisites for using the Web Manager and explanations about how the different types of user accounts use the Web Manager.</li> <li>• See “Web Manager for Administrators” on page 133 for more details about how KVM/net Plus administrators use the Web Manager.</li> </ul>
<b>On-Screen Display</b>	<p>The On Screen Display (OSD) can be used locally from a keyboard, monitor and mouse that is directly connected to the KVM/net Plus. When the monitor and the KVM/net Plus are on, the OSD login screen appears on the monitor.</p> <ul style="list-style-type: none"> <li>• See “To Connect to the User 1 Management Port” on page 85 for instructions on how to make the hardware connection.</li> <li>• See “On Screen Display” on page 345 for how KVM/net Plus administrators and regular users can use the OSD.</li> </ul>

**Table 1-6: Administration Options (Continued)**

<b>Linux Commands and KVM/net Plus-specific Commands</b>	<p>The KVM/net Plus offers the following types of access allowing administrators to log in and enter Linux commands and KVM/net Plus-specific commands in a shell running on the KVM/net Plus:</p> <ul style="list-style-type: none"> <li>• A local administrator who has a direct connection to the console port on the KVM/net Plus, who is running a terminal or terminal emulation program, and who knows the root password. The direct login requires authentication using the root password. The default shell defined for the root user is bash.</li> <li>• A remote administrator who uses telnet or ssh to connect to the KVM/net Plus and log in as root.</li> </ul> <p>See “To Connect to the Console Port” on page 84 and “Configuring Basic Networking Using the wiz Command” on page 87.</p>
--	--

## Cyclades Web Manager

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

Web Manager uses forms and dialog boxes (which are pop-up windows) to receive data input. See also, “Prerequisites for Using the Web Manager” on page 25.

Administrators, see “Web Manager for Administrators” on page 133. Regular users, see “Web Manager for Regular Users” on page 283.

# Prerequisites for Using the Web Manager

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

- An administrator needs to define basic network parameters on the KVM/net Plus so the Web Manager can be launched over the network.

See “Configuring Basic Networking Using the wiz Command” on page 87 for instructions on how to define network parameters on the KVM/net Plus.

The administrator also needs the following to be able to connect to the KVM/net Plus through the Web Manager:

- A networked Windows computer that has access to the network where the KVM/net Plus is installed.
- A supported browser (see Table 1-7).

## **Table 1-7: Supported Browsers**

---

Internet Explore 5, 6

Netscape 7

Mozilla

Firefox

---

- The IP address of the KVM/net Plus.

Entering the IP address of the KVM/net Plus in the address field of one of the supported browsers listed in Table 1-7 is the first step required to access the Web Manager.

When DHCP is enabled, a device's IP address may change each time the KVM/net Plus is booted up. Anyone wanting to access the KVM/net Plus must find out the currently assigned IP address. If DHCP is enabled and you do not know how to find out the current IP address of the KVM/net Plus, contact your system administrator for help. For more information,

see “Considerations When Choosing Whether to Enable DHCP” on page 55.

- A user account defined on the Web Manager

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

## TCP Ports

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

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

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

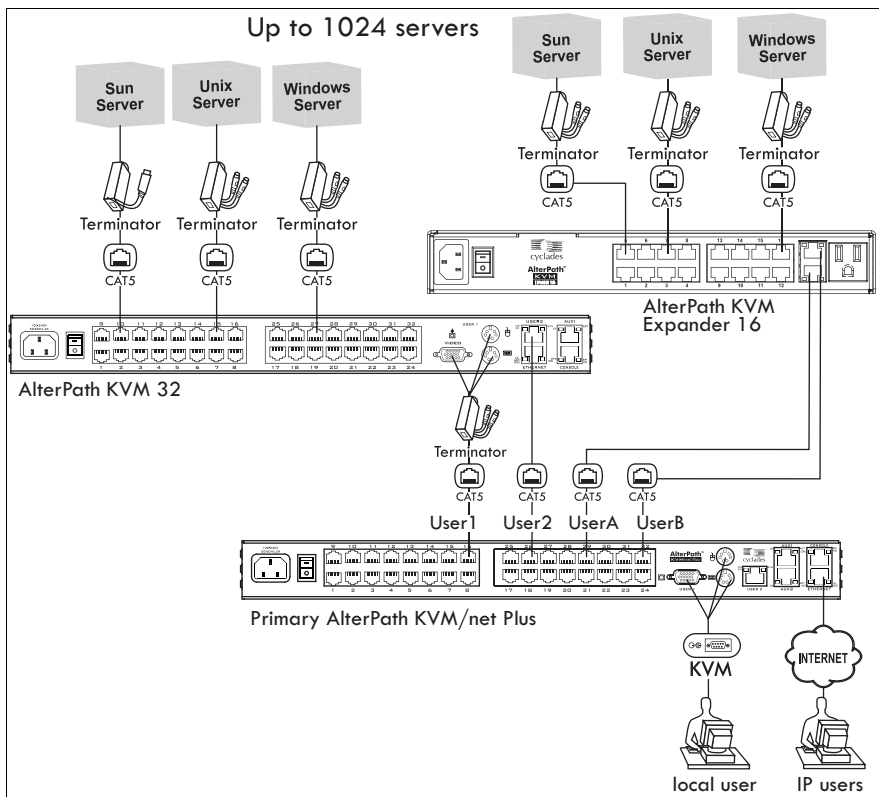
**Table 1-8:** Tasks: Configuring TCP Port Numbers

<b>Task</b>	<b>Where Described</b>
Change the TCP port number(s) assigned to the AlterPath Viewer(s)	“To Configure IP User (KVM Over IP) Sessions” on page 172
Change the TCP port number(s) assigned to in-band connections	“To Add or Modify an In-band (RDP) Server” on page 205

# Cascaded Devices

The KVM/net Plus supports cascading, which allows administrators to connect secondary KVM units to a primary KVM/net Plus. Cascading allows administrators to increase the number of managed devices to up to 1024 servers with a centralized configuration and access interface.

The following diagram depicts a basic cascaded configuration of a primary KVM/net Plus with 32 ports and one KVM and one KVM Expander cascaded from it.



**Figure 1-14:** Cascaded KVM Devices from an KVM/net Plus

As depicted in the previous figure, the KVM/net Plus supports one level of cascading: The primary KVM/net Plus controls the secondary level of KVM units connected to it. A secondary KVM unit can be a KVM, a KVM Expander, a KVM/net, or a KVM/net Plus.

Administrators can connect up to 32 KVM units to the master KVM/net Plus. Each cascaded KVM device has two management ports that can be connected to the primary KVM/net Plus. You can connect any one of the master KVM/net Plus' KVM ports to either the User 1 or User 2 management ports on the cascaded KVM or to the User A or User B management ports on the KVM Expander. The following table indicates which ports on each cascaded device can be used for cascading and which cables need to be used in order to connect them.

**Table 1-9: Connectors and Ports for Cascading KVM Units**

<b>KVM Unit</b>	<b>Management Ports</b>	<b>Connectors</b>
<b>KVM Expander</b>	User A, User B	CAT5 cable
<b>KVM</b>	User 1, User 2	CAT5 cable KVM Terminator (User1)
<b>AlterPath KVM/net</b>	User 1, User 2	CAT5 cable KVM Terminator (User1)
<b>KVM/net Plus</b>	User 1, User 2	CAT5 cable KVM Terminator (User1)

**Note:** In addition to a CAT5 cable, you need a KVM Terminator to connect to the User 1 port of a cascaded KVM/net Plus, KVM/net, or KVM.

## Accessing Ports on Cascaded KVM Devices

KVM/net Plus users can use the master KVM/net Plus to access all devices connected to KVM ports on the master and primary KVM units. However, only two port connections can be made to each cascaded unit at any time. Each physical port connection (for example to User 1 or User B) to the cascaded KVM devices allows a user to connect to one KVM port on the secondary KVM unit. So any user can connect to up to two KVM ports on a cascaded device at any time.

## KVM/net Plus Port Permissions

In the default configuration, only the “admin” and “root” users can access any ports. The KVM/net Plus administrator configures access for regular users as desired.

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

**Table 1-10:**Default Port Access Permissions

Default Access	Default Auth Type	Access Types	Where Documented
None	Local	No access Read only Read/Write Full access (Read/ Write/Power management)	“Understanding KVM Port Permissions” on page 30 “To Assign KVM Port Access to a User or Group” on page 186

The KVM/net Plus administrator must take the actions described under “Where Documented” to allow any other types of access than the defaults defined in the previous table. See “Authentication” on page 48 for the tasks related to setting up authentication.

## ***Understanding KVM Port Permissions***

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

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

For individual users and groups, if desired, the KVM/net Plus administrator can construct lists of KVM ports with the following types of permissions:

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

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

To allow users to access KVM ports, the KVM/net Plus administrator must do one or both of the following:

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

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

The KVM/net Plus administrator can specify different Default Permissions or KVM port permissions for any user or group. “KVM Port Permissions Hierarchy” on page 31 provides information that the KVM/net Plus administrator needs to understand in order to perform advanced configuration of KVM permissions.



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

**Table 1-11: Tools for Setting KVM Port Permissions**

<b>Tools</b>	<b>Where Documented</b>
Web Manager	“To Assign KVM Port Access to a User or Group” on page 186
OSD	“KVM Ports Screens” on page 386

## ***KVM Port Permissions Hierarchy***

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

### ***Decision 1: Check User’s KVM Port Permissions***

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

#### ***Example for Decision 1***

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

### ***Decision 2: Check Group's KVM Port Permissions***

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

---

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

---

#### ***Example for Decision 2***

- If user jim is trying to access port 4 and he is a member of a group called linux\_ca2 that has port 4 in a list of ports with read/write permissions, then jim is given read/write access.
- If user joan is trying to access port 4 and she is in a group called linux\_ca3 that has port 4 in a list of ports with no permission, then joan is denied access.
- If jerry and jill are trying to access port 4 and are in a group called linux\_ca4 that has no specific port permissions defined, then their access requests are passed to decision 3.
- If joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and are not in any group, then their access requests are passed to decision 3.

### ***Decision 3: Check Generic User's KVM Port Permissions***

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

#### ***Example for Decision 3***

- If user jerry is trying to access port 4 and the Generic User has port 4 in a list of ports with full access permissions, then jerry is given read writer and power management access.
- If user jill is trying to access port 4 and the Generic User has port 4 in a list of ports with no access permissions, then jill is denied access.

- If users joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and the Generic User does not have port 4 listed for any type of access, then their access request are passed to decision 4.

#### ***Decision 4: Check User's Default Permissions***

4. Does the user have a Default Permission that allows or denies access to the port?
  - If yes, access is allowed or denied.
  - If the user has no Default Permission, the user is under the Generic User's default permission, and the request for access goes to decision 5.

#### ***Example for Decision 4***

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

#### ***Decision 5: Check Group's Default Permissions***

5. Does the user belong to a group that has a Default Permission that allows or denies access to the port?
  - If yes, permission is granted or denied.
  - If no, go to decision 6.

#### ***Example for Decision 4***

- If user jordan trying to access port 4 is in a group called windows\_ca1 that has a Default Permission of full, then jordan is given read/write and power management access.
- If user jolanda trying to access port 4 is in a group called windows\_ca2 that has a Default Permission of no access, then jolanda is denied access.
- If user jennifer is not a member of any group with a Default Permission specified, then her access request is passed to decision 6.

## **Decision 6: Check Generic User's Default Permissions**

---

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

---

6. Does the Default Permission for the Generic User allow access to the port?
- If yes, access is granted.
  - If no, access is denied.

## **Server Access: In-band and Out of Band**

KVM/net Plus users can access servers over the Ethernet using the following methods:

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

The differences between the in-band and out-of-band connection methods are briefly described in the following table. For a more detailed description of the requirements and functionality of each connection method, see the following section, “Determining the Connection Type and its Supported Functionality” on page 36.

**Table 1-12:**In-band and Out of Band Connections

	<b>In-band</b>	<b>Out-of-Band</b>
<b>Connection Type</b>	Remote Desktop Protocol (RDP) over the Ethernet or PPP	Keyboard, video, mouse (KVM) CAT5 connection to a KVM/net Plus and Ethernet or PPP access to the KVM/net Plus Web Manager
<b>Supported Source Computers</b>	Client machine running a Windows operating system with a valid IP address	All Windows clients

**Table 1-12:**In-band and Out of Band Connections

	<b>In-band</b>	<b>Out-of-Band</b>
<b>Supported Target Servers</b>	Windows (Win2000, 2003, XP, and NT) Terminal Servers	PCs with a USB or PS/2 connectors or Sun servers with USB connectors
<b>Supported Browsers</b>	Internet Explorer 5, 6	Internet Explorer 6, Netscape 7, Mozilla, Firefox
<b>Direct Log In</b>	Not available	Available if configured by the KVM/net Plus administrator See “To Enable Direct Access to KVM Ports” on page 165.
<b>Power Management While Connected</b>	Not available	Available if configured by the KVM/net Plus administrator and if the server is plugged into an AlterPath PM IPDU that is connected to the KVM/net Plus. See “Power Management” on page 44.
<b>Viewer</b>	ActiveX viewer See “Viewing In-band Connections” on page 296	AlterPath Viewer See “Viewing KVM Connections” on page 294.

## ***Determining the Connection Type and its Supported Functionality***

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

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

**Table 1-13:** Available Functionality During KVM and In-band Connections

<b>Server Connection Labels</b>	<b>Description</b>
<b>(KVM)</b>	<p>Indicates that the server can be accessed only through an out-of-band, KVM connection.</p> <p>This server is connected to a KVM port on the KVM/net Plus or on a cascaded KVM unit.</p> <p>Users can control all applications on the server, have BIOS access, and can view POST, and boot messages. Users can access this server even when the network is down or after a system boot is completed.</p> <p>Users can also control the power flow on this server if the server is plugged into an AlterPath PM IPDU and the port is properly configured for power management.</p>
<b>(Inband)</b>	<p>Indicates that the Microsoft Terminal Server running RDP can be accessed only through an in-band connection and is not connected to a KVM port.</p> <p>Users can access this server only to run applications once the server is already running. The performance on in-band connections is slightly better than that of KVM connections, and no synchronization of keyboard and mouse is necessary.</p>

**Table 1-13:** Available Functionality During KVM and In-band Connections (Continued)

Server Connection Labels	Description
<b>(KVM + Inband)</b>	<p>Indicates that the server can be accessed through in-band and out-of-band (KVM) connections.</p> <p>The first time users select this server from the Connect drop-down list, an in-band connection is attempted. The connection automatically switches to KVM only if the in-band connection fails or if an in-band connection to this server already exists. Users who want to access this server with a KVM connection, must do one of the following:</p> <ul style="list-style-type: none"> <li>• Make two connection attempts to the same server from the Web Manager Connect to Server form.</li> </ul> <p>The first connection is an in-band connection viewed through an ActiveX viewer. The second connection is a KVM connection viewed through the AlterPath Viewer.</p> <p>See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 304.</p> <ul style="list-style-type: none"> <li>• Make a direct login to the KVM port.</li> </ul> <p>See “Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 301 and “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 302 for more information.</p>

# Administering Users of Connected Servers

This section reviews the tasks that KVM/net Plus administrators must do to enable access to connected servers.

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

## *Types of Access to Ports*

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

- Read only
- Read write
- Read write power

---

**Note:** The KVM/net Plus offers access privileges to KVM ports only. In-band connections are authenticated, and the access privileges are granted on the in-band server itself.

---

## *Tasks Related to Access to Connected Devices*

Planning should include the following steps:

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



During setup of the KVM/net Plus, the installer connects the desired servers to the ports as planned.

During configuration, the KVM/net Plus administrator does the following, if desired:

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

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

<b>Task</b>	<b>Where documented</b>
Specify an alias for a KVM port.	• “To Specify or Change the Alias for a KVM Port” on page 176
Specify an alias for a PM.	• “To Specify or Change the Alias of an IPDU” on page 159
Assign permissions to access ports.	• “To Assign KVM Port Access to a User or Group” on page 186
Assign permissions to IPDUs and outlets.	• “To Configure Users to Manage Specific Power Outlets” on page 158

## Redefining Keyboard Shortcuts (Hot Keys)

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

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

If desired, the KVM/net Plus administrator can redefine the default hot keys either through the Web Manager or the OSD.

### ***Redefining KVM Connection Hot Keys***

The hot key sequences used while connected to KVM ports have two parts, which are called the *common escape sequence* and the *command key*. The default common escape sequence is `Ctrl+k`, and the command key is different for each command. For example, the `q` command key is entered after `Ctrl+k` to quit the login session as shown here: `Ctrl+k q`. See “Hot Keys for Local” on page 323 for the defaults. Under `Configure>KVM` in the Web Manager, the common escape sequence is defined separately from the command keys. The KVM/net Plus administrator can redefine two different sets of command keys for users accessing KVM ports through the OSD (User 1 or User 2) and another set for connections made through the Web Manager.

### ***Redefining Sun Keyboard Equivalent Hot Keys***

The KVM/net Plus provides a default set of hot keys for use while connected to Sun servers through KVM ports to emulate keys that are present on Sun keyboards but are not present on Windows keyboards. The hot keys are made up of an escape key followed by a function key. See “Hot Keys for Emulating Sun Keyboard Keys” on page 324 for more details. The default escape key is the Windows key, which is labeled with the Windows logo. KVM/net Plus administrators can redefine the Sun emulation escape key to be one of the following: `Ctrl`, `Shift`, or `Alt`.

## Summary of Tasks for Redefining Hot Keys

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

**Table 1-14:** Tasks for Redefining Hot Keys

<b>Part</b>	<b>Web Manager Form</b>	<b>Where Documented</b>	<b>OSD Form</b>	<b>Where Documented</b>
KVM Common escape sequence	Configuration> KVM>General > General	“To Redefine KVM Session Keyboard Shortcuts” on page 166	Configure> General	“General Configuration Screens [OSD]” on page 355
KVM Command keys for the local user session	Configuration> KVM>General >User 1 Configuration> KVM>General >User 2	“To Redefine KVM Session Keyboard Shortcuts” on page 166	Configure> User Station	“User Station Screens” on page 382
KVM Command keys for IP user sessions	Configuration> KVM>General >IP Users		N/A	
Sun keyboard emulation escape key	Configuration> KVM>General	“To Redefine KVM Session Keyboard Shortcuts” on page 166	Configure> General	“KVM Ports Screens” on page 386

## ***Packet Filtering on the KVM/net Plus***

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

The IP Filtering form is structured in two levels:

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

IP filtering refers to the selective blocking of the passage of IP packets between global and local networks. The filtering is based on rules that describe the characteristics of the packet (that is, the contents of the IP header, the input/output interface, or the protocol).

This feature is used mainly in firewall applications to filter the packets that could potentially crack the network system or generate unnecessary traffic in the network.

The following table describes the different levels of IP filtering

**Table 1-15:**Levels of IP Filtering

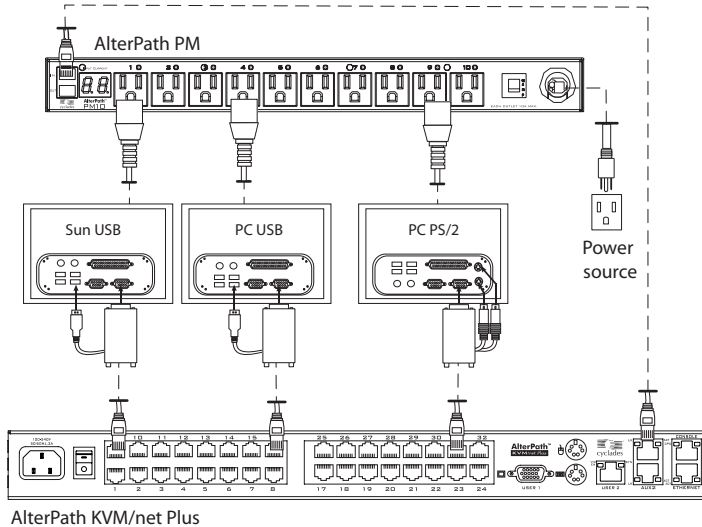
<b>Chain</b>	The filter table contains a number of built-in chains and may include user-defined chains. The built-in chains are called according to the type of packet. User-defined chains are called when a rule which is matched by the packet points to the chain. Each table has a set of built-in chains classified as follows: <ul style="list-style-type: none"><li>• INPUT - For packets coming into the box itself.</li><li>• FORWARD - For packets being routed through the box.</li><li>• OUTPUT - For locally generated packets.</li></ul>
--------------	--

**Table 1-15:** Levels of IP Filtering (Continued)

<b>Rule</b>	<p>Each chain contains a sequence of rules that control filtering. The rules address the following issues:</p> <ul style="list-style-type: none"> <li>• How the packet should appear in order to match the rule</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• What to do when the packet matches the rule</li> </ul> <p>The packet can be accepted, blocked, logged, or jumped to a user-defined chain.</p> <p>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.</p>
-------------	---

# Power Management

The KVM/net Plus enables users who have power management permissions to power off, power on, and reboot remote devices connected to an AlterPath PM intelligent power distribution unit (IPDU). By connecting one PM to the AUX 1 port and by daisy-chaining any combination of PM models, you can connect up to 128 outlets to one KVM/net Plus.



**Figure 1-15:** Connecting an AlterPath PM to the KVM/net Plus

See “Setting Up and Configuring Power Management” on page 46 for information about the procedures the KVM/net Plus administrator must perform before anyone can use the tools to manage power.

KVM/net Plus users most commonly perform power management through the Web Manager. See “Options for Managing Power” on page 44 for more information.

## Options for Managing Power

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

## ***Controlling Power Through the Web Manager IPDU Power Management Forms***

Through the Web Manager's IPDU Power Management form, users with power management permissions can perform power management on any device plugged into a PM connected to the AUX 1 port. See "Power Management for Regular Users" on page 288.

Administrators must configure users for IPDU power management. See "To Configure Users to Manage Specific Power Outlets" on page 158. Or see "Setting Up and Configuring Power Management" on page 46 for a list of all of the administration tasks involved in setting up power management.

## ***Controlling Power While Connected to KVM Ports***

Users who have power management permissions can do power management while connected to servers through KVM ports by using the Power Management options on the Access window or by using a keyboard shortcut that brings up a power management screen on the OSD for local users. The default keyboard shortcut while connected through the OSD is Ctrl+k p.

See "To Power On, Power Off, or Reboot the Connected Server [KVM]" on page 318 for instructions on managing power through the Web Manager. See "To Power On, Power Off, or Reboot the Connected Server" on page 329 for instructions on managing power through the OSD.

Administrators must perform multiple configuration tasks in order to set up and grant users permission for power management. See "Setting Up and Configuring Power Management" on page 46 for a list of all of the administration tasks involved in setting up power management.

## Setting Up and Configuring Power Management

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

Two types of power management can be set up and configured on the KVM/net Plus:

- Power management of any device plugged into an IPDU connected to the AUX 1 port.  
See “Controlling Power Through the Web Manager IPDU Power Management Forms” on page 45.
- Power management while accessing a server connected to a KVM port and plugged into an IPDU connected to the AUX 1 port.  
See “Controlling Power While Connected to KVM Ports” on page 45.

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

**Table 1-16:**Tasks: General Power Management Set Up

Task	Where Documented/Notes
<b>1</b> Install PM units.	<ul style="list-style-type: none"> <li>• “To Connect a PM to the AUX 1 Port” on page 117</li> <li>• “To Connect Multiple PMs to the KVM/net Plus” on page 118</li> </ul>
<b>2</b> Configure the AUX 1 port for use with power management.	“To Configure the AUX 1 Port for Use With a PM” on page 251
<b>3</b> Plug devices into outlets on the PM connected to the AUX 1 port.	Devices plugged into connected PMs can be managed from the KVM/net Plus Web Manager Access Page.
<b>4</b> Configure users to manage power.	“To Configure Users to Manage Specific Power Outlets” on page 158



The following additional configuration tasks must be performed for power management while accessing a server connected to a KVM port and plugged into an IPDU connected to the AUX 1 port:

**Table 1-17:**Tasks: KVM-connected Power Management

Task	Where Documented/Notes
5 Plug servers connected to KVM ports into outlets on the PM connected to the AUX_1 port.	This is the first step in allowing users to control power not only from the Web Manager Access page, but while connected to KVM ports as well. Refer to the documentation of your PM model for more information if needed.
5 Associate the ports to which the servers are connected with the power outlets to which the servers are plugged in.	“To Configure a KVM Port for Power Management” on page 174
6 Give users full access (read, write, power) permission on the KVM port(s).	“To Assign KVM Port Access to a User or Group” on page 186

## Security

The KVM/net Plus comes with the following configurable security features:

- Encryption  
See Encryption.
- Authentication  
See Authentication.

### ***Encryption***

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

See “Security” on page 189 for instructions.

## Authentication

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

### Choosing Among Authentication Methods

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

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

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

**Table 1-18:**Supported Authentication Types for KVM/net Plus and Port Types

Authentication Type	Description	KVM/net Plus	All KVM Ports
None	No login required	N/A	X
Local	Uses user/password file for local authentication on the KVM/net Plus	X [Default]	X [Default]

**Table 1-18:**Supported Authentication Types for KVM/net Plus and Port Types

<b>Authentication Type</b>	<b>Description</b>	<b>KVM/net Plus</b>	<b>All KVM Ports</b>
Kerberos	Uses Kerberos network authentication protocol	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails	X	X
KerberosDownlocal	Uses local authentication if Kerberos server is down	X	X
LDAP	Uses LDAP (Light-weight directory access protocol)	X	X
LDAP/Local	Uses local authentication if LDAP authentication fails	X	X
LDAPDownlocal	Uses local authentication if LDAP server is down	X	X
NIS	Uses NIS authentication	X	X
NIS/Local	Uses local authentication if NIS authentication fails	X	X
NISDownlocal	Uses local authentication if NIS server is down	X	X
NTLM	Uses SMB authentication for Microsoft Windows NT/2000/2003	N/A	X

**Table 1-18:**Supported Authentication Types for KVM/net Plus and Port Types

<b>Authentication Type</b>	<b>Description</b>	<b>KVM/net Plus</b>	<b>All KVM Ports</b>
RADIUS	Uses RADIUS authentication	X	X
RADIUSDownlocal	Uses local authentication if RADIUS server is down	X	X
RADIUS/local	Uses local authentication if RADIUS authentication fails	X	X
TACACS+	Uses Terminal Access Controller Access Control System (TACACS+) authentication.	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails	X	X
TACACS+Downlocal	Uses local authentication if TACACS+ server is down	X	X

## ***Tools for Specifying Authentication Methods***

The administrator generally uses the Web Manager for specifying an authentication method for the KVM/net Plus and for all KVM ports, as described in “Configuring an Authentication Method” on page 191. Optionally, the administrator can use the OSD (on screen display) for selecting an authentication method and specifying an authentication server (when needed).

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

**Table 1-19:**Tasks: Specifying Authentication Methods

<b>Task</b>	<b>Where Documented/Notes</b>
Choosing an authentication method for the KVM/net Plus	<ul style="list-style-type: none"> <li>• Web Manager – “To Configure an Authentication Method for KVM/net Plus Logins” on page 192</li> <li>• OSD – “Authentication Screens” on page 405</li> </ul>
Choosing an authentication method for the for all KVM ports	<ul style="list-style-type: none"> <li>• Web Manager – “To Configure an Authentication Method for Logins Through KVM Ports” on page 193</li> <li>• OSD – “General Configuration Screens [OSD]” on page 355</li> </ul>
Configuring a remote authentication server	<p>If configuring any authentication method other than Local, an authentication server must be set up for that method.</p> <ul style="list-style-type: none"> <li>• Web Manager – “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194</li> <li>• OSD – “Authentication Screens” on page 405</li> </ul>

## Notifications, Alarms, and Data Buffering

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

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

- Local—stored in the KVM/net Plus’ flash memory
- Remote files—stored in either of the two following types of servers:
  - NFS servers
  - Syslog servers

For more details about syslog servers see, “Syslog Servers” on page 52.

For more background about setting up logging, notifications, alarms, and for links to all related procedures in this manual, see “Configuring Logging and Alarms” on page 53.

### ***Syslog Servers***

Messages about the KVM/net Plus, its connected IPDUs, and other connected devices can be sent to central logging servers, called syslog servers. Data from KVM-connected computers can optionally be stored in files on syslog servers.

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

#### ***Prerequisites for Logging to Syslog Servers***

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

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net Plus.  
Facility numbers are used on the syslog server for handling messages generated by multiple devices. See “Facility Numbers for Syslog

Messages” on page 53 for more background on how facility numbers are used.

### ***Facility Numbers for Syslog Messages***

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

### ***Example of Using Facility Numbers***

The syslog system administrator sets up a server called “syslogger” to handle log messages from two KVM/net Plus units. One KVM/net Plus is located in São Paulo, Brazil, and the other KVM/net Plus is in Fremont, California. The syslog server’s administrator wants to aggregate messages from the São Paulo KVM/net Plus into the `local1` facility, and to aggregate messages from Fremont KVM/net Plus into the `local2` facility.

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

## ***Configuring Logging and Alarms***

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

- “To Add a Syslog Server [Wizard]” on page 150
- “To Delete a Syslog Server [Wizard]” on page 150
- “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 215
- “To Configure Creation of Alarms and Syslog Files for IPDUs” on page 160

## VPN and the KVM/net Plus

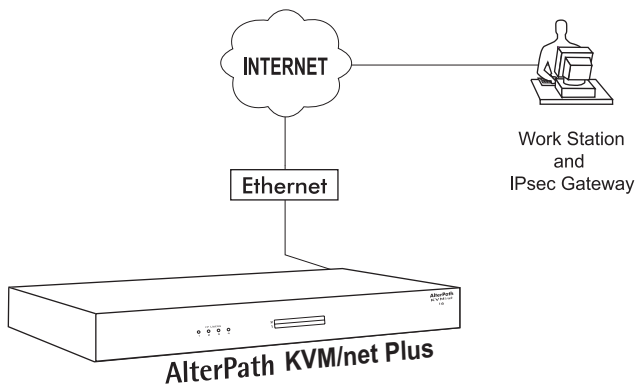
The KVM/net Plus administrator can set up VPN (Virtual Private Network) connections to establish encrypted communications between the KVM/net Plus and an individual host or all the hosts on a remote subnetwork. The encryption creates a security tunnel for communications through an intermediate network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

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

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

The KVM/net Plus is referred to as the Local or “Left” host, and the remote gateway is referred to as the Remote or “Right” host.

The following figure shows a single host running IPsec acting as its own security gateway on the right end and the KVM/net Plus acting as its own gateway on the left end.



**Figure 1-16:** KVM/net Plus VPN Example



In summary, you can use the VPN features on the KVM/net Plus to create the two following types of connections:

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

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

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

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

## Considerations When Choosing Whether to Enable DHCP

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

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

# Monitoring Temperatures

KVM/net Plus administrators can monitor three temperature sensors on the KVM/net Plus and modify graph display settings, create graph profiles, and apply an existing profile to the current view.

The sensors are located at the following locations within the KVM/net Plus:

- Power supply
- Fan
- FPGA (field programmable gate array)

The graphs display new readings at a specified interval. The following table shows graph features that can be saved in reusable profiles.

**Table 1-20:**Temperature Graph Parameters

Field/Menu	Use	Default	Allowed Values
<b>yGrid Boxes</b>	Specify a different number of rows.	18	1-55
<b>xGrid Boxes</b>	Specify a different number of columns Each graph cell represent the interval between readings.	299	1-999
<b>yMin Value</b>	Specify a different minimum value in degrees Fahrenheit to display on the y-axis.	-30°F/ -34.4°C	-196.6°F/ 127°C
<b>yMax Value</b>	Specify the maximum value in degrees Fahrenheit to display on the y-axis.	150°F/ 65.6°C	260.6°F/ 127°C
<b>Mean Temp</b>	Specify a different temperature to use as a basis for comparing the actual temperature. In line graphs, the Mean Temp is indicated by a red, horizontal line. In bar graphs, the colors of the bars indicate the following: <ul style="list-style-type: none"> <li>• Blue – Less than mean temperature.</li> <li>• Red – Greater than mean temperature.</li> <li>• Black – Equal to the mean temperature.</li> </ul>	75°F/ 23.8°C	-196.6°F/ 127°C to 260.6°F/ 127°C

**Table 1-20:** Temperature Graph Parameters (Continued)

<b>Field/Menu</b>	<b>Use</b>	<b>Default</b>	<b>Allowed Values</b>
<b>Graph Type</b>	Chose another graph type.	line	line bar
<b>Grid Line Color</b>	Choose another color for the lines.	white	white gray darkgrey lightgray magenta orange pink white
<b>Graph BG Color.</b>	Select the background color.	light gray	yellow green cyan gray darkgrey lightgray magenta orange pink white

For instructions on how to change the time interval for readings and how to monitor the temperature, see “Temperature Sensor” on page 263.

## KVM Terminator Usage and Types

An AlterPath KVM Terminator is used when connecting a computer or a cascaded KVM device to a KVM port on the AlterPath KVM/net Plus.

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

The Terminator comes in three models shown in the following table:

**Table 1-21:**AlterPath KVM Terminators

<b>Server Type</b>	<b>Connection</b>	<b>KVM Terminator Model</b>	<b>Part Number</b>
PC	Mini DIN 6-pin (COM)	PS/2	ATP4610
PC	USB port	PC USB	ATP4620
Sun USB	USB port. (This Terminator does not work with all Sun computers. The Sun computer must have a VGA and USB port.)	Sun USB	ATP4630

See “To Connect Computers to KVM Ports” on page 82 for instruction on using the KVM Terminators.

When a KVM/net Plus is ordered, the customer selects a KVM Terminator for each type of computer to be connected to the KVM/net Plus' KVM ports. For example, when ordering a KVM/net Plus with four KVM ports to be connected to two Windows servers with DIN connectors and two Sun servers with VGA ports and USB connectors, the customer would order two PS/2 Terminators and two Sun USB Terminators.

# KVM Expander

The AlterPath KVM Expander is designed to connect to the primary KVM/net Plus to increase the number of ports that a primary KVM/net Plus can manage.

---

**Note:** The AlterPath KVM Expander is compatible with the KVM/net Plus, the KVM/net, and the KVM. The term primary KVM unit refers to the three types of KVM units.

---

Front view of the AlterPath KVM Expander:



Back view of the AlterPath KVM Expander 16:



The following sections offer an introduction to the KVM Expander:

- “KVM Expander Features” on page 60
- “KVM Expander Models and Components” on page 61
- “Adding the KVM Expander to the KVM/net Plus Unit’s List of Cascaded Devices” on page 66
- “Upgrading the KVM Expander Microcontroller Code” on page 66

## ***KVM Expander Features***

The KVM Expander has no CPU, memory, or Flash; therefore, it relies on the intelligence of the primary KVM unit to control its KVM ports, making for a simple processing core as well as a cost-effective method of cascading a KVM/net Plus, a KVM/net, or a KVM.

The KVM Expander does support the following features:

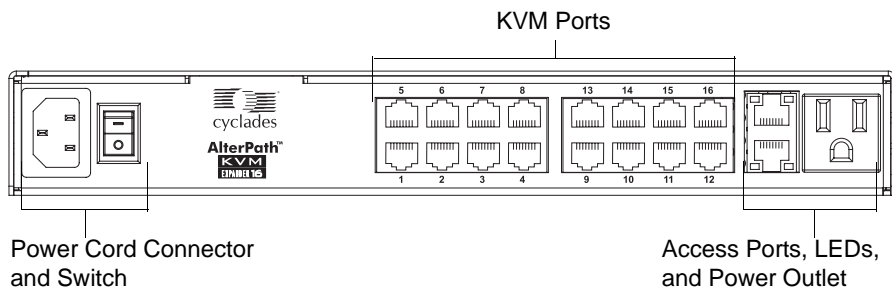
- Allows the connection of 8 or 16 servers  
See “KVM Expander Models and Components” on page 61 for more details.
- Supports all existing Terminators  
See “KVM Terminator Usage and Types” on page 58 for more details.
- Is compatible with the AlterPath KVM, KVM/net, and KVM/net Plus units  
See “Cascaded Devices” on page 27 for more details.
- Operates with up to two input ports – User A and User B  
See “Ports on the KVM Expander” on page 62 for more details.
- Supports horizontal or vertical rack mounting  
See “Setting Up the KVM Expander” on page 122 for more details.
- Allows daisy-chaining of KVM Expander units through its AC power outlet  
See “To Power On Devices Daisy Chained to the KVM Expander’s Power Outlet” on page 125 for more details.
- Displays port status with LEDs.  
See “LEDs on the KVM Expander” on page 63

## KVM Expander Models and Components

The KVM Expander comes in two models, which differ only in number of KVM ports:

**Table 1-22:** KVM Expander Model Numbers and Port Options

Model Number	Part Numbers	KVM Ports
8	ATP4208	8
16	ATP4216	16



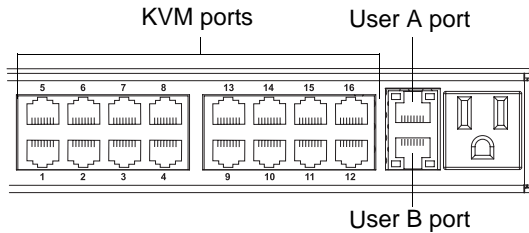
**Figure 1-17:** KVM Expander Back Panel Components

The following sections explain the components of the KVM Expander:

- “Ports on the KVM Expander” on page 62
- “LEDs on the KVM Expander” on page 63
- “Power Outlets on the KVM Expander” on page 63

## Ports on the KVM Expander

The KVM Expander has two CAT5 access ports and either 8 or 16 KVM ports.



**Figure 1-18:**Ports on the KVM Expander Back Panel

**Table 1-23:**KVM Expander Port Types

Port Type	Use and Connection Information
User A and User B	<p>The access ports can be connected with an RJ-45 cable to KVM ports on the primary KVM unit. Once the KVM Expander is configured as a cascaded device on the master KVM unit, users can connect to one or both ports. Each port allows one connection to a server plugged into the KVM Expander, so a maximum of two server connections can be made at one time.</p> <p>See “Installing the AlterPath KVM Expander” on page 119.</p>
KVM ports	<p>KVM ports on the KVM Expander work exactly as the KVM ports on the KVM/net Plus: They allow the connection of a CAT 5 cable to a Terminator, which is connected to a PC with a USB or a PS/2 connector or a Sun server with a USB connector.</p> <p>See “KVM Ports” on page 12 for more background information on KVM ports.</p> <p>See “Connecting Servers to the KVM Ports” on page 80 for information on connecting servers to the KVM ports.</p>



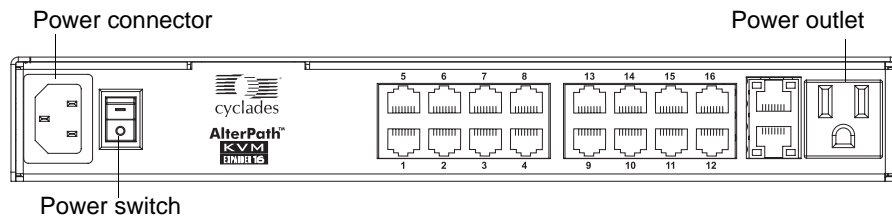
## ***LEDs on the KVM Expander***

The two LEDs on either side of the User A and User B ports on the KVM Expander blink when data activity occurs through the User A or User B port respectively.

## ***Power Outlets on the KVM Expander***

The KVM Expander has a power connector for power input and a power outlet for daisy chaining additional KVM Expanders or any other device.

**Caution!** The total amount of power consumed by devices daisy-chained to the KVM Expander must not exceed seven amps.



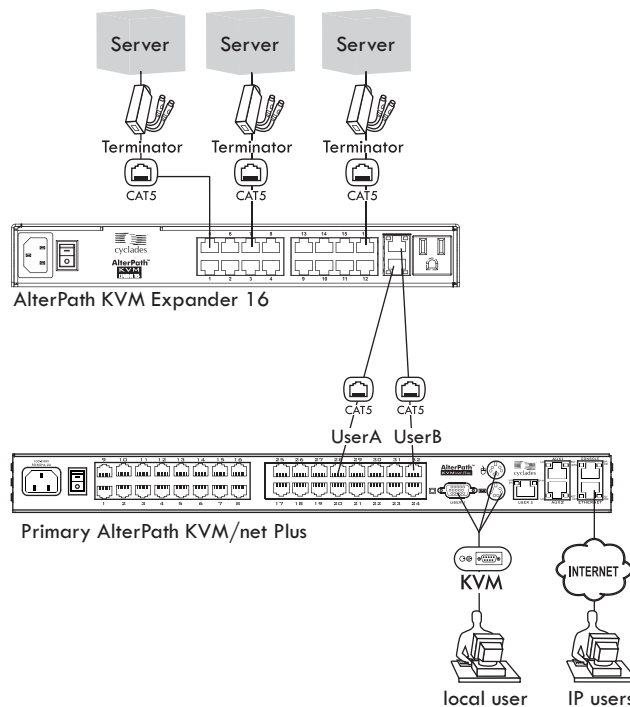
## Cascading a KVM Expander

The KVM Expander can support up to two users simultaneously accessing its KVM ports. In a two-user configuration, a primary KVM switch uses two connections for each KVM Expander-to-primary KVM switch configuration:

- User A port – One CAT5 cable between a KVM port on the primary KVM unit and the User A port on the KVM Expander
- User B port – One CAT5 cable between a KVM port on the primary KVM unit and the User B port on the KVM Expander

In a single user configuration, only one CAT5 cable is connected from a KVM port on the primary KVM unit to either of the user ports on the KVM Expander.

The following diagram displays a KVM Expander cascaded from a KVM/net Plus.



**Figure 1-19:** Connecting a KVM Expander to the KVM/net Plus

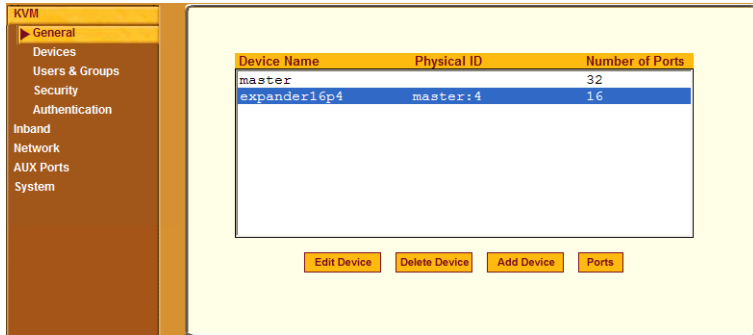
The following table shows the maximum number of servers a primary KVM/net Plus, KVM/net, or KVM can support when cascaded with a KVM Expander 8 or a KVM Expander 16.

**Table 1-24:**Maximum Number of Supported Servers

<b>KVM Unit</b>	<b>Model Number</b>	<b>KVM Expander and Model Number</b>	<b>Maximum Number of Servers</b>
KVM	32	KVM Expander 16	512
KVM	32	KVM Expander 8	256
KVM/net	16	KVM Expander 16	256
KVM/net	16	KVM Expander 8	128
KVM/net Plus	1601/1602/1604	KVM Expander 16	256
KVM/net Plus	1601/1602/1604	KVM Expander 8	128
KVM/net Plus	3201/3202/3204	KVM Expander 16	512
KVM/net Plus	3201/3202/3204	KVM Expander 8	256

## ***Adding the KVM Expander to the KVM/net Plus Unit's List of Cascaded Devices***

Once the administrator connects the KVM Expander to the primary KVM unit, the administrator must add the Expander to the primary unit's list of cascaded devices. Using the KVM/net Plus Web Manager in Expert Mode, go to: Configuration>KVM>Devices to see the form displayed in the following figure.



**Figure 1-20:**Devices Form on KVM/net Plus Web Manager

See “Configuring Cascaded KVM Units” on page 177 for instructions on adding, deleting, and modifying cascaded devices.

## ***Upgrading the KVM Expander Microcontroller Code***

Once a KVM Expander is installed and configured, administrators can use the Microcode Update form on the primary KVM unit to upgrade the microcode for a KVM Expander. Using the KVM/net Plus Web Manager in Expert Mode, go to: Management > Microcode Update to see the form displayed in the following figure.

**Figure 1-21:**Microcode Update Form on KVM/net Plus Web Manager

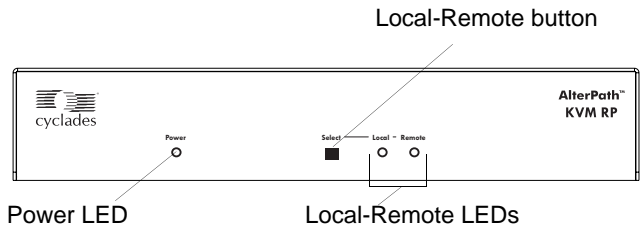
See “Microcode Upgrade” on page 276 for instructions on updating the microcode on a KVM Expander.

## User Access

The primary KVM switch takes care to prevent the same server port from being accessed by both user ports. If this happens, the last user to access the server port will have read-only access.

# AlterPath KVM RP

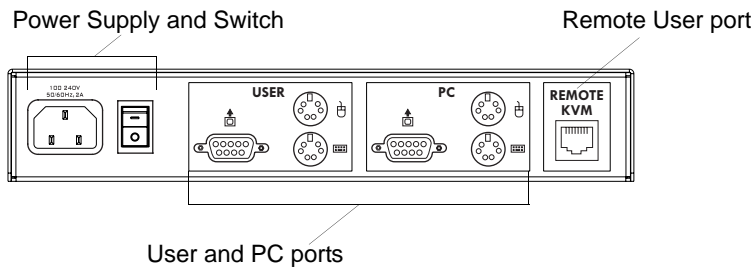
While using the AlterPath KVM RP, an administrator has full access to the OSD menus, so all local administration tasks can be performed in an office or at any other location up to 500 feet away from the KVM/net Plus. In addition, you do not need a dedicated monitor, keyboard, and mouse to use the RP; the RP box allows you to use the monitor, keyboard, and mouse of your regular work station and use keyboard shortcuts to toggle between the view at your local work station and the view of the KVM/net Plus. The RP also offers keyboard shortcuts to manage the extended local access to the KVM/net Plus. The following diagram displays the connections between the RP, the KVM/net Plus, and the local keyboard, monitor, and mouse. The AlterPath KVM RP is available in one model whose part number is ATP4710.



**Figure 1-22:**KVM RP Front

## Connectors on the Back of the KVM RP

The RP has a power supply and a User, a PC, and a Remote User port as displayed in the following figure.



**Figure 1-23:**KVM RP Back Panel

The following table offers more details about the use of and cables for each port on the back of the RP.

**Table 1-25:KVM RP Port Types**

<b>Port Type</b>	<b>Use and Connection Information</b>
Remote User	Its RJ-45 connection can be connected by a CAT5 cable to the User 2 port on the KVM/net Plus.
User [PS/2 and VGA]	Keyboard, video, and mouse (KVM) management port. Includes two PS/2 ports and a VGA port, which can be connected with a KVM cable to the PS/2 ports and a VGA port on the back of the computer at the local work station.
PC [PS/2 and VGA]	Keyboard, video, and mouse (KVM) management port. Includes two PS/2 ports and a VGA port, which can be connected to a local station's mouse, keyboard, and monitor.





# Chapter 2

## Installing the KVM/net Plus

This chapter outlines and described tasks for installing the KVM/net Plus and provides other important installation-related information.

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

---

<b>1</b>	Review the contents of the shipping box	Page 73
<b>2</b>	Set up the KVM/net Plus	Page 75
<b>3</b>	Make an Ethernet connection	Page 79
<b>4</b>	Connect servers to be managed through the KVM/net Plus	Page 80
<b>5</b>	Make a direct connection (terminal or local monitor, keyboard, and mouse) to the KVM/net Plus to prepare for basic network configuration	Page 84
<b>6</b>	Power on the KVM/net Plus and connected devices	Page 85
<b>7</b>	Perform basic network configuration (using the wiz command or OSD network screen)	Page 86
<b>8</b>	Finish configuration and manage the connected devices using the Web Manager	Page 99

---

Also see the following instructions for setting up the KVM/net Plus:

---

Changing Default Passwords	Page 100
Enabling Access to the Web Manager without Making a Direct Connection	Page 102
Preconfiguring the KVM/net Plus for Remote Installation	Page 105
Additional Configuration Tasks	Page 106


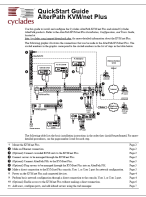

---

Perform the optional procedures in “Advanced Installation Procedures” on page 113 if you are installing a PCMCIA card, an intelligent power distribution unit (IPDU), an external modem, an AlterPath KVM RP, an AlterPath KVM Expander, or an other cascaded KVM devices.


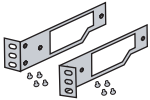
# Shipping Box Contents AlterPath KVM/net Plus

The shipping box for the KVM/net Plus contains the KVM/net Plus along with the items shown in Table 2-1. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

**Table 2-1: Shipping Box Contents, Part Numbers, and Description (Sheet 1 of 2)**

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0346	<i>AlterPath KVM/net Plus Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.

**Table 2-1:** Shipping Box Contents, Part Numbers, and Description (Sheet 2 of 2)

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: <ul style="list-style-type: none"> <li>• To connect a server to a KVM port (with the appropriate Terminator from Table 1-21 on page 58). See “Connecting Servers to the KVM Ports” on page 80.</li> <li>• To connect an Ethernet port to the LAN. See “To Make an Ethernet Connection” on page 79.</li> <li>• To connect a terminal to a console port. See “To Connect to the Console Port” on page 84.</li> <li>• To connect an IPDU or external modem to an AUX port. See “Connecting AlterPath PMs to the KVM/net Plus” on page 117 and “Connecting an External Modem” on page 116.</li> </ul>
<input type="checkbox"/>		HAR0370	2 - Mounting brackets with 8 - screws (2 spares)	Use to mount the KVM/net Plus to a rack or wall. See “To Mount the KVM/net Plus” on page 76.

When ordering the KVM/net Plus, customers also order one KVM Terminator for each server to be connected to one of the KVM ports. The number and types of KVM Terminators in each order are based on the number of KVM ports on the KVM/net Plus model that is being shipped and on the types of

servers that are to be connected to the KVM ports. For details, see “KVM Terminator Usage and Types” on page 58.

---

**Note:** For more information about cabling, see “RS-232 Cabling Tutorial” at <http://www.cyclades.com/resources>, under “White Papers.” For ordering information, see “Cyclades Product Guide,” available at: <http://www.cyclades.com/common/www/pdf/catalog.en.pdf>.

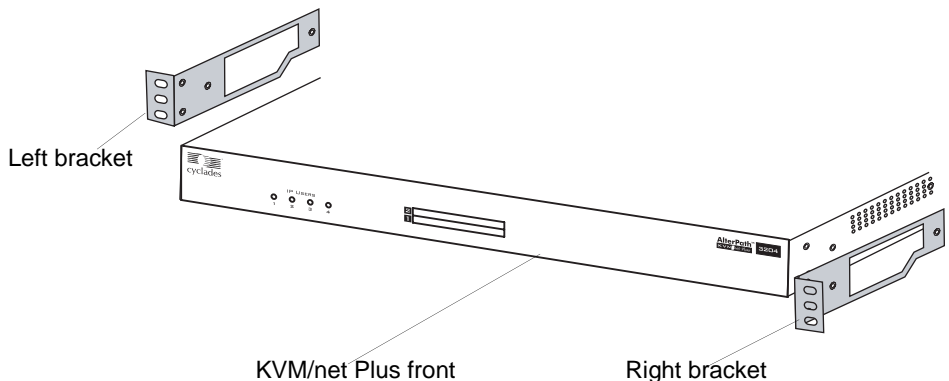
---

## Setting Up the KVM/net Plus

You can mount the KVM/net Plus on a rack or place it on a desktop or other flat surface. Two brackets are supplied with eight Phillips screws for attaching the brackets to the KVM/net Plus for mounting.

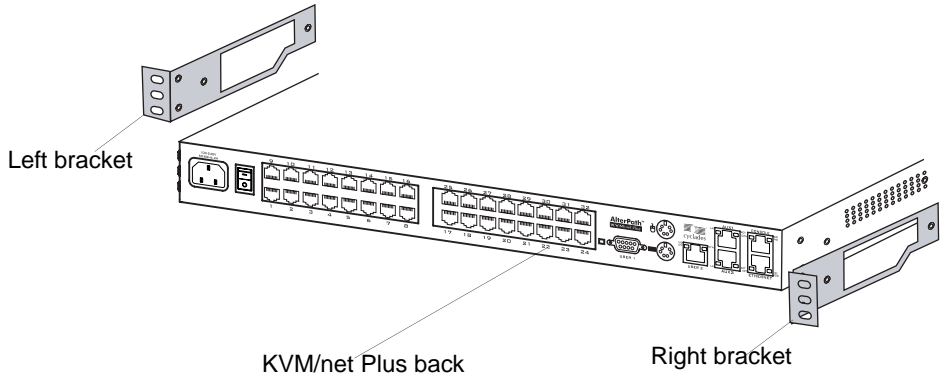
- If you are not mounting the KVM/net Plus, place the KVM/net Plus on a desk or table.
- If you are mounting the KVM/net Plus, obtain a Phillips screwdriver and appropriate nuts and bolts before starting the following procedure.

The following graphics depict the orientation of the left and right brackets for front mounting the KVM/net Plus.



**Figure 2-1:** KVM/net Plus and Brackets for Front Mounting

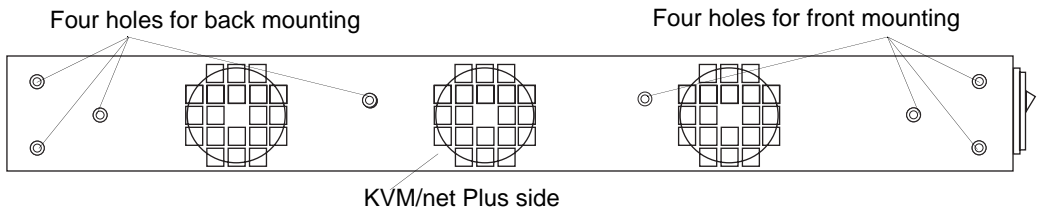
The following graphics depict the orientation of the left and right brackets for back mounting KVM/net Plus.



**Figure 2-2:** KVM/net Plus and Brackets for Back Mounting

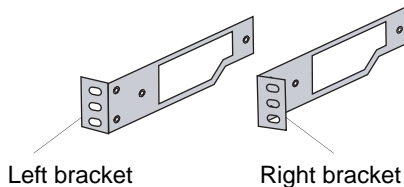
### ▼ **To Mount the KVM/net Plus**

1. Decide whether you need to mount the KVM/net Plus by the front or back and locate the appropriate sets of holes on the KVM/net Plus.



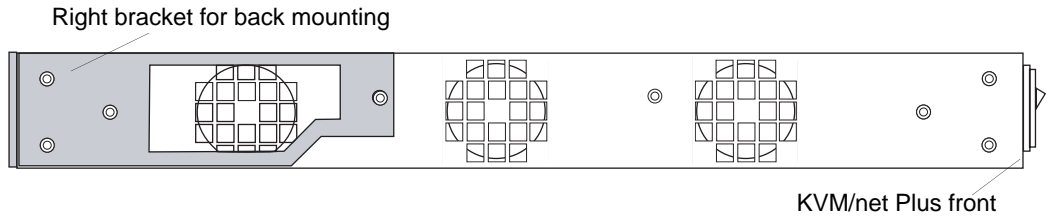
**Figure 2-3:** Rack Mounting Holes on the KVM/net Plus

2. Locate the left bracket and the right bracket as depicted in the following diagram.

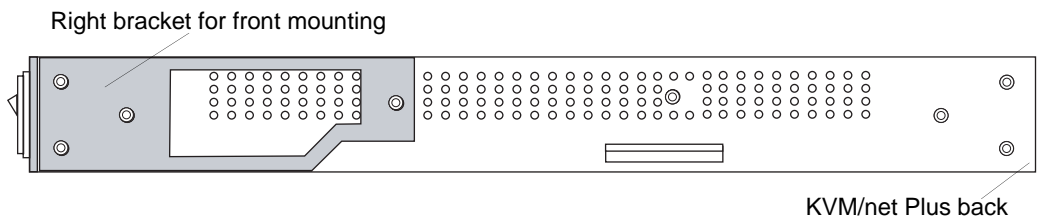


3. Attach the right bracket to the right side of the KVM/net Plus.

Whether you are facing the front or back of the KVM/net Plus, the right bracket must be attached to the right side.



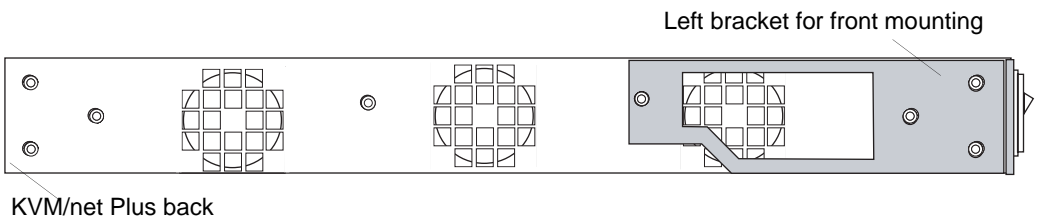
**Figure 2-4:** Right Bracket for Back Mounting the KVM/net Plus



**Figure 2-5:** Right Bracket for Front Mounting the KVM/net Plus

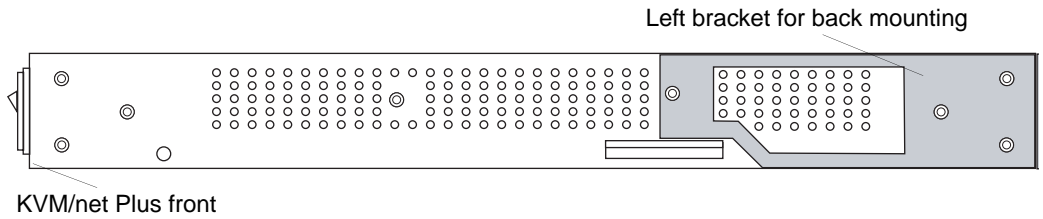
**4.** Attach the left bracket to the left side of the KVM/net Plus.

Whether you are facing the front or back of the KVM/net Plus, the left bracket must be attached to the left side.



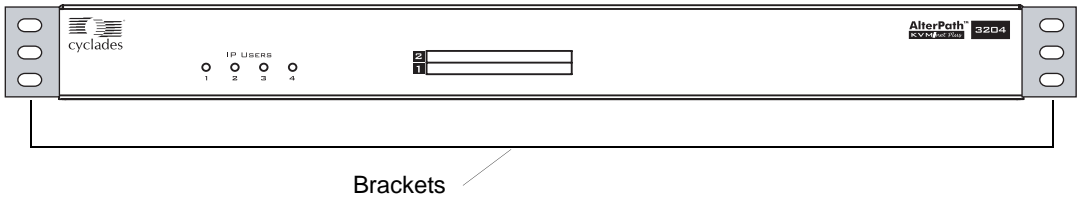
**Figure 2-6:** Left Bracket for Front Mounting the KVM/net Plus

## Installing the KVM/net Plus



**Figure 2-7:** Left bracket for Back Mounting the KVM/net Plus

The following figure shows the bracket flanges on the front of the KVM/net Plus after the brackets are installed.



5. Use a Phillips screwdriver to tighten the screws.
6. Use the mounting hardware recommended for your rack to mount the KVM/net Plus on a rack.

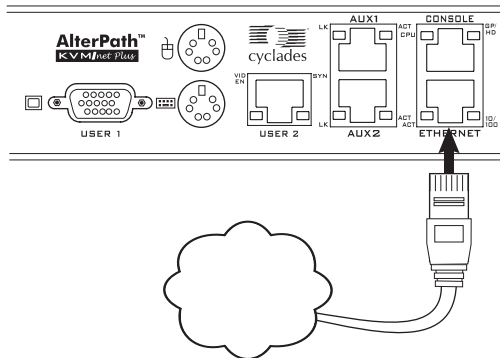


# Making an Ethernet Connection

Make an Ethernet connection to the KVM/net Plus in order to have Ethernet access to the Web Manager and remote access to devices connected to the KVM/net Plus.

## ▼ To Make an Ethernet Connection

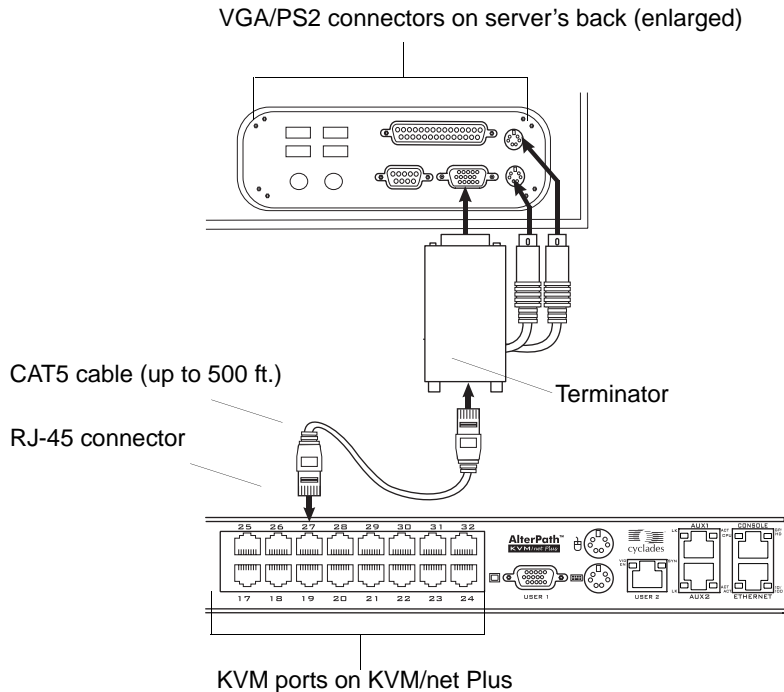
1. Connect one end of an Ethernet cable to your local area network (LAN).
2. Connect the other end to the Ethernet port on the KVM/net Plus.



Remote connections can also be made with a PCMCIA modem card or through an external modem connected to the AUX 2 port. See “Modem Connections” on page 339 for background information and instructions.

## Connecting Servers to the KVM Ports

You need to connect a KVM Terminator to every server before connecting it to a KVM port. Three Terminator types are available: PC PS/2 for servers with VGA and PS/2 connectors, PC USB for servers with VGA and USB connectors, and Sun USB Terminators for Sun servers with USB connectors. See “KVM Terminator Usage and Types” on page 58 for more details about the KVM Terminators, which are ordered and shipped with the KVM/net Plus.



---

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

---

Follow the procedures below when connecting computers to KVM ports on KVM/net Plus or on the KVM Expander. For connecting AlterPath PMs or cascaded KVM units, see Chapter 3, “Advanced Installation Procedures.”

---

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

---

## ▼ **To Prepare to Connect Servers to the KVM/net Plus**

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

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

- All servers are installed and fully configured.
  - User accounts with the appropriate permissions level exist on each server and you have the computer's root password for users who need root access to manage the server through the KVM/net Plus.
  - On all computers to be connected to KVM server ports, the mouse settings have been modified, as described in "Avoiding Conflicting Mouse Settings" on page 107.
2. If a server is to use remote authentication, do the following steps:
    - a. Make sure that the following prerequisite configuration is complete:
      - Authentication servers are installed and fully configured.
      - You have the root password for all users who need root access to manage the server through the KVM/net Plus.

---

**Note:** You may want to assign different passwords for a server's administrator on the KVM/net Plus and on the server's remote authentication server. If the administrator logs into the server using the password for the authentication server and log in fails, the failure can indicate that the authentication server is down and that the server's administrator should be notified to take action.

---

- b. Obtain the information you need to identify the authentication server on the KVM/net Plus from the server's administrator.
- c. After the KVM/net Plus is installed, make sure to specify the desired authentication method for the ports that are connected to each server.

See “Authentication” on page 48 for background information and see “Configuring an Authentication Method” on page 191 for the procedure.

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

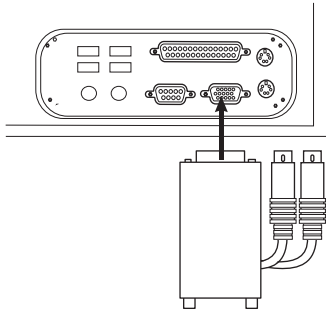
### ▼ **To Connect Computers to KVM Ports**

Do these steps after completing “To Prepare to Connect Servers to the KVM/net Plus” on page 81.

1. Select the appropriate Terminator.

Three Terminator types are available: PS/2 for PCs, USB for PCs, and USB for Sun systems. See “KVM Terminator Usage and Types” on page 58 for more details about the Terminators, which are ordered and shipped with the KVM/net Plus.

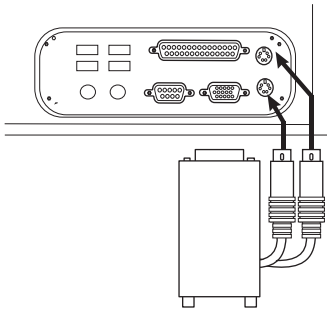
2. Connect the Terminator’s VGA (HD-15 male) connector to the computer’s VGA (monitor) port, tightening both screws firmly but not over-tightening.



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

The VGA DB-15 mini extender can be ordered separately from Cyclades.

4. To complete the connection of a PS/2 Terminator to a PC, connect the Terminator's purple and green connectors to the purple keyboard port and green mouse port on the PC.



5. To complete the connection of a USB Terminator to a PC or Sun computer, plug the USB connector from the Terminator to the computer's USB port.
6. To extend the connection from the computer to the KVM/net Plus, connect an RJ-45 to RJ-45 CAT5 cable up to 500 feet long to the Terminator.
7. Connect the RJ-45 connector on other end of the cable to a KVM port on the KVM/net Plus.
8. Repeat Step 1. through Step 7. for all computers to be connected to the KVM ports.
9. If any user is using a PC with Windows XP server pack 2 installed and Internet Explorer 5 or 6 to remotely administer a connected server, make sure the procedure under "Avoiding Internet Explorer Conflicts" on page 110 has been done on the PC.
10. If this is a first-time installation, go to "Making a Direct Connection for Network Configuration" on page 84.

## Making a Direct Connection for Network Configuration

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

- Connect a terminal or computer to the CONSOLE port.  
See “To Connect to the Console Port” on page 84.
- Connect a keyboard, monitor, and mouse to the keyboard, monitor, and mouse connectors on the KVM/net Plus.  
See “To Connect to the User 1 Management Port” on page 85.

See “Enabling Access to the Web Manager without Making a Direct Connection” on page 102, if desired, for other procedures that require advanced system administration expertise.

### ▼ *To Connect to the Console Port*

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

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

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

---

Serial Speed: <b>9600</b> bps	Stop Bits: <b>1</b>
Data Length: <b>8</b> bits	Flow Control: <b>None</b>
Parity: <b>None</b>	ANSI emulation

---

4. Go to Chapter 2. “Powering On the KVM/net Plus and Connected Devices” on page 85.

### ▼ **To Connect to the User 1 Management Port**

1. Plug the station's monitor, keyboard, and mouse cables to the Keyboard, Video, and Mouse connectors, labelled User 1, on the KVM/net Plus.
2. Go to “Powering On the KVM/net Plus and Connected Devices” on page 85.

## **Powering On the KVM/net Plus and Connected Devices**

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

### ▼ **To Power On the KVM/net Plus**

1. Make sure the KVM/net Plus' power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug in the power cable.
3. Turn the KVM/net Plus' power switch on.

The KVM/net Plus beeps once.

### ▼ **To Power On Connected Devices**

Do this after “Connecting Servers to the KVM Ports” on page 80.

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

## Performing Basic Network Configuration

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

- Through a console connection, log in and use the `wiz` command.  
See “Configuring Basic Networking Using the `wiz` Command” on page 87.
- Through a local KVM connection, log into the OSD and configure networking through the network screen.  
See “Configuring Basic Networking Using the OSD” on page 90.

Before you start, collect the following network information from the administrator of the network where the KVM/net Plus is to reside.

<input type="checkbox"/> Hostname:	
<input type="checkbox"/> KVM/net Plus’ public IP address:	
<input type="checkbox"/> Domain name:	
<input type="checkbox"/> DNS server’s IP address:	
<input type="checkbox"/> Gateway IP address:	
<input type="checkbox"/> Network mask:	
<input type="checkbox"/> KVM/net Plus’ MAC address (from the label on the bottom):	
<input type="checkbox"/> NTP server’s IP address (if you are using a time/date server):	

**Note:** The following procedures tell you to disable DHCP. Enabling DHCP requires a DHCP server at your site. See “Considerations When Choosing Whether to Enable DHCP” on page 55 for more details and see “To Use a Dynamic IP



Address to Access the Web Manager” on page 103 for the tasks that must be performed.

---

## Configuring Basic Networking Using the *wiz* Command

The following procedures require a hardware connection already made between the KVM/net Plus’ console port and the COM or USB port of a computer, as described under “To Connect to the Console Port” on page 84.

### ▼ To Log Into the KVM/net Plus Through the Console

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

```
KVM/net Plus login: root
Password: cyclades
```

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

### ▼ To Change the Password Through the Console

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

---

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

---

1. Enter the **passwd** command.

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

2. Enter a new password when prompted.

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

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

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

```
[root@KVM/net Plus /]# wiz
```

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

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

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

```
Hostname [ KVM/net Plus ]:  
boston_branch_kvm
```

4. Press Enter to disable DHCP.

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

5. Enter a public IP address to assign to the KVM/net Plus.

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

6. Enter the domain name.

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

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

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

8. Enter the IP address for the gateway.

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

9. Enter the netmask for the subnetwork.

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

10. To apply and confirm these parameters, see “To Apply and Confirm the Network Parameters Defined Using the wiz Command” on page 89.

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

This procedure must be completed immediately after defining network parameters using the wiz command as described in “To Use the wiz Command to Configure Network Parameters” on page 88

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

```
Current configuration:

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

2. Enter **y** if the values shown are correct, or press Enter.
3. The following prompt appears when “y” is entered.

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

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

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

5. To confirm the configuration, enter the `ifconfig` command.
6. The new network parameters display.
7. Log out from the terminal session.

8. In a HyperTerminal application on a Windows PC, go to “File > Exit”.
9. If performing a first-time installation, go to “Completing Configuration Using the Web Manager” on page 99.

## ***Configuring Basic Networking Using the OSD***

This procedure requires a hardware connection already made between the KVM/net Plus’ KVM management port and a local monitor, keyboard, and mouse, as described under “To Connect to the User 1 Management Port” on page 85. After the KVM/net Plus and monitor are powered on, the AlterPath Viewer appears displaying the OSD login screen.



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

**Table 2-2:** OSD Equivalents for Common Actions

<b>Action</b>	<b>OSD Equivalent</b>
Press OK.	Tab to the OK button and press the Enter key on your keyboard.
Enter <any value>.	Type the value in the appropriate field and press the Enter key.
Save changes.	Tab to the Save button and press the Enter key.
Select <an option>.	Press an arrow key to navigate. Select the menu option and then press the Enter key.

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

Action	OSD Equivalent
Go to a specific screen, as in: “Go to ‘Configure > Users and Groups > Local Users > Change Password’.”	From the Main menu, select the first option shown in the menu path; “Configure” in the example. On the next menu, select the next option shown after the > (right angle bracket); “Users and Groups” in the example. Repeat until you select the last option in the menu path.
Exit the OSD.	Click the X box on the upper right of the viewer. If you are on the Main Menu, you can select Exit.

---

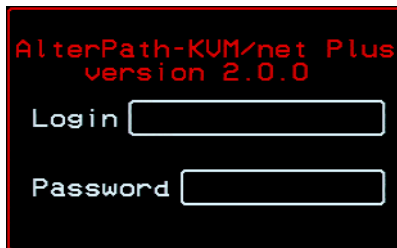
**Note:** If your keyboard has a Return key instead of an Enter key, press the “Return” key when you see “Enter.”

---

### ▼ *To Log Into the OSD*

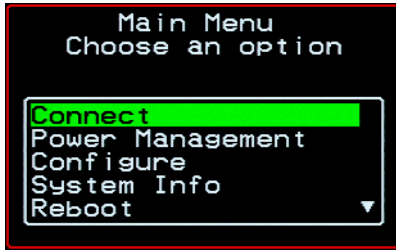
1. On the OSD login screen, enter “admin” as the Login name.
2. Enter the password.

The default password is “cyclades.” If the password has been changed from the default, use the current password.



3. Press Enter.

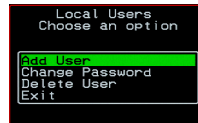
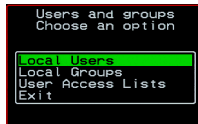
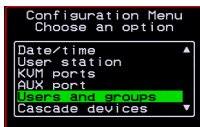
The OSD Main Menu appears.



4. If you are performing an initial configuration of basic networking parameters, go to “To Change a Password Using the OSD” on page 92; otherwise, go to “To Configure Network Parameters Using the OSD” on page 94.

### ▼ *To Change a Password Using the OSD*

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



---

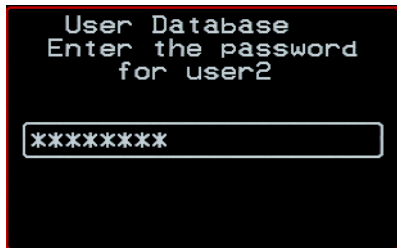
**Warning!** If the “admin” password has not been changed, change it now. Changing the default password closes a security hole that could be easily exploited.

---

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



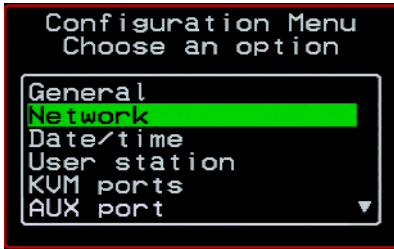
3. Enter a new password.



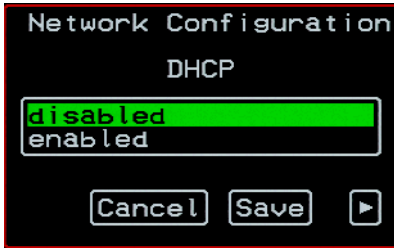
4. Re-enter the new password.  
The password confirmation dialog box appears.
5. Press Enter.  
The Local Users menu appears.
6. Select Exit or press the Esc key to exit the Local Users menu.  
You can use the Exit or Cancel option or the Esc key to exit any window on the OSD.
7. If you are performing an initial configuration of basic networking parameters, see "To Configure Network Parameters Using the OSD" on page 94.
8. Otherwise, go to the appropriate menu option for your next task.

▼ **To Configure Network Parameters Using the OSD**

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

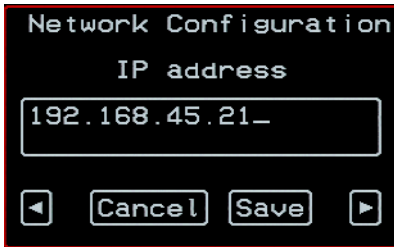


The DHCP form appears.



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

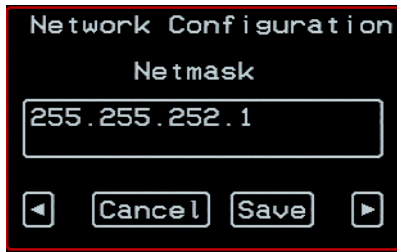
The IP address form appears.



3. Enter the IP address for the KVM/net Plus and press Enter.

The Netmask form appears.





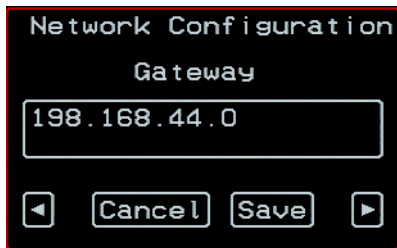
Network Configuration

Netmask

255.255.252.1

◀ Cancel Save ▶

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



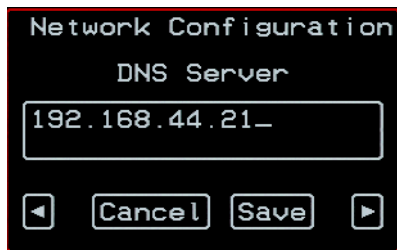
Network Configuration

Gateway

198.168.44.0

◀ Cancel Save ▶

5. Enter the IP address for the gateway and press Enter.  
The DNS Server form appears.



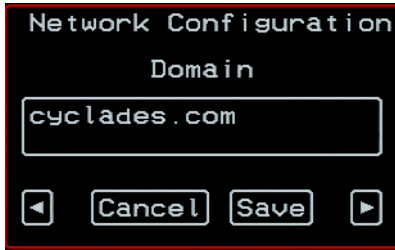
Network Configuration

DNS Server

192.168.44.21\_

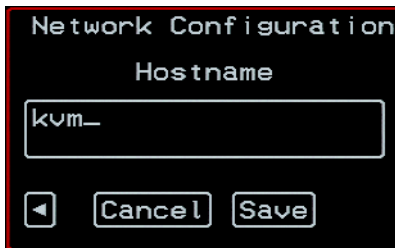
◀ Cancel Save ▶

6. Enter the IP address for the DNS server and press Enter.  
The Domain form appears.



7. Enter the domain name and press Enter.

The Hostname form appears.



8. Enter the hostname for the KVM/net Plus and save the changes to complete the basic network configuration.

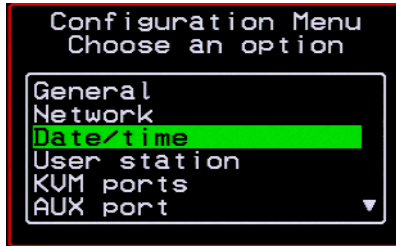
The Configuration menu appears.

- To configure an NTP (network time protocol) server or to enter the date and time manually, go to “To Set the Time and Date Using the OSD” on page 97.
- If you do not wish to configure the time and date at this time, and if you are performing an initial configuration of basic networking parameters, go to: “Completing Configuration Using the Web Manager” on page 99.
- Otherwise, go to the appropriate menu option for your next task or exit from the OSD.

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

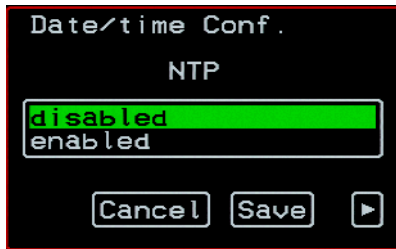
1. From the Main menu of the OSD, go to Configure.

The Configuration menu appears.



2. Select Date/time.

The Date/time conf. form appears.



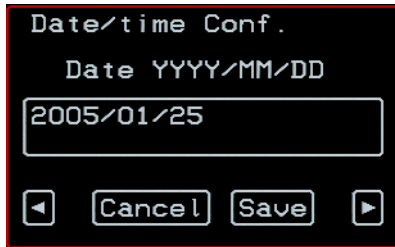
3. To enable the NTP time and date server, do the following.
  - a. On the Date/time conf. form, select the “enabled” option.

The NTP server screen appears



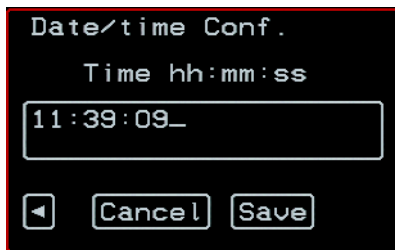
## Installing the KVM/net Plus

- b. Enter the IP address of the NTP server.
  - c. Save the changes.
4. To enter the date and time manually, do the following.
- a. On the Date/time conf. form, select disabled.  
The Date entry screen appears.



The screenshot shows a terminal window titled "Date/time Conf.". Below the title, it says "Date YYYY/MM/DD". A text input field contains the date "2005/01/25". At the bottom of the window, there are four buttons: a left arrow, "Cancel", "Save", and a right arrow.

- b. Enter the date in the format shown and press Enter.  
The Time entry screen appears.



The screenshot shows a terminal window titled "Date/time Conf.". Below the title, it says "Time hh:mm:ss". A text input field contains the time "11:39:09\_". At the bottom of the window, there are three buttons: a left arrow, "Cancel", and "Save".

- c. Enter the time in the format shown and save the changes.  
If you are performing an initial configuration of basic networking parameters, go to: "Completing Configuration Using the Web Manager" on page 99.  
Otherwise, go to the appropriate menu option for your next task.

# Completing Configuration Using the Web Manager

The “admin” user can administer the KVM/net Plus and its connected devices through the Web Manager without doing any additional configuration.

The following list shows other common configuration tasks:

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

See “Web Manager for Administrators” on page 133 for procedures for performing the common KVM/net Plus administration tasks listed in this section.

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

- Let other users manage servers or PMs without being able to make changes to the KVM/net Plus configuration
- Assign users or groups to specific ports, restricting users to a limited set of devices
- Let other users share all administration of the KVM/net Plus

## Changing Default Passwords

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

### ▼ *Changing admin's Default Password [Web Manager]*

1. Bring up the Web Manager.
2. Log in as admin using the default password, “cyclades”.
3. In Wizard Mode, go to **Step3: Access**.
4. Select “admin” from the Users List.
5. Click the “Change Password” button.
6. Enter the password into the New Password field.
7. Enter the password again into the Repeat New Password field.
8. Click OK when done.

### ▼ *Changing the Root Password [Command Line]*

1. Verify that a terminal or a computer with a terminal emulator is connected to the console port on the KVM/net Plus.
2. From the terminal or terminal emulator, log into the console port as **root**, using the existing password. [The default password is cyclades.]

KVM login: root

Password: cyclades

- a. Enter the **passwd** command.

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

- b. Enter a new password when prompted.

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

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

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

4. Log out.

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

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

## ▼ **Changing Default Passwords [OSD]**

This procedure requires a hardware connection already made between the KVM/net Plus' KVM management port and a local monitor, keyboard, and mouse, as described in "To Connect to the User 1 Management Port" on page 85. Do the following to change the passwords for the root and admin users.

1. Log into the OSD.
2. From the Main Menu, select the Configure option.
3. From the Configure Menu, select the Users and Groups option.
4. From the list of users on the User Database screen, select the user name.
5. On the "Enter the Password" screen, enter the new password.
6. On the password confirmation window, re-enter the password.
7. Select OK.

## Enabling Access to the Web Manager without Making a Direct Connection

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

- The KVM/net Plus ships with a default IP address: 192.168.160.10. You can use the default address to bring up the Web Manager, assign a fixed IP address to the KVM/net Plus and specify other network parameters without making a direct connection. To do so, you must temporarily change the IP address of a computer on the same subnet. See “To Use the Default IP Address to Access the Web Manager” on page 102.”
- DHCP is enabled on the KVM/net Plus by default. If you have network access to the DHCP server for the KVM/net Plus, and if you are able to

disc70  
over the KVM/net Plus’ dynamically assigned IP address, you do not need to make a direct connection. Discovering the current IP address requires entering the KVM/net Plus’ MAC address. Make a note of the MAC address, which is on a label at the bottom of the unit in the form *NN-NN-NN-NN-NN-NN*, and go to “To Use a Dynamic IP Address to Access the Web Manager” on page 103.”

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

The default IP address for the KVM/net Plus is 192.168.160.10. This procedure assumes that you are able to temporarily change the IP address of a computer that is on the same subnet as the KVM/net Plus.

1. Set up the AlterPath KVM/net Plus.  
See “To Mount the KVM/net Plus” on page 76.
2. Connect computers and other devices to be managed through the KVM/net Plus.  
See “Connecting Servers to the KVM Ports” on page 80.
3. Power on the KVM/net Plus and connected devices.  
See “Powering On the KVM/net Plus and Connected Devices” on page 85.



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

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

5. Bring up a browser on the computer whose address you changed, enter the KVM/net Plus' default IP address (`http://192.168.160.10`) to bring up the Web Manager, and log in.
6. To allow subsequent use of the Web Manager from any computer, go to the Wizard: "Step 1: Network Settings" to change the default IP address to a fixed public IP address and to configure the other basic network parameters and save them to Flash.
7. Restore the computer's IP address to its previous IP address.
8. Finish configuring KVM/net Plus users and ports using the Web Manager.

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

This procedure assumes that DHCP is enabled on the KVM/net Plus.

1. Set up the AlterPath KVM/net Plus.  
See "To Mount the KVM/net Plus" on page 76.
2. Connect computers and other devices to be managed through the KVM/net Plus.  
See "Connecting Servers to the KVM Ports" on page 80.
3. Power on the KVM/net Plus and connected devices.  
See "Powering On the KVM/net Plus and Connected Devices" on page 85.
4. To obtain the KVM/net Plus' current IP address from the console port do the following:
  - a. Using the console port, log in as "root."  
See "To Connect to the Console Port" on page 84 for instructions if needed.

## Installing the KVM/net Plus

- b. Execute the command

```
ifconfig eth0
```

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

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

5. To obtain the KVM/net Plus’ current IP address from the DHCP server, supply the MAC address from the bottom side of the KVM/net Plus’ chassis. (The address has the form: *NN-NN-NN-NN-NN-NN*, as in this example: 00-60-3D-01-36-B4.)
6. Finish configuring KVM/net Plus users and ports using the Web Manager.

# Preconfiguring the KVM/net Plus for Remote Installation

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

If you would prefer to have Cyclades preconfigure the KVM/net Plus with basic network parameters at Cyclades Corporation before it is shipped, ask your Cyclades contact to put you in touch with Cyclades professional services. For a fee, they can preconfigure the KVM/net Plus with parameters you supply.

## ▼ *To Preconfigure the KVM/net Plus*

1. Perform the tasks listed in the following table to preconfigure the KVM/net Plus for installation at another location.

<b>Task</b>	<b>Where Documented</b>
Make a direct connection to prepare for basic network configuration.	“Making a Direct Connection for Network Configuration” on page 84
Power on the KVM/net Plus and connected devices.	“Powering On the KVM/net Plus and Connected Devices” on page 85
Perform basic network configuration.	“Performing Basic Network Configuration” on page 86

2. If you ship the KVM/net Plus to a remote location for installation, also send the following:
  - A record of the KVM/net Plus’ fixed IP address and other network parameters.
  - A copy of the instructions under “To Set Up a Preconfigured KVM/net Plus” on page 106.

## ▼ **To Set Up a Preconfigured KVM/net Plus**

Perform the tasks shown in the following table with a KVM/net Plus that has been preconfigured as described in “To Preconfigure the KVM/net Plus” on page 105. After the tasks are completed in the order shown, a remote administrator can bring up the Web Manager by entering the KVM/net Plus’ fixed IP address in a browser.

<b>Task</b>	<b>Where Documented</b>
<b>1</b> Set up the AlterPath KVM/net Plus.	“Setting Up the KVM/net Plus” on page 75
<b>2</b> Make an Ethernet connection.	“Making an Ethernet Connection” on page 79
<b>3</b> Connect computers and other devices.	“Connecting Servers to the KVM Ports” on page 80
<b>4</b> Power on the KVM/net Plus and connected devices.	“Powering On the KVM/net Plus and Connected Devices” on page 85

## **Additional Configuration Tasks**

See the following sections for other procedures.

<b>Task</b>	<b>Where Documented/Notes</b>
Avoiding Conflicting Mouse Settings	“Avoiding Conflicting Mouse Settings” on page 107
Avoiding Internet Explorer Conflicts	“Avoiding Internet Explorer Conflicts” on page 110
Assigning Your Own TCP Viewer Port Address	“Types of Ports” on page 9

# Avoiding Conflicting Mouse Settings

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

Work with the administrators of computers to be connected to the KVM/net Plus to ensure that one of the following procedures is performed, depending on the type of computer:

- “To Prevent Mouse Conflicts [Windows XP/Windows 2003]” on page 107
- “To Prevent Mouse Conflicts [Windows 2000 / ME]” on page 108
- “To Prevent Mouse Conflicts [Windows 95/98/NT]” on page 108
- “To Prevent Mouse Conflicts [Linux]” on page 109

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

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

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

1. As administrator, on the Start menu, go to: Settings > Control Panel > Mouse > Pointer Options.
2. To set the mouse pointer acceleration to none, do the following:
  - a. Click the **Advanced** button.  
The Advanced Setting Pointer Speed dialog box appears.
  - b. On Windows ME, clear the **Pointer acceleration** check box.
  - c. On Windows 2000, clear the **Enable pointer acceleration** check box.
  - d. Click **OK**.
3. Set the motion speed to medium by moving the slider to the middle of the **Adjust how fast the pointer moves** scale.
4. Click **OK**.
5. To disable transition effects do the following:
  - a. Go to: Control Panel > Display > Effects.
  - b. Clear **Use transition effects for menus and tooltips**.
  - c. Click **OK**.

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

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

## ▼ **To Prevent Mouse Conflicts [Linux]**

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

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

The root prompt appears.

```
#
```

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

```
# xset m 0
```

6. Exit the AlterPath Viewer.

---

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

---

## Avoiding Internet Explorer Conflicts

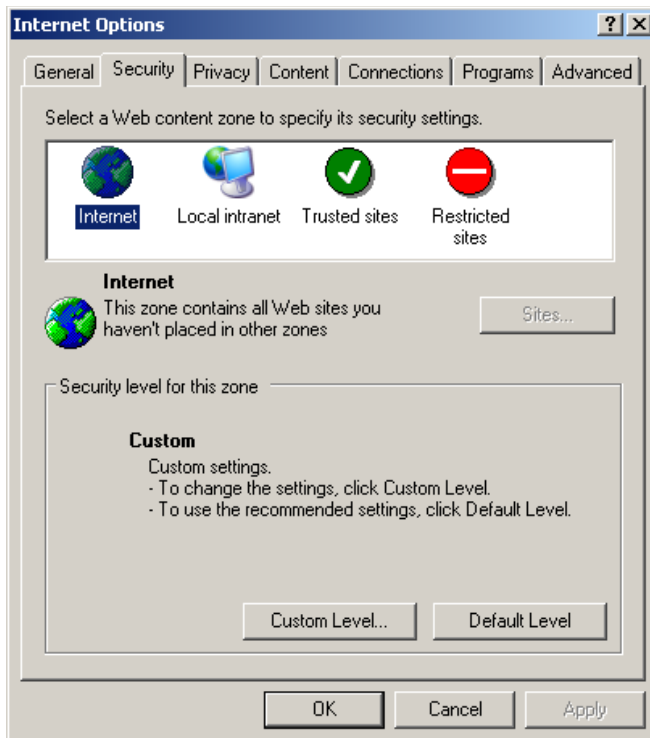
The procedure described in this section must be performed on a PC if all the following are true:

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

### ▼ To Modify IE Security Settings

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

The **Security** form appears.

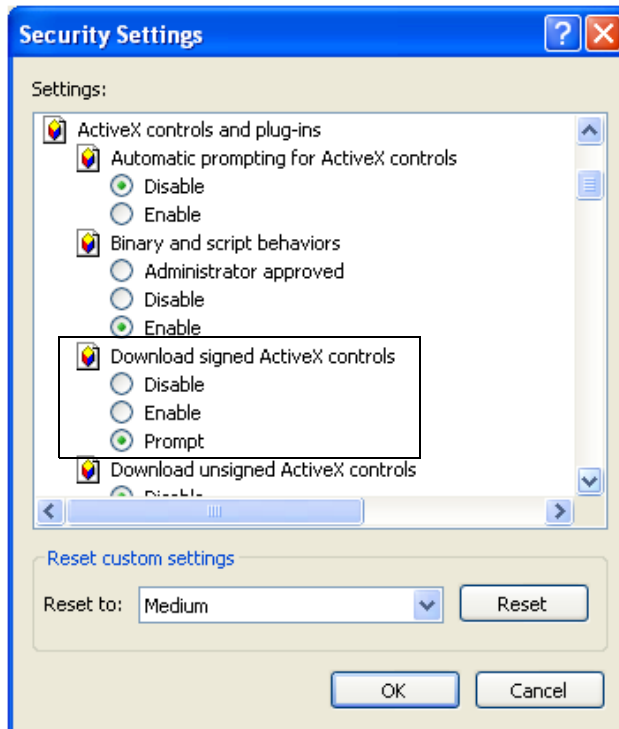




2. Click the **Custom Level** button.

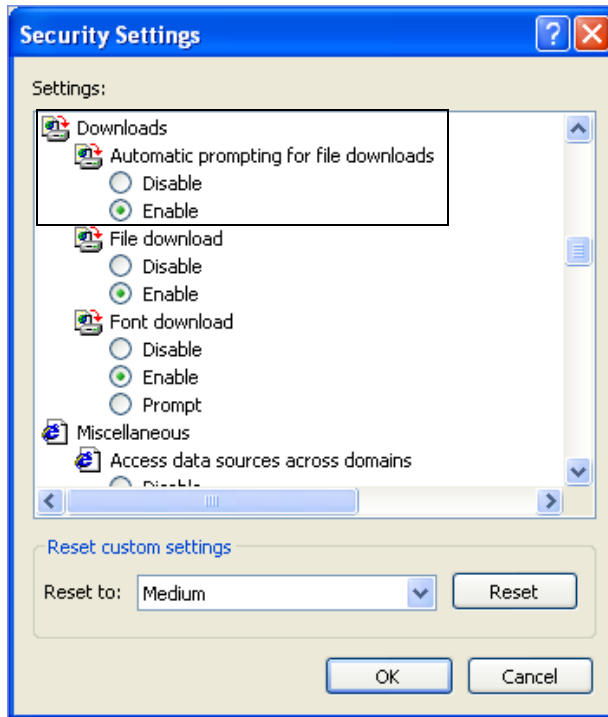
The Security Settings form appears.

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



4. Select either **Enable** or **Prompt**.
5. If you selected **Enable**, press the **OK** button.
6. If you selected **Prompt**, go to **Downloads** > **Automatic prompting for file downloads**, and select **Enable**.

## Installing the KVM/net Plus



7. Select the **OK** button.

# Chapter 3

## Advanced Installation Procedures

KVM/net Plus supports the installation of related components, which are used to extend the access to and control of the KVM/net Plus and its connected devices.

The following table lists the components that can be installed with the KVM/net Plus and shows the page numbers where the tasks are described in more detail.

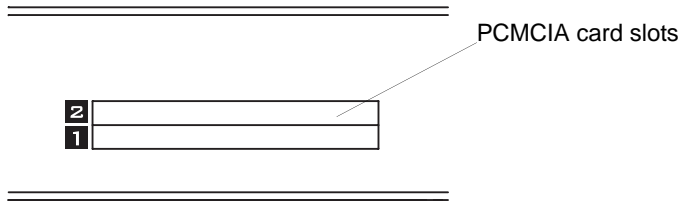
---

PCMCIA cards	Page 114
External modems	Page 116
AlterPath PM	Page 117
AlterPath KVM Expander	Page 119
Cascaded KVM units	Page 126
AlterPath KVM RP	Page 129

---

## Installing PCMCIA Cards in the Front Card Slots

The front panel of the KVM/net Plus has two PCMCIA card slots as depicted in the following figure. You can insert and configure one modem card in one of the slots.

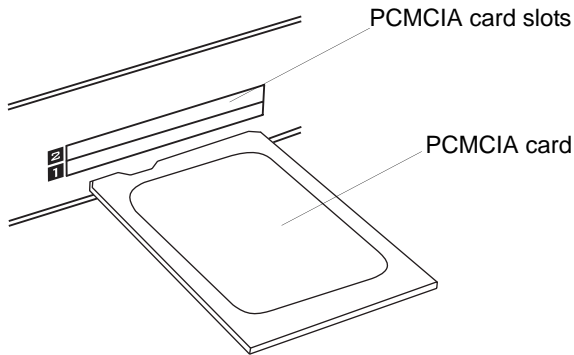


**Figure 3-1:** PCMCIA Card Slots on the KVM/net Plus Front Panel

### ▼ *To Install a PCMCIA Card in the Front Card Slot*

1. Insert the PCMCIA modem card into slot 1 or slot 2.

Slide the card in until it is firmly seated.



---

**Note:** You can insert one card in each of the slots, but the KVM/net Plus supports configuration of only one modem card at a time.

---

2. Use a phone cord to connect the jack on the PCMCIA card to a live telephone line.
3. Use the Web Manager or the OSD to configure the PCMCIA card.
  - For instructions on using the Web Manager, see “To Configure a Modem Card” on page 216.
  - For instructions on using the OSD, see “PCMCIA Screens” on page 401.

See “Modem Connections” on page 339 for instructions on making dial up connection to the KVM/net Plus.

## ▼ **To Remove a PCMCIA Card from the Front Card Slot**

---

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

---

1. Eject the card by using the Eject button on the Web Manager PCMCIA Management form.

If needed, see “To Eject a PCMCIA Card From the Card Slot” on page 219.
2. Physically remove the card from the slot.

## Connecting an External Modem

You can connect a modem to either or both of the AUX ports on the KVM/net Plus. After the modem is connected and properly configured, you can use it to dial in to the KVM/net Plus when the production network or management network is down, or when Ethernet access is unavailable.

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

This procedure requires the following cables and connectors:

- A straight through cable with an RJ-45 connector on one end and the appropriate connector or adapter (USB, DB-9, or DB-25) on the other end for connecting the AUX port to the appropriate port on the external modem.
  - A phone cord with RJ-11 connectors on both ends for connecting the modem to the phone line.
1. Connect the RJ-45 end of the cable to the AUX port on the KVM/net Plus.
  2. Connect the other end of the cable to the modem.
  3. Use a phone cable to connect the jack on the modem to a live telephone jack at your site.
  4. Configure the AUX port for PPP.

See “AUX Ports” on page 250 and “To Configure the AUX 1 Port for Use With a PM” on page 251.

## Connecting AlterPath PMs to the KVM/net Plus

You can control an AlterPath Power Management (PM), intelligent power distribution unit (IPDU), by connecting it to the AUX 1 port on the KVM/net Plus. By daisy-chaining any combination of PM models, you can control up to 128 outlets from one KVM/net Plus.

### ▼ **To Connect a PM to the AUX 1 Port**

1. Use an RJ-45 CAT5 cable to connect the AUX 1 port on the KVM/net Plus to the In port of your AlterPath PM.
2. Configure the AUX 1 port for power management. See “To Configure the AUX 1 Port for Use With a PM” on page 251.

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

Task	Where Documented
Install multiple PM units.	“To Connect Multiple PMs to the KVM/net Plus” on page 118
Manage the power of devices connected to configured PM units.	<ul style="list-style-type: none"> <li>• Web Manager – “IPDU Power Management” on page 154</li> <li>• OSD – “Power Management Menu” on page 350</li> </ul>
Control the power of a device while connected to it through a KVM port.	<ul style="list-style-type: none"> <li>• Web Manager – “To Power On, Power Off, or Reboot the Connected Server” on page 329</li> <li>• OSD – “To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets” on page 337</li> </ul>

## ▼ **To Connect Multiple PMs to the KVM/net Plus**

This procedure assumes that you have one AlterPath PM connected to the AUX 1 port of the KVM/net Plus. See “To Connect a PM to the AUX 1 Port” on page 117 for the procedure.

1. Connect one end of an RJ-45 cable to the Out port of the “master” AlterPath PM, which is connected to the AUX 1 port of the KVM/net Plus.
2. Connect the other end of the RJ-45 cable to the In port of the next AlterPath PM (slave).
3. To connect another PM to the slave, connect one end of an RJ-45 cable to the Out port of an already connected PM.
4. Repeat Step 3 until you have connected the desired number of PMs.  
You can control up to 128 power outlets in any combination of PM models.

See “IPDU Power Management” on page 154 for information on managing your PMs with the Web Manager.



# Installing the AlterPath KVM Expander

The following table gives a high-level list of steps involved in setting up, installing, and configuring the KVM Expander with links to detailed information about each step.

---


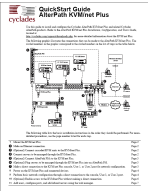

<b>1</b>	Review the contents of the shipping box	Page 120
<b>2</b>	Set up the KVM Expander	Page 122
<b>3</b>	Connect computers to the KVM ports on the KVM Expander	Page 80
<b>4</b>	Connect the KVM Expander to the KVM/net Plus	Page 128
<b>5</b>	Power on the KVM Expander and connected devices	Page 125
<b>6</b>	Add the KVM Expander to the primary KVM unit's list of cascaded devices	Page 178

---



## Shipping Box Contents KVM Expander

The shipping box for the AlterPath KVM Expander contains the KVM Expander along with the items shown in Table 3-1. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

**Table 3-1:** KVM Expander Shipping Box Contents, Part Numbers, and Description

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0346	<i>AlterPath KVM/net Plus Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.

**Table 3-1: KVM Expander Shipping Box Contents, Part Numbers, and Description**

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: <ul style="list-style-type: none"> <li>• To connect a server to a KVM port (with the appropriate Terminator from Table 1-21 on page 58). See “Connecting Servers to the KVM Ports” on page 80.</li> <li>• To connect the KVM Expander User A or User B ports to a KVM port on the KVM/net Plus . See “To Connect a KVM Expander to the Primary KVM/net Plus” on page 128 .</li> </ul>
<input type="checkbox"/>		HAR0453	2 - Mounting brackets with 8 - screws (2 spares)	Use to mount the KVM/net Plus to a rack or wall. See “To Mount the KVM Expander” on page 122.

When ordering the KVM Expander, customers also order one KVM Terminator for each server to be connected to one of the KVM ports. The number and types of KVM Terminators in each order are based on the number of KVM ports on the KVM Expander model that is being shipped and on the types of servers that are to be connected to the KVM ports. For details, see “KVM Terminator Usage and Types” on page 58.

**Note:** For more information about cabling, see “RS-232 Cabling Tutorial” at <http://www.cyclades.com/resources>, under “White Papers.” For ordering information, see “Cyclades Product Guide,” available at: <http://www.cyclades.com/common/www/pdf/catalog.en.pdf>.

## Setting Up the KVM Expander

The KVM Expander is a 1U device that can be mounted on the side of a rack or placed on a desktop or other flat surface. Two brackets are supplied with six Phillips screws for attaching the brackets to the KVM Expander for mounting.

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

---

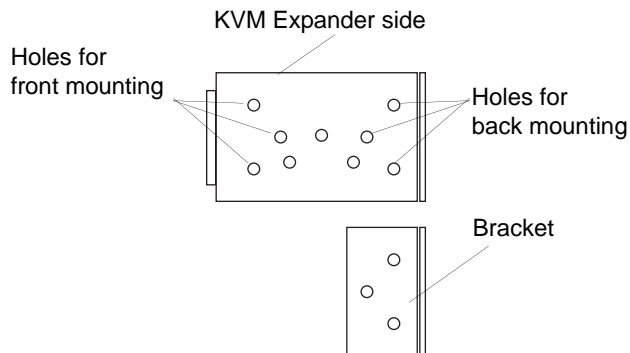
**Note:** Place the KVM Expander in a location that is within the 500 feet distance allowable between the KVM/net Plus and its connected computers. Using cables longer than 500 feet in total length can compromise performance.

---

### ▼ To Mount the KVM Expander

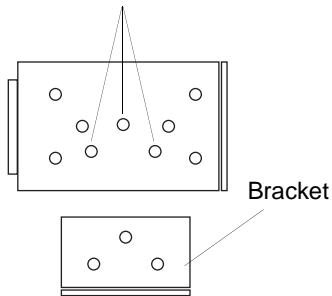
1. Connect the two supplied brackets to the KVM Expander, connecting one bracket to each side of the box.
  - a. Decide whether you need to mount the KVM Expander by the front or back and locate the appropriate sets of holes on the KVM Expander.

The following figure shows the angle of a bracket being installed for rack mounting.



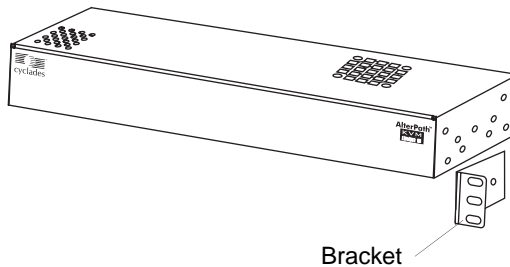
The following figure shows the angle of a bracket being installed for wall mounting.

Holes for wall mounting

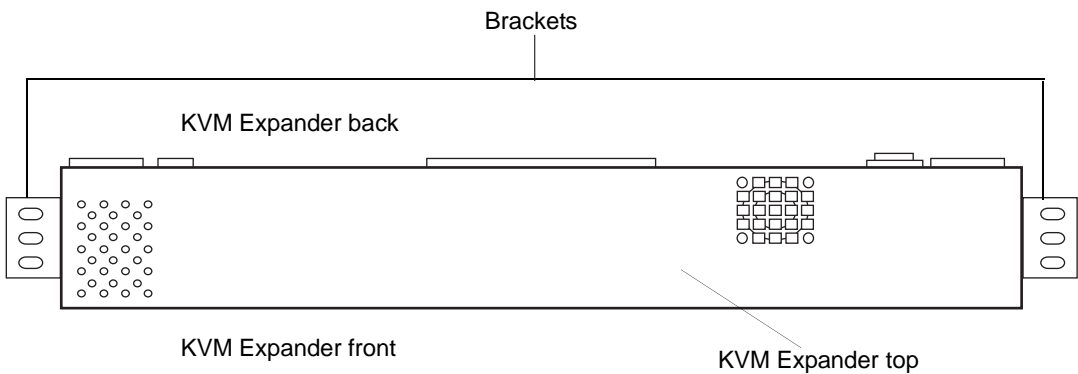


- b. For each bracket, insert a screw through each of the three holes on the bracket into the appropriate holes at either the front or back of the KVM Expander.

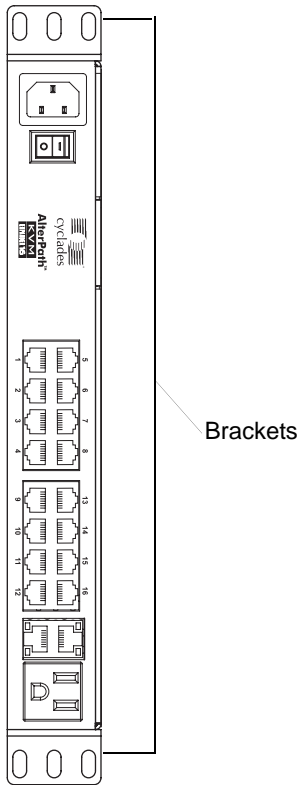
The following figure shows the brackets as they appear from the side and front of the KVM Expander after the brackets are installed for rack mounting.



The following figure shows the brackets as they appear from the top of the KVM Expander after the brackets are installed for wall mounting.



The following figure shows the bracket flanges on the front of the KVM Expander after the brackets are installed for rack mounting.

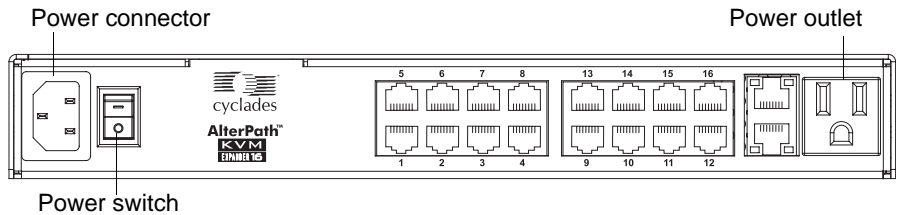


- c. Use a Phillips screwdriver to tighten the screws.
- 2.** Use screws or nuts and bolts as appropriate to mount the KVM Expander on the wall, on a rack, or in a cabinet.
- 3.** Use screws or nuts and bolts as appropriate to mount the KVM Expander on a rack.

## Powering On the KVM Expander and Connected Devices

The KVM Expander has a power connector for power input and a power outlet for daisy chaining additional KVM Expanders or any other device.

**Caution!** The total amount of power consumed by devices daisy-chained to the KVM Expander must not exceed seven amps.



### ▼ To Power On the KVM Expander

1. Make sure the KVM Expander's power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug in the power cable.
3. Turn the KVM Expander's power switch on.

### ▼ To Power On Devices Daisy Chained to the KVM Expander's Power Outlet

1. Make sure the KVM Expander's power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug the power cable of a device in the power outlet located on the back right of the KVM Expander.
3. Turn the KVM Expander's power switch on.

### ▼ To Power On KVM-connected Devices

Do this after "Connecting Servers to the KVM Ports" on page 80.

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

## Connecting Cascaded KVM Units to the Primary KVM/net Plus

KVM/net Plus supports the cascading of three types of secondary KVM devices: the AlterPath KVM, the KVM Expander, and the KVM/net Plus. See the following sections for the appropriate instructions:

- “To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net Plus” on page 127
- “To Connect a KVM Expander to the Primary KVM/net Plus” on page 128

Each of these cascaded devices has its own set up and installation instructions which must be performed in addition to connecting the device to the master KVM/net Plus:

- AlterPath KVM – See the *AlterPath KVM Manual* for installation instructions.
- KVM Expander – See the “Installing the AlterPath KVM Expander” on page 119 for installation instructions.
- KVM/net Plus – See the “Installing the KVM/net Plus” on page 71 for installation instructions.

For background information on cascading, see “Cascaded Devices” on page 27.



## ▼ **To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net Plus**

1. Power off all KVM hardware and connected devices.
2. To connect to the User 2 port of a secondary KVM, KVM/net, or KVM/net Plus, do the following:
  - a. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net Plus.
  - b. Connect the other end of the CAT5 cable to the User 2 port on the secondary KVM, KVM/net, or KVM/net Plus.
3. To connect to the User 1 port of a secondary KVM, KVM/net, or KVM/net Plus, do the following:
  - a. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net Plus.
  - b. Connect the other end of the CAT5 cable to a KVM Terminator.
  - c. Connect the Terminator's VGA and PS/2 connectors to the User 1 port on the secondary KVM, KVM/net, or KVM/net Plus.

See "Connecting Servers to the KVM Ports" on page 80 for detailed instructions on how to connect devices to KVM ports using KVM Terminators.
4. Repeat steps 1 through 3 for each secondary KVM to be connected to the primary KVM/net Plus.

## ▼ **To Connect a KVM Expander to the Primary KVM/net Plus**

See “Installing the AlterPath KVM Expander” on page 119 for background information on the KVM Expander.

1. Power off all KVM hardware and connected devices.
2. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net Plus.
3. Connect the other end of the CAT5 cable to the User A and or the User B port on the secondary KVM Expander.

---

**Note:** To enable two concurrent KVM connections to ports on the KVM Expander, connect two CAT5 cables to two ports on the KVM/net Plus. Connect one CAT5 cable to the User A port and the other CAT5 cable to the User B port on the KVM Expander.

---

4. Repeat steps 1 through 3 for each secondary KVM Expander to be connected to the primary KVM/net Plus.

## Installing the AlterPath KVM RP


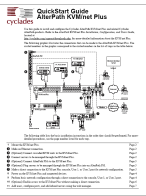


With a CAT5 cable up to 500 feet long, the AlterPath KVM RP can be connected to the User 2 port of the KVM/net Plus unit, enabling the extended user to perform local administration tasks or to select the local keyboard, video, and mouse console between a local station and a server connected to the KVM/net Plus.

Tasks	Where Documented/Notes
1 Place the RP on a desk or table up to 500 feet away from the KVM/net Plus.	You can use a CAT5 cable of up to 500 feet long to extend the local administration of the KVM/net Plus.
2 Connect the RP to the KVM/net Plus.	“To Connect the RP to the KVM/net Plus” on page 131.
3 Connect a keyboard, monitor, and mouse to the RP.	“Options for Accessing the RP” on page 131
4 Supply power to and turn on the RP.	“Supplying Power to the RP” on page 132
5 Use the RP to control the KVM/net Plus.	“Controlling the OSD Through the AlterPath KVM RP” on page 418

## Shipping Box Contents KVM RP

The shipping box for the KVM RP contains the KVM RP along with the items shown in Table 3-2. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

**Table 3-2: KVM RP Shipping Box Contents, Part Numbers, and Description**

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0346	<i>AlterPath KVM/net Plus Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use to connect the User 2 port on the KVM/net Plus to the Remote User port on the KVM RP. See “To Connect the RP to the KVM/net Plus” on page 131.

**Table 3-2: KVM RP Shipping Box Contents, Part Numbers, and Description**

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		ATP4710	KVM cable	Use to connect the VGA port, PS/2 keyboard port, and PS/2 mouse port on the back of your PC to the PC VGA port, PS/2 keyboard port, and PS/2 mouse port on the RP. See “To Connect the RP to the Local Work Station” on page 132 more information.

### ▼ **To Connect the RP to the KVM/net Plus**

1. Put one end of a CAT5 cable into the Remote User port on the KVM RP.
2. Put the other end of the CAT5 cable into the User 2 port on the KVM/net Plus.

## **Options for Accessing the RP**

The KVM RP offers two options for monitor, keyboard, and mouse control. Administrators can connect a dedicated keyboard, monitor, and mouse directly to the RP. Or administrators can connect the RP to their local work station in order to toggle the keyboard, monitor, and mouse control between the KVM/net Plus and the local computer.

### ▼ **To Connect the RP to a Dedicated Keyboard, Monitor, and Mouse**

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

### ▼ **To Connect the RP to the Local Work Station**

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

---

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

---

## **Supplying Power to the RP**

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

### ▼ **To Power On the KVM RP**

1. If the RP has its own dedicated keyboard, monitor, and mouse connected to its USER port, do the following:
  - a. Make sure the KVM/net Plus' power switch is off.
  - b. Plug in the power cable.
  - c. Turn the KVM/net Plus' power switch on.
2. If the RP is connected to the local PC, turn the KVM/net Plus' power switch on.

The power is supplied by the PC. See "To Connect the RP to the Local Work Station" on page 132 for instructions on connecting the RP to the local PC.

# Chapter 4

## Web Manager for Administrators

This chapter is for administrators who use the Web Manager for managing and configuring the KVM/net Plus. Two types of administrators can access all the Web Manager functions described in this chapter:

- An administrator who knows the password for the “admin” account, which is configured by default
- An optionally configured regular user whose account is in the “admin” group (See “Users & Groups” on page 181 for how the admin adds a regular user account and adds the account to the admin group.)

Administrators whose accounts are configured without administrative access can log into the Web Manager as regular users and then access connected devices, as described in Chapter 5. “Web Manager for Regular Users” on page 283. For more background about the differences between user types, see “Types of Users” on page 20.

Before following the procedures in this chapter, review “Prerequisites for Using the Web Manager” on page 25, if needed, to make sure that you can connect to the Web Manager.

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

---

Common Features of Administrators’ Windows	Page 136
Logging Into the Web Manager and Saving Changes	Page 138
Administrative Modes	Page 141
Wizard Mode	Page 141
Expert Mode	Page 151

---

## Common Tasks

The following table lists common tasks that KVM/net Plus administrators perform with links to the procedures.

---

Task	Where Documented/Notes
Set up other users to access connected devices without being able to make changes to the KVM/net Plus configuration	<ul style="list-style-type: none"><li>• “To Add a User [Wizard]” on page 145</li><li>• “To Add a User [Expert]” on page 182</li></ul>
Assign users or groups to specific ports, restricting access to a limited set of devices	<ul style="list-style-type: none"><li>• “To Assign KVM Port Access to a User or Group” on page 186</li></ul>
Set up other users to share all administration of the KVM/net Plus	<ul style="list-style-type: none"><li>• “To Add a User [Wizard]” on page 145</li><li>• “To Add a User [Expert]” on page 182</li></ul>
Enable direct login to ports from the Web Manager login screen	<ul style="list-style-type: none"><li>• To Enable Direct Access to KVM Ports</li></ul>
Set up logging of system messages to a syslog server	<ul style="list-style-type: none"><li>• “To Add a Syslog Server [Wizard]” on page 150</li><li>• To Delete a Syslog Server [Wizard]</li><li>• To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]</li><li>• To Configure Creation of Alarms and Syslog Files for IPDUs</li></ul>

---



Task	Where Documented/Notes
Configure power management for one or both of the AUX ports (if the port is connected to an optional AlterPath PM or other supported IPDU device)	<ul style="list-style-type: none"> <li>• “To Configure the AUX 1 Port for Use With a PM” on page 251</li> </ul> <p>Also see the procedures under “IPDU Power Management” on page 154 including:</p> <ul style="list-style-type: none"> <li>• “To View Status, Lock, Unlock, and Cycle Power Outlets” on page 156</li> <li>• “To View and Reset IPDU Information” on page 157</li> <li>• “To Configure Creation of Alarms and Syslog Files for IPDUs” on page 160</li> <li>• “To Upgrade Firmware on an AlterPath PM” on page 161</li> </ul>
Choose among authentication methods and specify authentication servers for logins to the KVM/net Plus and for logins to devices connected to the KVM/net Plus’ ports	<ul style="list-style-type: none"> <li>• “To Configure an Authentication Method for KVM/net Plus Logins” on page 192</li> <li>• “To Configure an Authentication Method for Logins Through KVM Ports” on page 193</li> </ul>
Specify encryption levels for KVM ports	<p>“To Configure Encryption on Port Connections [Expert]” on page 190</p>
Configure rules for the KVM/net Plus to filter packets like a firewall	<ul style="list-style-type: none"> <li>• “To Add a Chain for IP Filtering” on page 231</li> <li>• “To Edit A Chain for IP Filtering” on page 233</li> <li>• “To Add a Rule for IP Filtering” on page 233</li> <li>• “To Edit a Rule for IP Filtering” on page 230</li> </ul>

## Common Features of Administrators' Windows

The features of all Web Manager windows for KVM/net Plus administrators are described in the following sections:


- Control and logout buttons and KVM/net Plus Information  
See “Administrators’ Control Buttons, Logout Button, and KVM/net Plus Information.”
- Getting more information  
See “Obtaining More Information” on page 137

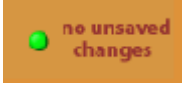
### ***Administrators’ Control Buttons, Logout Button, and KVM/net Plus Information***

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


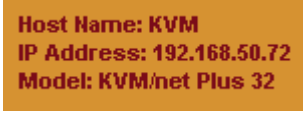


The following table describes the uses for each control button.

Button Name	Use
<b>try changes</b>	Tests the changes entered on the current form without saving them.
<b>cancel changes</b>	Cancels all unsaved changes.
<b>apply changes</b>	Applies all unsaved changes.
<b>reload page</b>	Reloads the page.
<b>Help</b>	Brings up the online help with information relating to the current form.
	The unsaved changes button appears on the lower right hand corner of the Web Manager and a graphical LED blinks red whenever the current user has made any changes and has not yet saved the changes.

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

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

Window Area	Purpose
	Click this button to log out.
	Displays the hostname and IP address assigned during initial configuration (see “Performing Basic Network Configuration” on page 86). Also displays the model name of the KVM/net Plus.

## ***Obtaining More Information***

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

# Logging Into the Web Manager and Saving Changes

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

---

To Log Into the Web Manager as Admin	Page 138
To Save Configuration Changes	Page 138

---

For procedures specific to each mode, see “Administrative Modes” on page 141.

## ▼ *To Log Into the Web Manager as Admin*

This procedure assumes that the prerequisites described under “Prerequisites for Using the Web Manager” on page 25 are done and that you can connect to the Web Manager.

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

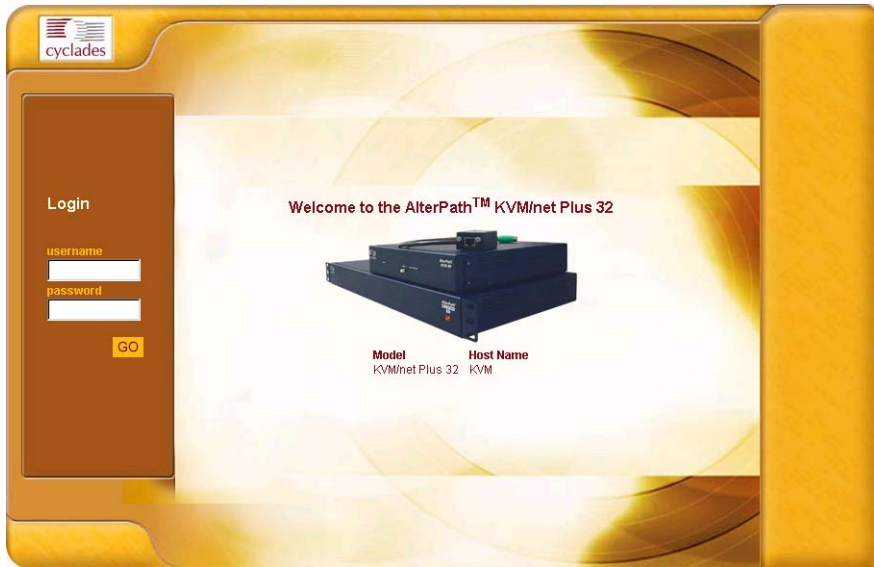
---

**Note:** Devices like the AlterPath KVM/net Plus that are installed in computer rooms are usually assigned fixed IP addresses. If DHCP is enabled, you must find out the dynamically assigned IP address each time before you bring up the Web Manager. Check with the administrator who configured the basic network parameters on the KVM/net Plus, for help finding the IP address, if needed. Or see “Considerations When Choosing Whether to Enable DHCP” on page 55 for a list of ways to find out the KVM/net Plus IP address assigned by the DHCP server.

---

- a. If DHCP is enabled, enter the dynamically assigned IP address.
- b. If DHCP is not enabled, use a fixed IP address assigned by the administrator to the KVM/net Plus.

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



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



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

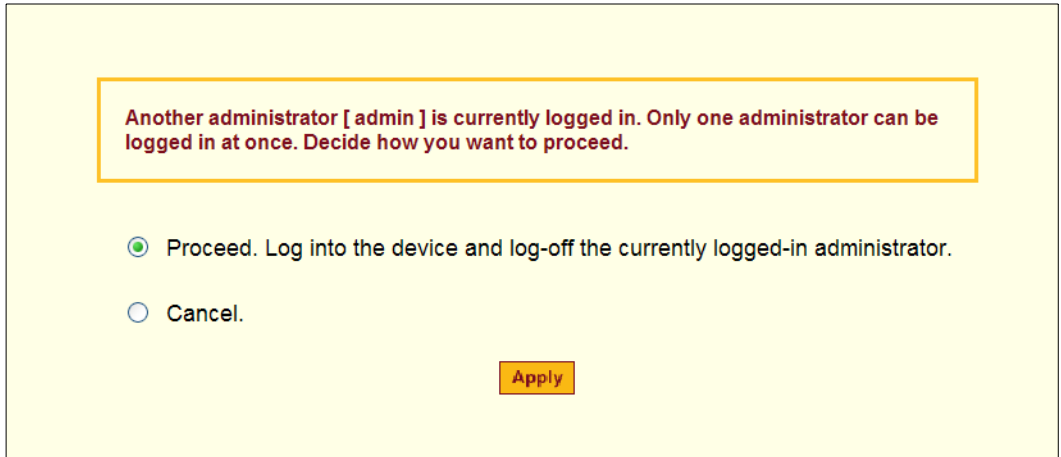
```
IP_address/login.asp?portname=portnumber
```

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

See “Web Manager Login Screen” on page 297 for background information on the multiple ways to login to the Web Manager.

**3.** Enter your account’s username and password.

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



---

**Note:** For more information about the numbers of simultaneous logins allowed, see “Simultaneous KVM/net Plus Logins” on page 21.

---

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

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

### ▼ **To Save Configuration Changes**

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

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

The “no unsaved changes” graphical LED appears.

# Administrative Modes

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

- “Wizard Mode” on page 141
- “Expert Mode” on page 151



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

## Wizard Mode

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



**Figure 4-1:** Example Window in Wizard Mode

After you log in as described in “To Log Into the Web Manager as Admin” on page 138, Expert mode is in effect by default. To change to Wizard mode, select the Wizard button, which displays only in Expert mode.

## ***Procedures in Wizard Mode***

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

To Change Network Settings [Wizard]	Page 143
To Add a User [Wizard]	Page 145
To Delete a User [Wizard]	Page 147
To Change a Password [Wizard]	Page 147
To Add a Syslog Server [Wizard]	Page 150
To Delete a Syslog Server [Wizard]	Page 150

## ***Steps in Wizard Mode***

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

Step 1: Network Settings [Wizard]	Page 142
Step 2: Access [Wizard]	Page 144
Step 3: System Log [Wizard]	Page 149

### ***Step 1: Network Settings [Wizard]***

In Wizard Mode, selecting "Step 1: Network Settings" brings up a form for reconfiguring existing network settings. During initial setup of the KVM/net Plus, the administrator configures the default basic network settings that were needed to enable logins through the Web Manager. (See "Performing Basic Network Configuration" on page 86, if desired, for more information about the initial network configuration.) You can skip this step if the current settings are correct. Check with your network administrator if you are not sure.

Before making any changes to existing network settings, you may want to review "Performing Basic Network Configuration" on page 86, which provides a form to record information you need to collect ahead of time.



In Expert mode, under Configuration>Network, you can specify additional networking-related information: a Console Banner, a secondary IP address and secondary network mask, and an MTU. See “To Configure Host Settings [Expert]” on page 212. In Expert mode under Configuration>Network, you can configure syslog servers for ports; specify rules for filtering syslog messages, specify PCMCIA card, Virtual Private Network (VPN), and SNMP settings; specify IP filtering rules (for the KVM/net Plus to act as a firewall), and perform other advanced configuration tasks.

## ▼ To Change Network Settings [Wizard]

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

See the list of network information to collect under “Performing Basic Network Configuration” on page 86, if needed.

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

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

---

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

---

The screenshot shows the 'Step 1: Network Settings' wizard screen. On the left is a sidebar with three steps: 'Step 1: Network Settings' (highlighted), 'Step 2: Access', and 'Step 3: System Log'. The main content area has a yellow background and contains the following text:

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

Below this is a 'DHCP' checkbox, which is currently unchecked. Underneath are several input fields:

- Host Name: KVM
- IP Address: 192.168.50.72
- Network Mask: (empty)
- Domain Name: cyclades.com
- DNS Server: 192.168.44.21
- Gateway IP: (empty)

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

4. Click the “apply changes” button.

---

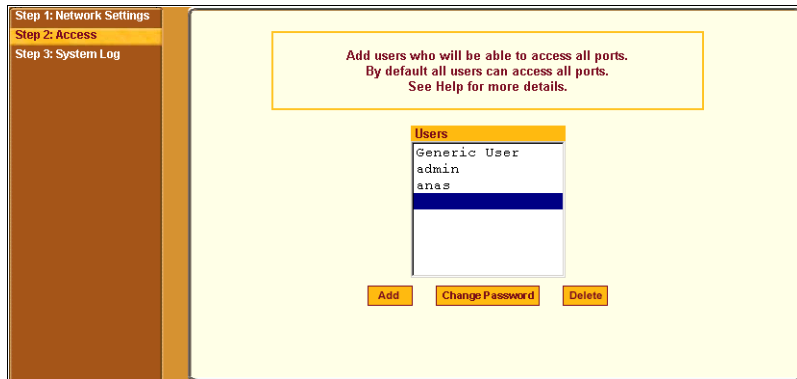
**Warning!** If you change the KVM/net Plus’ IP address and apply the changes, you will need to reconnect to the Web Manager with the new IP address.

---

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

## Step 2: Access [Wizard]

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



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

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

- Admin
- Generic User

The Admin (the “admin” account) has access to all functions of the Web Manager and has access to all ports on the KVM/net Plus.

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

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

---

To Add a User [Wizard]	Page 145
To Delete a User [Wizard]	Page 147
To Change a Password [Wizard]	Page 147

---

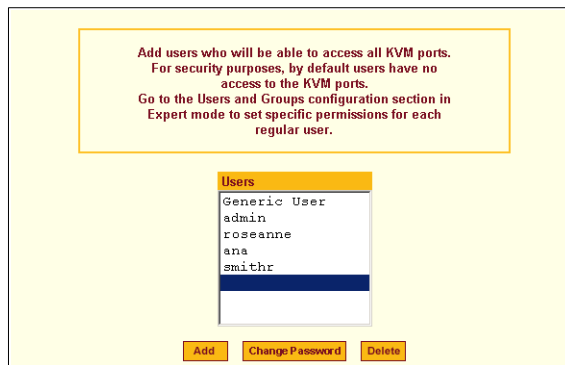
**Note:** To perform advanced configuration of users and groups, for example, to restrict user access to KVM ports, or to create a group, go to Expert>Configuration>Users and Groups.

---

## ▼ **To Add a User [Wizard]**

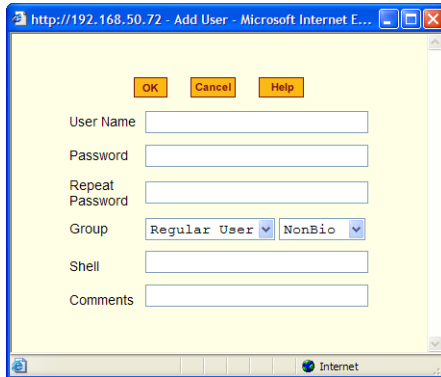
1. In Wizard mode, go to Step 3: Access.

The Access form appears.



2. Click Add.

The “Add User” dialog box appears.



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

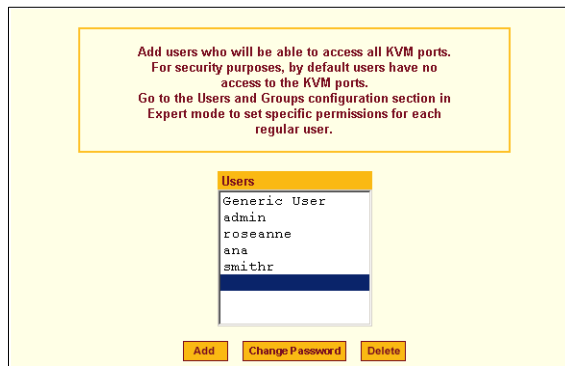
Field Name	Definition
<b>User Name</b>	The username for the account being added.
<b>Password</b>	The password for the account.
<b>Group</b>	On the drop-down list, Select Regular User [Default] or Admin. <b>Note:</b> To configure a user to be able to perform all KVM/net Plus administration functions, select the “Admin” group. See “Types of Users” on page 20, if needed, for more background.
<b>Shell</b>	Optional. The default shell when the user makes a ssh or telnet connection with the switch. Choices are: sh or bash. The default is sh.
<b>Comments</b>	Optional notes about the user’s role or configuration.

4. Click OK.
5. Click the “apply changes” button.

## ▼ **To Delete a User [Wizard]**

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

The “Access” form appears.



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

The username disappears from the Users list.

3. Click the “apply changes” button.

## ▼ **To Change a Password [Wizard]**

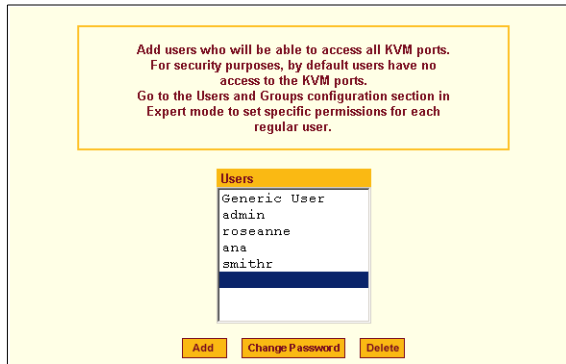
---

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

---

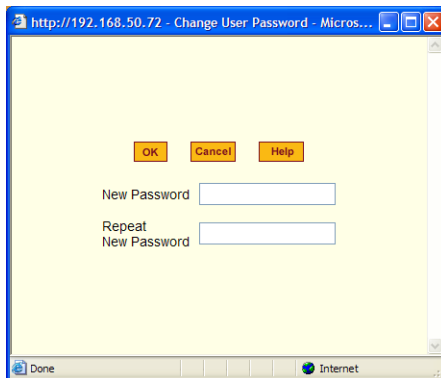
1. In Wizard mode, go to “Step 3: Access.”

The “Access” form appears.



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

The “Change User Password” dialog box appears.



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

## Step 3: System Log [Wizard]

In Wizard mode, selecting “Step 3: System Log” brings up a form for identifying one or more syslog servers to receive syslog messages from the KVM/net Plus.

Before performing this procedure, make sure an already-configured syslog server is available to the KVM/net Plus.

Obtain the following information from the syslog server’s administrator:

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net Plus

Each syslog server has eight local facility numbers (Local 0 through Local 7) that the syslog server’s administrator can assign and use for handling log messages from different locations. See “Syslog Servers” on page 52, if needed, for more background on logging and on how facility numbers are used.

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

To Add a Syslog Server [Wizard]	Page 150
To Delete a Syslog Server [Wizard]	Page 150

Use this form to configure system logging for the KVM/net Plus. More advanced configuration of syslog servers and event notification can be done in Expert mode. To configure system logging for messages relating to KVM

ports, in Expert mode go to “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 215.

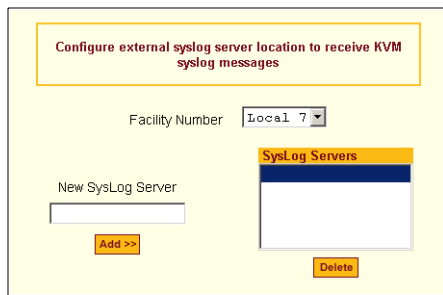
## ▼ **To Add a Syslog Server [Wizard]**

This procedure assumes you have the following information:

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net Plus

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

The System Log form appears.



The screenshot shows a web form titled "Configure external syslog server location to receive KVM syslog messages". It features a "Facility Number" dropdown menu currently set to "Local 7". Below this is a "New SysLog Server" text input field with an "Add >>" button to its right. To the right of the input field is a "SysLog Servers" list box, which is currently empty, with a "Delete" button below it.

2. From the Facility Number drop-down list, select the facility number.

3. In the New Syslog Server field, enter the IP address of a syslog server, and select the Add button. (Repeat this step until all syslog servers are listed.)

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

5. Click “apply changes.”

## ▼ **To Delete a Syslog Server [Wizard]**

1. From the Syslog Server list, select the syslog server that you want to delete from the current facility location, and select Delete.

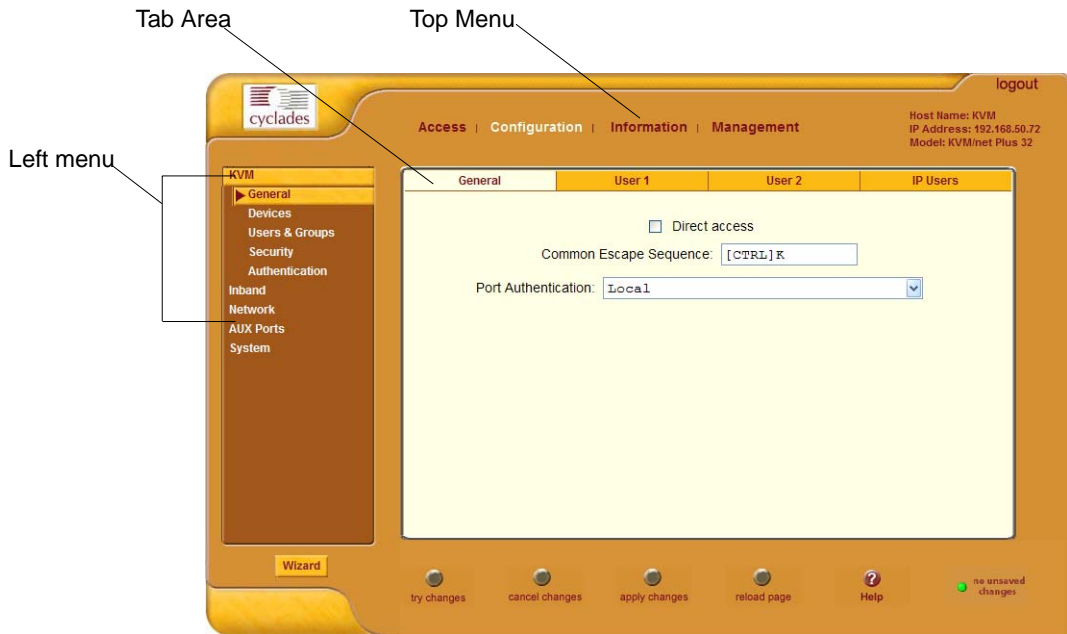
2. Repeat this step for as many servers you need to delete.

3. Click “apply changes.”



# Expert Mode

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



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

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

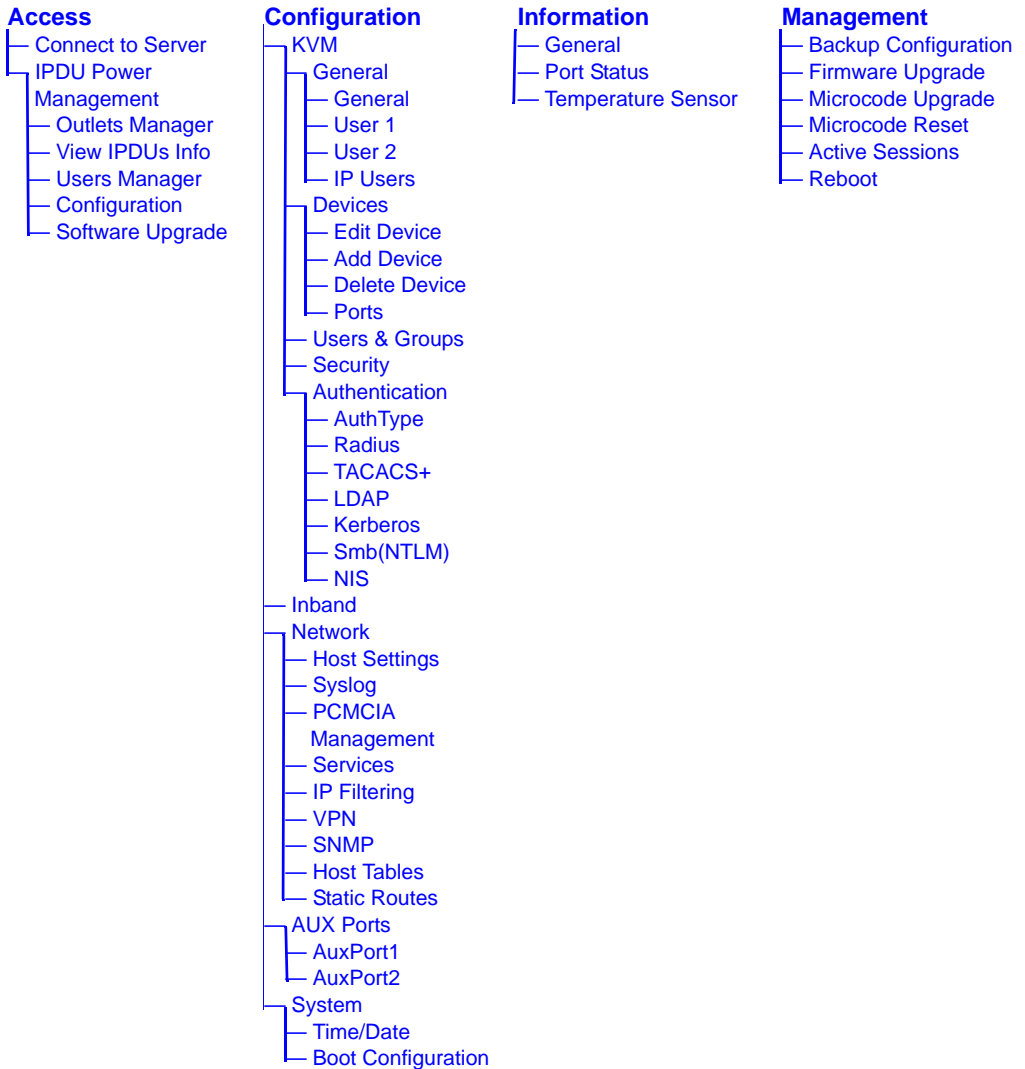
---

**Note:** Procedures in this manual use shortcuts to tell how to get to Web Manager forms. For example, a step telling the user to access the “IP Users” form in the right tab in the previous figure would use this convention, “In Expert mode, go to Configuration>KVM>General>IP Users.”

---

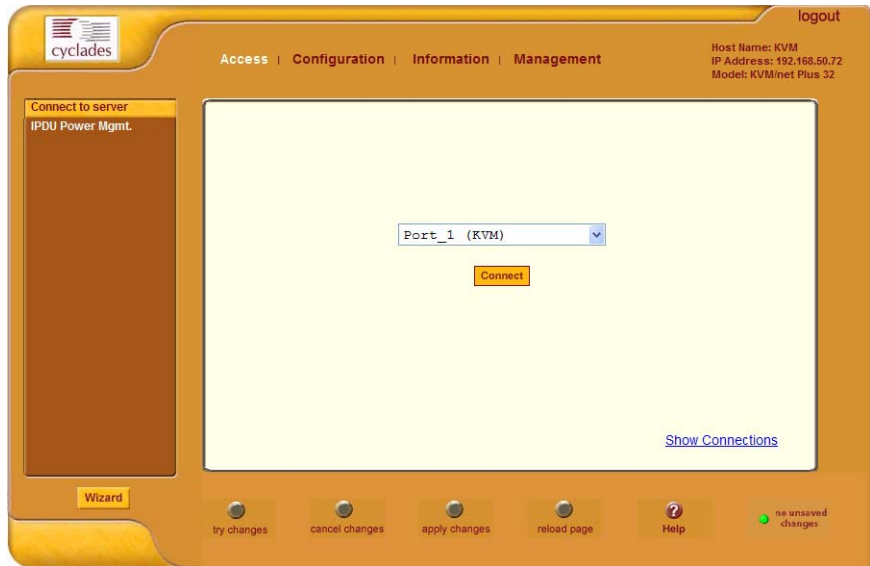
## Overview of Menus and Forms in Expert Mode

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



# Access

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



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

- “Connect to Server” on page 153
- “IPDU Power Management” on page 154

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

## ***Connect to Server***

On the “Connect to Server” form under Access, you can connect to servers that are connected to KVM ports or to in-band servers that use RDP (Remote Desktop Protocol). Chapter 6: Accessing Connected Devices discusses connecting to servers in more detail.

## IPDU Power Management

On the “IPDU Power Management” forms under “Access” in Expert mode, you can manage power of devices that are plugged into the outlets on one or more intelligent power distribution units (IPDUs).



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

- An AlterPath PM or is connected to the AUX 1 port on the KVM/net Plus. The AlterPath PM can be daisy chained to allow you to manage power for up to 128 devices from the KVM/net Plus.

See “To Connect a PM to the AUX 1 Port” on page 117 for installation procedures.

- The AUX port is configured for power management.

See “To Configure the AUX 1 Port for Use With a PM” on page 251.

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

- “Outlets Manager” on page 155
- “View IPDUs Info” on page 156
- “Users Manager” on page 157
- “Configuration” on page 159
- “Software Upgrade” on page 160

















See the following sections for related procedures:

- “To View Status, Lock, Unlock, and Cycle Power Outlets” on page 156
- “To View and Reset IPDU Information” on page 157
- “To Configure Users to Manage Specific Power Outlets” on page 158
- “To Configure Creation of Alarms and Syslog Files for IPDUs” on page 160
- “To Upgrade Firmware on an AlterPath PM” on page 161

## Outlets Manager

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

- Check the status
- Turn on
- Turn off
- Cycle (by briefly switching the outlet off and on)
- Lock
- Unlock

Outlets Manager	View IPDUs Info	Users Manager	Configuration	Software Upgrade
<b>Device/Port: master/AUX</b>				
Outlet	Outlet Name	Outlet State	Power Up Interval	
1	out1	  Cycle	0.50	
2	out2	  Cycle	0.50	
3	out3	  Cycle	0.50	
4	out4	  Cycle	0.50	
5	out5	  Cycle	0.50	
6	out6	  Cycle	0.50	
7	out7	  Cycle	0.50	
8	out8	  Cycle	0.50	

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

1. In Expert mode, go to Access>Power Manage IPDU>Outlets Manager.

The “Outlets Manager” form appears.

Yellow bulbs indicate an outlet is switched on and an opened padlock indicates that the outlets are unlocked. An orange “Cycle” button is active next to each outlet that is on.

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

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

1	out1				0.50
2	out2				0.50

4. To power an outlet off and quickly power it on again, click the adjacent “Cycle” button.
5. Click “apply changes.”

### **View IPDUs Info**

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

- Number of outlets on each unit
- Current
- Temperature
- Alarm threshold levels
- Firmware version

You can also clear values for the maximum current and the maximum temperature.

Outlets Manager	View IPDUs Info	Users Manager	Configuration	Software Upgrade
<b>AUX Port 1: General Information</b>		<input type="button" value="Clear Max Detected Current"/> <input type="button" value="Clear Max Detected Temperature"/>		
Name: PowerMgm-1	Syslog: ON	Number of Outlets: 8		
Number of Units: 1	Buzzer: ON	Over Current Protection: OFF		
<b>Master Unit Information:</b>				
Model: PM8 20A	Software Version: 1.5.0			
Alarm Threshold: 20.0A				
Current: 0.0A	Maximum Detected: 1.3A			
Temperature:	Maximum Detected:			

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

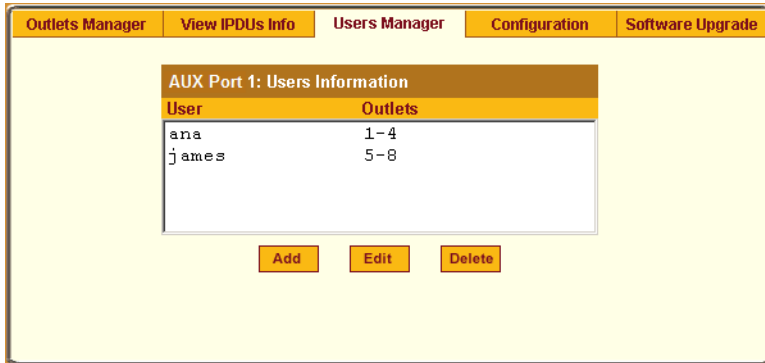
1. In Expert mode, go to Access>IPDU Power Management>View IPDUs Info.

The “View IPDUs Info” form appears.

2. To clear the stored values for the maximum detected current, select the “Clear Max Detected Current” button.
3. To clear the stored values for the maximum detected temperature, click the “Clear Max Detected Temperature” button.
4. Click “apply changes.”

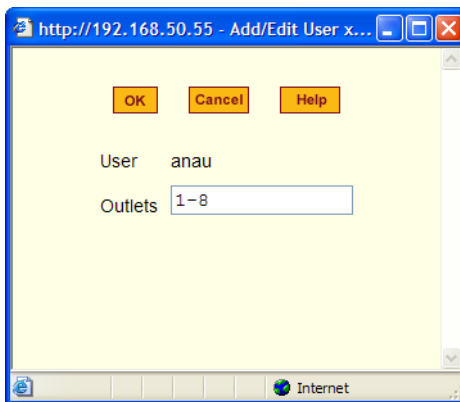
### **Users Manager**

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



▼ **To Configure Users to Manage Specific Power Outlets**

1. In Expert mode, go to Access>IPDU Power Management>Users Manager.  
The “Users Manager” form appears.
2. To remove a user’s ability to manage power, select the username and click “Delete.”
3. To edit a user, select the username from the view table and click “Edit.”  
Skip to Step 5..  
The “Add/Edit User x Outlets” dialog box appears.



4. To add a new user, click “Add.”  
The “Add/Edit User x Outlets” dialog box appears.
5. In the “Add/Edit User x Outlets” dialog box, do the following as appropriate.



- a. Enter the username in the “User” field.
- b. Enter or modify the numbers of the outlets to which the user is assigned in the “Outlets” field.

Use a comma to separate outlet numbers, and use a hyphen to indicate a range of outlets (for example: 1, 3, 6, 9-12).

6. Click OK.

7. Click “apply changes.”

## Configuration

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

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

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

The Configuration form shows the ports that are currently connected to IPDUs. The following figure displays an example form that appears for a KVM/net Plus with an AlterPath PM connected to AUX 1 port.

### ▼ To Specify or Change the Alias of an IPDU

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

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

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

### ▼ **To Configure Creation of Alarms and Syslog Files for IPDUs**

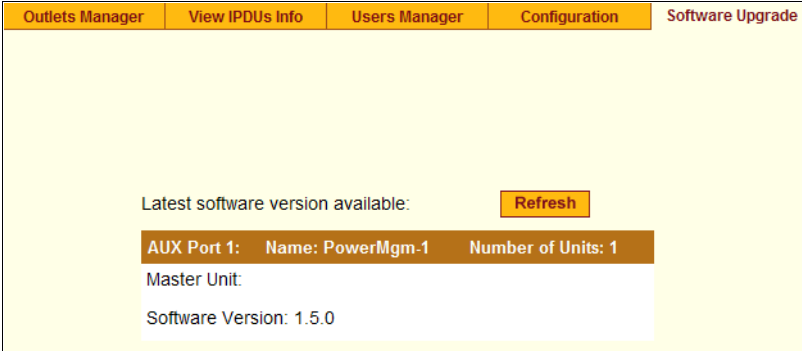
1. In Expert mode, go to Access>IPDU Power Management>Configuration.  
The Configuration form displays entries for all ports configured for power management.
2. Click the appropriate check boxes to enable or disable Over Current Protection, the generation of Syslog files, and the sounding of a Buzzer if a defined threshold is exceeded.

An alarm sounds on the PM, not the KVM/net Plus.

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

### **Software Upgrade**

On the “Outlets Manager” form under Access>IPDU Power Management in Expert mode, you can upgrade the Power Management firmware for AlterPath PM IPDUs.



The screenshot shows a web interface with a navigation bar at the top containing five tabs: "Outlets Manager", "View IPDUs Info", "Users Manager", "Configuration", and "Software Upgrade". The "Software Upgrade" tab is active. Below the navigation bar, the main content area displays the following information:

- Latest software version available: [Refresh](#)
- AUX Port 1: Name: PowerMgm-1 Number of Units: 1
- Master Unit:
- Software Version: 1.5.0

An entry appears for every connected PM and for each slave. The version of the currently installed firmware displays on the form. If the KVM/net Plus has access to the Internet, clicking the Refresh button checks for a more-recent version of the PM firmware at the Cyclades website.

If the KVM/net Plus does not have access to the Internet, upgrade is possible only if you first download a more-recent version of the PM firmware onto the KVM/net Plus.

## ▼ **To Upgrade Firmware on an AlterPath PM**

Perform this procedure if the firmware on a connected AlterPath PM is older than the most-recent firmware available at Cyclades, Corp.

This procedure requires one of the two following prerequisites be met:

- The KVM/net Plus has access to the Internet so that it can automatically download the PM firmware from the Cyclades FTP server.

OR

- An Update button appears on the form.

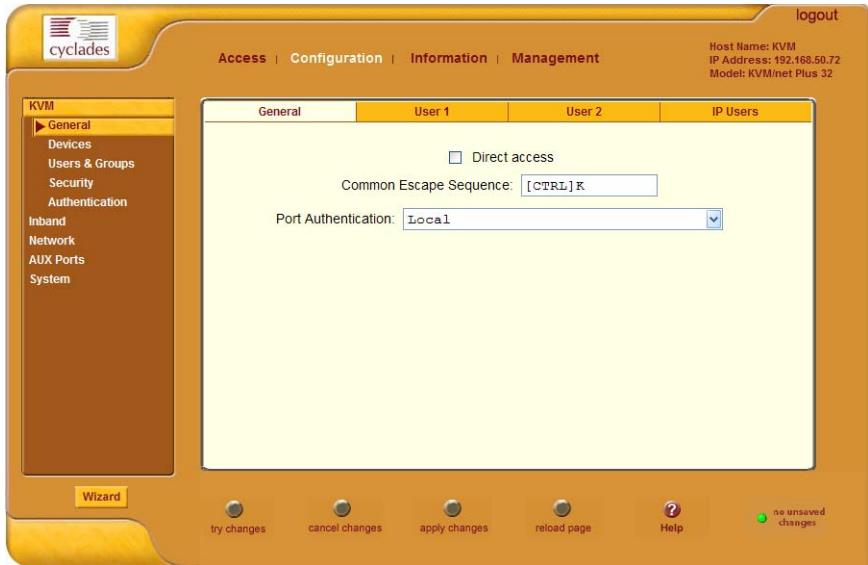
An Update button appears on the Access>Power Management>Software Upgrade form if a copy of a more-recent version of the AlterPath PM firmware exists in the KVM/net Plus' /tmp directory under the filename: /tmp/pmfirmware.

1. If the KVM/net Plus can contact the Cyclades FTP server, and if a more recent version of the firmware is available at Cyclades, download the updated firmware onto the KVM/net Plus.
  - a. Download the firmware onto a computer with a direct connection to the KVM/net Plus.
  - b. Copy the firmware file to the KVM/net Plus and put it in: /tmp/pmfirmware.
2. In Expert mode, go to Access>Power Management>Software Upgrade. The Software Upgrade form appears.
3. If the KVM/net Plus has access to the Internet, click the Refresh button.
 

The KVM/net Plus contacts the Cyclades website to check if a more recent version of the PM firmware is available. If a more recent version is available, the KVM/net Plus downloads it from Cyclades and installs it on the PM.
4. Click "Update."
5. Click "apply changes."

# Configuration

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

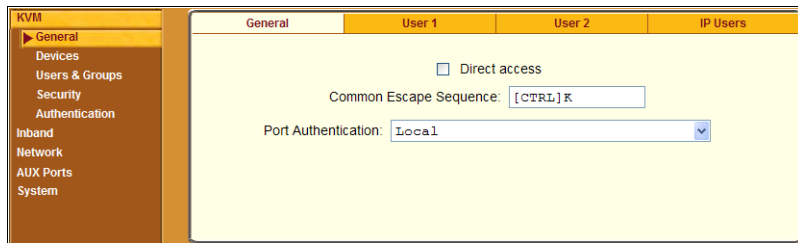


See the following sections for details about the tasks performed using the forms under Configuration in Expert mode:

- “KVM” on page 163
- “Configuring In-band (RDP) Servers” on page 203
- “Network” on page 209
- “AUX Ports” on page 250
- “System” on page 253

## KVM

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

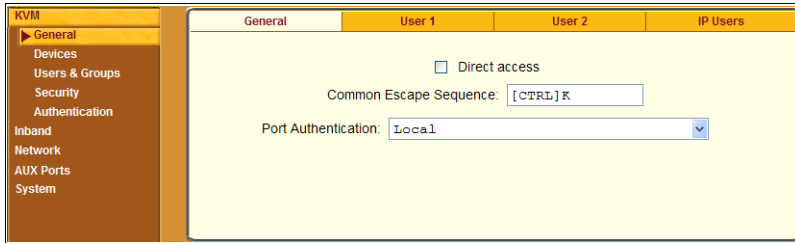


You can use the KVM menu options for custom configuration of KVM ports. The following table provides links to the sections where the options are described.

Web Manager Form	Where Documented
General	“General” on page 164
Devices	<ul style="list-style-type: none"> <li>• “Configuring Individual KVM Ports” on page 172</li> <li>• “Configuring Cascaded KVM Units” on page 177</li> </ul>
Users & Groups	“Users & Groups” on page 181
Security	“Security” on page 189
Authentication	<ul style="list-style-type: none"> <li>• “Configuring an Authentication Method” on page 191</li> <li>• “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194</li> </ul>

## General

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



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

---

General	“General” on page 164.
User 1, User 2, and IP Users	“Local User and IP Users” on page 168

---

## General

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

---

Parameter Name	Definition	Where Documented
Direct Access	Selecting this check box enables logins to KVM ports directly from the Web Manager Login screen.	<ul style="list-style-type: none"> <li>• “Enabling Direct Access to KVM Ports” on page 165</li> <li>• “To Enable Direct Access to KVM Ports” on page 165</li> </ul>

---

Parameter Name	Definition	Where Documented
Common Escape Sequence	Redefines keyboard shortcuts used during local KVM connections	<ul style="list-style-type: none"> <li>• “Redefining KVM Connection Keyboard Shortcuts (Hot Keys)” on page 166</li> <li>• “To Redefine KVM Session Keyboard Shortcuts” on page 166</li> </ul>
Authentication Type	Allows you to choose whether authentication is required for KVM port logins. If needed, see the introduction to authentication on the KVM/net Plus under “Authentication” on page 48.	<ul style="list-style-type: none"> <li>• “Specifying Authentication for KVM Port Logins” on page 167</li> <li>• “To Specify an Authentication Method for KVM Port Logins” on page 167</li> </ul>

### ***Enabling Direct Access to KVM Ports***

When direct access to KVM ports is enabled, users authorized to access KVM ports can use a port field on the Web Manager login screen to log in and connect directly to the port. See “To Log Into the Web Manager as Admin” on page 138, if desired, for an example of the login screen when direct login is enabled.

#### **▼ To Enable Direct Access to KVM Ports**

1. Go to Configuration>KVM>General in Expert mode.  
The General form appears.
2. Select the “Direct access” check box.
3. Click “apply changes.”

## ***Redefining KVM Connection Keyboard Shortcuts (Hot Keys)***

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

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

	<b>Common Escape Sequence</b>	<b>Command Key</b>	<b>Where Defined</b>
<b>Format</b>	“Ctrl” + “letter key”	“letter key”	<ul style="list-style-type: none"> <li>• Configuration&gt;KVM&gt;General&gt;General</li> </ul>
<b>Defaults</b>	Ctrl+k	<p>“p” to bring up the “power management” window, “q” to quit, and so forth. See Table 6-7, “Default Local Keyboard Shortcuts Through the OSD,” on page 323 for all the default command keys.</p>	<ul style="list-style-type: none"> <li>• Configuration&gt;KVM&gt;General&gt;User 1</li> <li>• Configuration&gt;KVM&gt;General&gt;User 2</li> <li>• Configuration&gt;KVM&gt;General&gt;IP Users</li> </ul>

### **▼ To Redefine KVM Session Keyboard Shortcuts**

1. Go to Configuration>KVM>General in Expert mode.  
The General form appears.
2. To redefine the “Common Escape Sequence” enter a key combination starting with the Ctrl key and followed by a letter, for example, **Ctrl m**.
3. To redefine the command key portion of any KVM-session keyboard shortcuts, do one of the following steps.
  - To change the command key for administrators who access KVM ports through the User 1 port, go to the User 1 tab.



- OR -

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

- OR -

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

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

### ***Specifying Authentication for KVM Port Logins***

Choice of authentication types for KVM ports are:

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

#### **▼ *To Specify an Authentication Method for KVM Port Logins***

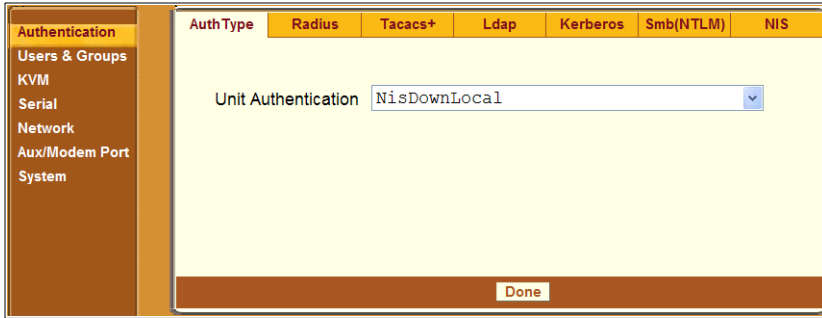
This procedure configures a single authentication method that applies whenever anyone attempts to log into a device through a connected KVM port.

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

The General form appears.

2. Select an authentication method from the Authentication drop-down list.

The default option is None.



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

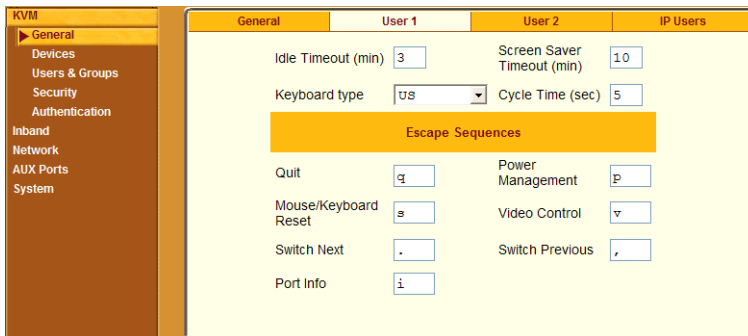
The changes are stored in `/etc/kvmd.conf` on the KVM/net Plus.

5. If you select any authentication method other than None or Local, make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194.

### Local User and IP Users

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



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

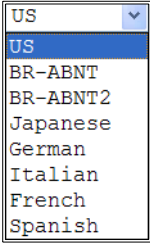
redefine the default session parameters that apply when a user is using the OSD through a KVM RP connection to the User 2 port on the KVM/net Plus.

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

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

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

Field Name	Definition
<b>Idle Timeout</b>	Sets the maximum time (in minutes) for the session to be idle before it is closed. The maximum value is 60 minutes. A value of 0 disables the idle timeout.
<b>Screen Save Timeout</b>	Sets the time (in minutes) for the session to be idle before the screen saver activates. The maximum value is 60 minutes. A value of 0 disables the idle timeout. [User 1 and User 2 only.]

Field Name	Definition
<b>Keyboard Type</b>	<p>Sets the keyboard type. [User 1 and User 2 only.] Choose the type of keyboard connected to the User 1 and User 2 ports on the KVM/net Plus. The options from the drop-down list are shown in the figure.</p> 
<b>Cycle Time</b>	<p>Change the cycle time (in seconds) within the following range: 3 to 60 seconds. [User 1 and User 2 only.]</p>
<b>TCP Viewer Ports</b>	<p>Change the number of the TCP port used for the AlterPath Viewer. [IP Users only.] The default is 5900+. You may need to change the default, for example, if your firewall is blocking port 5900. (For more details, see “TCP Ports” on page 26.) Port numbers 1-1024 are reserved. Indicate a range of ports by entering a plus sign (+) after the first port number (as in 2500+) or by entering a dash between two port numbers (as in 2500-2501). Indicate a set of nonadjacent port numbers by separating port numbers with commas (as in 2500, 2508).</p>

On the “User 1” and “User 2” and “IP Users” forms, you can also redefine the command key portion of keyboard shortcuts for each type of user. For more information about redefining keyboard shortcuts, see “Redefining Keyboard Shortcuts (Hot Keys)” on page 40 and “To Redefine KVM Session Keyboard Shortcuts” on page 166 if needed.

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

To Configure IP User (KVM Over IP) Sessions	Page 172
To Redefine KVM Session Keyboard Shortcuts	Page 166

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

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a local user is directly logged into the KVM/net Plus.

1. In Expert mode, go to Configuration>KVM>General>.
2. To configure parameters for the User 1 port, select the User 1 tab.

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

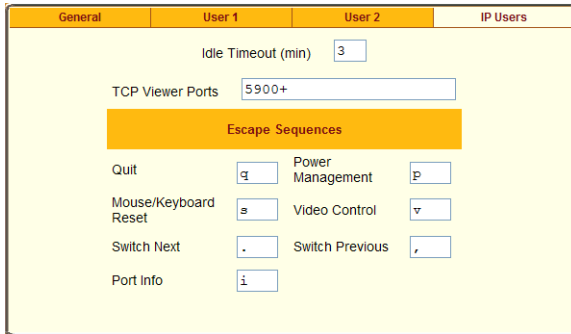
The User 1 and User 2 forms are identical except that User 1 modifies the User 1 port options, while User 2 modifies the User 2 port options.

4. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.
5. To change the screen saver timeout, enter a different number of minutes in the “Screen Saver Timeout” field.
6. To change the keyboard type, select a different keyboard from the “Keyboard type” drop-down list.
7. To change the cycle time, enter a different number of seconds in the “Cycle Time” field.
8. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
9. Click “apply changes.”

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

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

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



General	User 1	User 2	IP Users
Idle Timeout (min) <input type="text" value="3"/>			
TCP Viewer Ports <input type="text" value="5900+"/>			
<b>Escape Sequences</b>			
Quit	<input type="text" value="q"/>	Power Management	<input type="text" value="P"/>
Mouse/Keyboard Reset	<input type="text" value="s"/>	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"/>		

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

## **Configuring Individual KVM Ports**

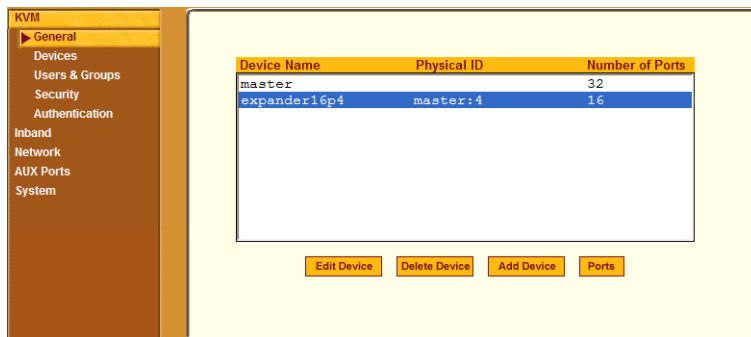
On the Modify Port dialog box, you can do the following:

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

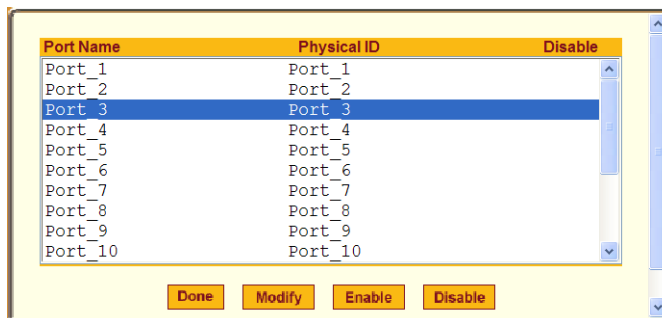
The following table lists the related procedures with links to where they are described.

To Configure a KVM Port for Power Management	Page 174
To Specify or Change the Alias for a KVM Port	Page 176
To Enable or Disable a KVM Port	Page 176

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

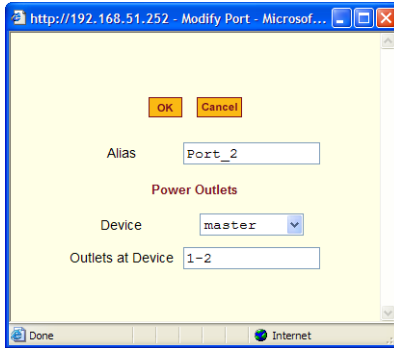


The device name “master” stands for the KVM/net Plus, which is the master KVM unit in a cascaded configuration. Other device names may appear below “master” depending on the number of KVM units cascaded to the master. Selecting the name of a KVM unit in the list and clicking the “Ports” button brings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



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

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



### ▼ **To Configure a KVM Port for Power Management**

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

- The computer is plugged into an IPDU connected to the KVM/net Plus’ AUX 1 port.
- The AUX 1 port has been configured for power management.  
See “To Configure the AUX 1 Port for Use With a PM” on page 251, if needed.
- You know the outlet number or numbers to which the computer’s power cable or cables are plugged.

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

The Devices form appears.

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

The Port Name list appears.



Port Name	Physical ID	Disable
FremWin98	Port_1	
FremNT	Port_2	
FremLin2	Port_3	
Port_4	Port_4	Yes
Port_5	Port_5	
Port_6	Port_6	Yes
Port_7	Port_7	
Port_8	Port_8	
Port_9	Port_9	
Port_10	Port_10	

Done    Modify    Enable    Disable

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

The Modify Port dialog box appears.

4. In the Alias field, type an alias for the port
5. In the Device drop-down list, select the device that port is on.  
The device could be the master KVM/net Plus or a cascaded KVM unit.
6. In the Outlets at Device field, type the outlet number(s) of the IPDU that the server is plugged into.  
Use commas (,) to separate outlets and use a hyphen (-) to indicate a range.
7. Click the OK button.
8. Click the “apply changes” button to save your configuration.

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

1. Go to Configuration>KVM>Devices in Expert mode, select the device that includes the port(s) you wish to modify.
2. Click the “Ports” button.  
A list of all the selected ports appears.
3. Select a single port to be modified, and then select the “Modify” button.  
The “Modify Port” dialog box appears.
4. To change the port’s alias, do the following steps.
  - a. Enter a new alias in the “Alias” field.
  - b. Click OK on the dialog box.
5. Click “Done” on the form listing all the ports.
6. Click “apply changes.”

### ▼ **To Enable or Disable a KVM Port**

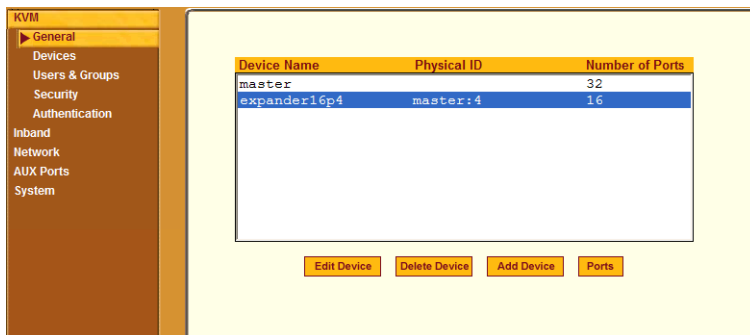
1. Go to Configuration>KVM>Devices in Expert mode, and select the device that contains the port(s) you wish to enable or disable.
2. Click the “Ports” button.  
A form listing all the selected ports appears.
3. Select the port(s) to be enabled or disabled, and then select the “Enable” or “Disable” button.
4. Click “Done” on the form listing all the ports.
5. Click “apply changes.”

## Configuring Cascaded KVM Units

The Devices form allows you to configure one or more secondary KVM units to a primary KVM unit, a process also known as cascading or daisy-chaining. See “Cascaded Devices” on page 27 for background information.

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

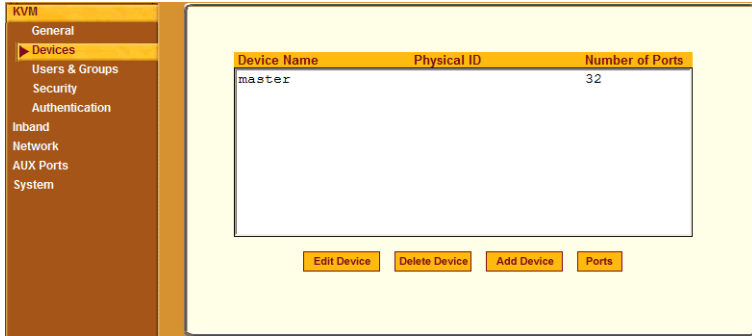
- Add a secondary KVM unit to be cascaded from the master KVM/net Plus.  
See “To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net Plus” on page 178
- Edit the configuration of a cascaded device.  
See “To Edit the Configuration of a Cascaded KVM Unit” on page 179
- Delete the configuration of a cascaded device.  
See “To Delete the Configuration of a Cascaded KVM Unit” on page 181



▼ **To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net Plus**

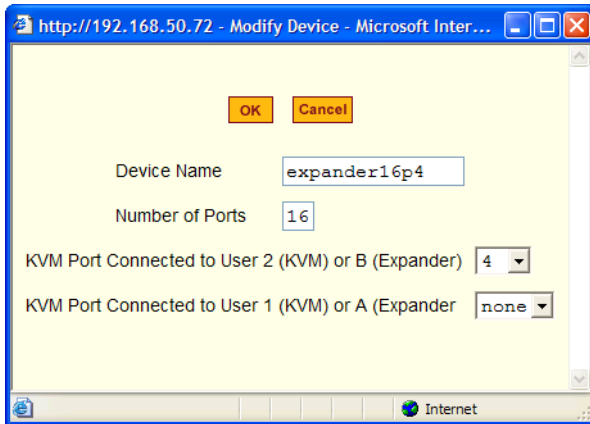
1. In Expert mode, go to: Configuration>KVM>Devices.

The Devices configuration form appears.



2. Click the Add Device button.

The Modify Device dialog box appears.



3. In the Device Name field, specify a name for the secondary device or KVM unit.
4. In the Number of Ports field, enter the number of ports contained in the cascaded device.
5. In the KVM Port Connected to User 2 (KVM) or B (Expander) drop-down list, enter the port number of the master KVM/net Plus that is connected to

the User 2 port of the secondary KVM device or the B port on the Expander.

---

**Note:** See “Connecting Cascaded KVM Units to the Primary KVM/net Plus” on page 126 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net Plus.

---

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

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

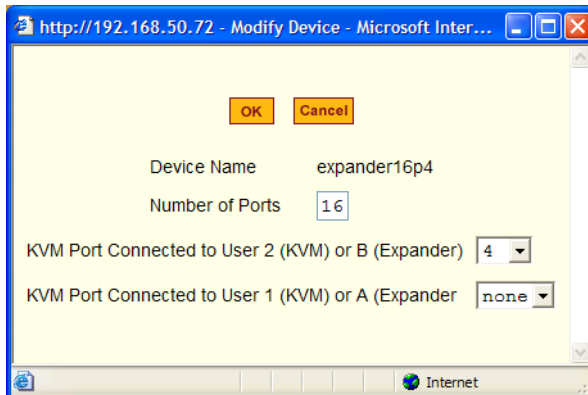
1. In Expert mode, go to: Configuration>KVM>Devices.

The Devices form appears.

Device Name	Physical ID	Number of Ports
master		32
expander16p4	master:4	16

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

The Modify Port dialog box appears.



3. In the Number of Ports field, enter the number of ports contained on the cascaded device.
4. To enable one user to access the ports on the cascaded KVM unit, in the KVM Port Connected to User 2 (KVM) or B (Expander) drop-down list, select the port number on the master KVM/net Plus that is connected to the User 2 port on the secondary KVM device or the B port on the Expander.

---

**Note:** See “Connecting Cascaded KVM Units to the Primary KVM/net Plus” on page 126 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net Plus.

---

5. To enable two users to access the ports on the cascaded KVM unit, in the Port Connected to User 1 or (KVM) or A (Expander) drop-down list, enter the secondary KVM port that is connected to the User 1 port of the primary KVM/net Plus or the User A port on the Expander.
6. Click the OK button.
7. Click “apply changes” to save your configuration.

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

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

The Devices form appears.

Device Name	Physical ID	Number of Ports
master		32
expander16p4	master:4	16

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

The system deletes the selected device.

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

## Users & Groups

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

KVM

- General
- Devices
- Users & Groups
- Security
- Authentication
- Inband
- Network
- AUX Ports
- System

User List

Generic User
admin
anas

Group List

--

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

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

---

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

---

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

### ▼ **To Add a User [Expert]**

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

The Users & Groups form appears.

2. Click “Add.”

The “Add User” dialog box appears.



The screenshot shows a web browser window with the address bar displaying 'http://192.168.50.72 - Add User - Microsoft Internet Explorer'. The main content area has a yellow background and contains the following form elements:

- Two buttons at the top: 'OK' and 'Cancel'.
- 'User Name' field: contains the text 'johnr'.
- 'Password' field: contains seven black dots.
- 'Repeat Password' field: contains seven black dots.
- 'Group' field: a drop-down menu with 'Regular User' selected.
- 'Shell' field: is empty.
- 'Comments' field: contains the text 'Power on ports 1-4 and 8'.

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

Field Name	Definition
<b>User Name</b>	Name of the user to be added.
<b>Password</b>	The password associated with the user name.
<b>Group</b>	On the left drop-down list, select “Regular User [Default]” or “Admin.” <b>Note:</b> To configure a user to be able to perform all administrative functions, select the “Admin” group. See “Types of Users” on page 20 for more details.
<b>Shell</b>	Optional. The default shell when the user makes an <code>ssh</code> or <code>telnet</code> connection with the switch. Choices are: <code>sh</code> or <code>bash</code> . The default is <code>sh</code> .
<b>Comments</b>	Optional notes about the user’s role or configuration.

4. Click OK.

5. Click “apply changes.”

▼ **To Delete a User or Group [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.  
The Users & Groups form appears.
2. Select the name of a user or group to delete.
3. Click “Delete.”
4. Click “apply changes.”

▼ **To Change a User’s Password [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.  
The Users & Groups form appears.
2. Select the name of the user whose password you want to change.
3. Click “Change Password.”  
The Change User Password” dialog box appears.
4. Enter the new password in the “New Password” field and enter it again in the “Repeat New Password” field.
5. Click OK.
6. Click “apply changes.”

▼ **To Add a Group**

1. In Expert mode, go to Configuration>Users & Groups.  
The Users & Groups form appears.
2. Under the list of groups, click “Add.”  
The “Add Group” dialog box appears.
3. Type the name for the new group.
4. Type the usernames of the users you want to add to the group.  
Use commas to separate the names.
5. Click OK.
6. Click “apply changes.”

### ▼ **To Modify a Group**

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

The Users & Groups form appears.

2. Select the name of a group to modify.
3. Click “Edit.”  
The “Edit Group” form appears.
4. Add or delete users from the group as desired.
5. Click OK.
6. Click “apply changes.”

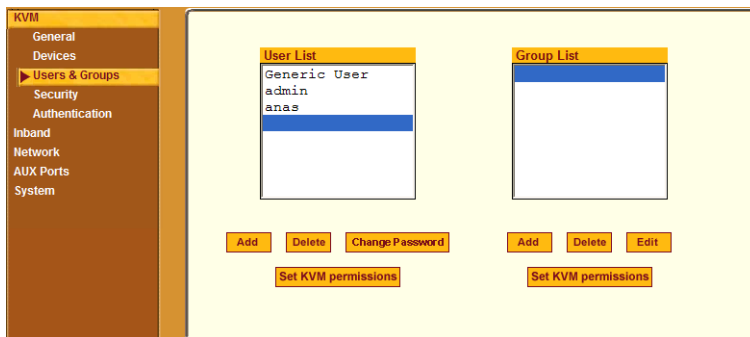
### ▼ **To Select Users and Groups for Assigning KVM Port Access**

Perform this procedure to select users to access computers connected to KVM ports.

1. Go to Expert>Configuration>Users & Groups.

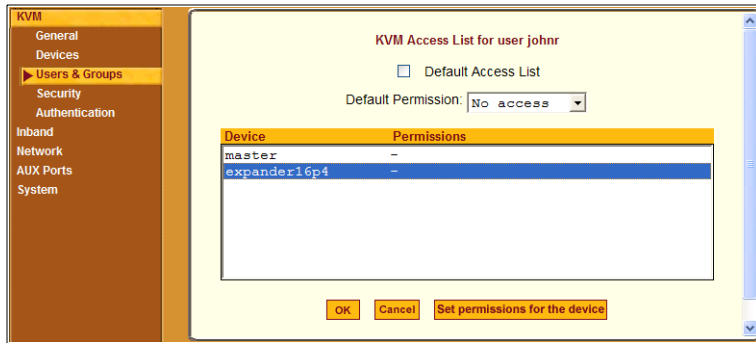
The Users & Groups form appears.

2. To set KVM port access for a regular user, select the name of the user or of multiple users from User List.



3. To set KVM port access permissions for a group, select the name of the group from the Group List.
4. Click the “Set KVM Permissions” button.

The “KVM Access list for “*username*” or “*groupname*” dialog box appears.



---

**Note:** When the “Default Access List” check box is checked, the user or group has the same permissions that are assigned to the Generic User. Changes made on this form when a username is selected convert the user into a non-generic user.

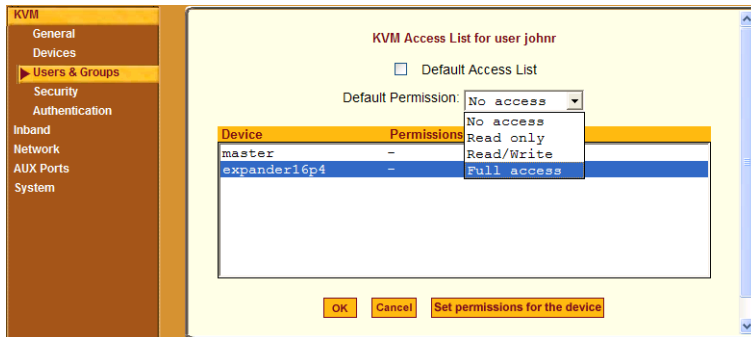
---

5. Go to “To Assign KVM Port Access to a User or Group” on page 186.

### ▼ **To Assign KVM Port Access to a User or Group**

Perform this procedure when you want to specify the types of access a user or group of users can have to computers that are connected to the KVM/net Plus’ KVM ports.

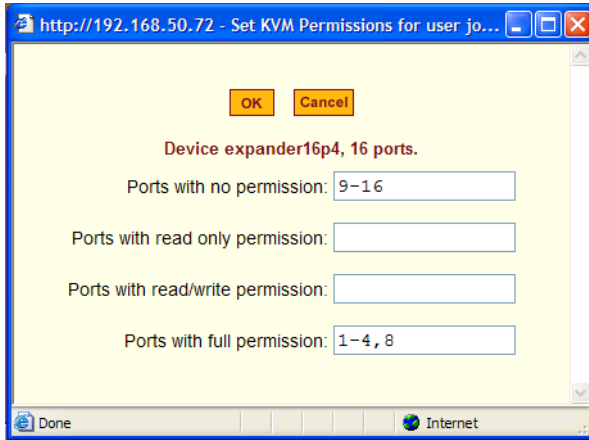
1. Go to Expert>Configuration>Users & Groups, and select a user or group.  
If needed see “To Select Users and Groups for Assigning KVM Port Access” on page 185.
2. To assign to the selected user or group the same permissions assigned to the Generic User, make sure the “Default Access List” check box is checked and click OK.
3. To re-define the KVM permissions for the selected user or group, clear the check box.
4. Select the desired access option from the “Default Permission:” drop-down list.



As shown in the previous screen example, the options are: “No access,” “Read only,” “Read/Write,” “Full access.”

5. To configure access to a device and all of its ports, do the following:
  - a. Select one or more devices from the Device list.
  - b. From the Default Permissions drop-down list, select the permissions you wish to apply.
  - c. Go to Step 8.
6. To configure access to individual ports or groups of ports, do the following:
  - a. Select a device from the Device list.
  - b. Click the “Set permissions for the device” button.

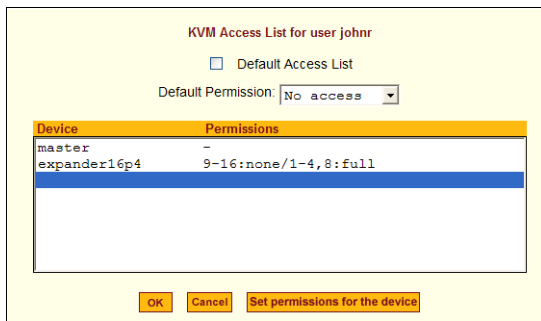
The “Set KVM Permissions for the device” dialog box displays as shown in the following screen example. (The example shows the dialog box when the “master” device is selected.)



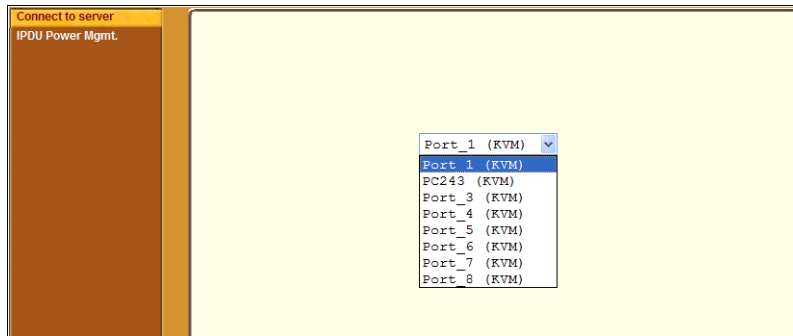
In the fields for each desired category, type either port aliases or numbers, separating them either by commas or dashes.

7. Click OK.

The newly set permissions appear next to the Device name in the Permissions column, as shown in the following screen example, which shows the restrictions applied to the user name “johnr.”



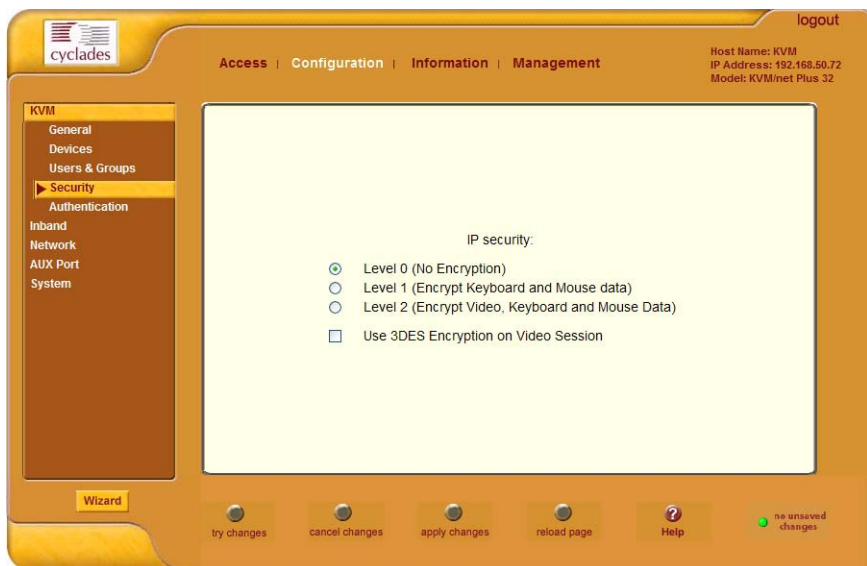
The following screen example illustrates how the previous settings affect access to ports. When an individual or member of a group with the access permissions shown in the previous screen logs into the Web Manager, the list of ports displayed does not include ports 9 to 16 (because they were configured with no access).



8. Click OK.
9. Click “apply changes.”

## Security

Selecting Configuration>KVM>Security in Expert mode brings up the form shown in the following figure. Administrators can specify that communications are encrypted between the KVM/net Plus and any computer attached to a KVM port.



The Security form allows you to configure your IP security with the following levels:

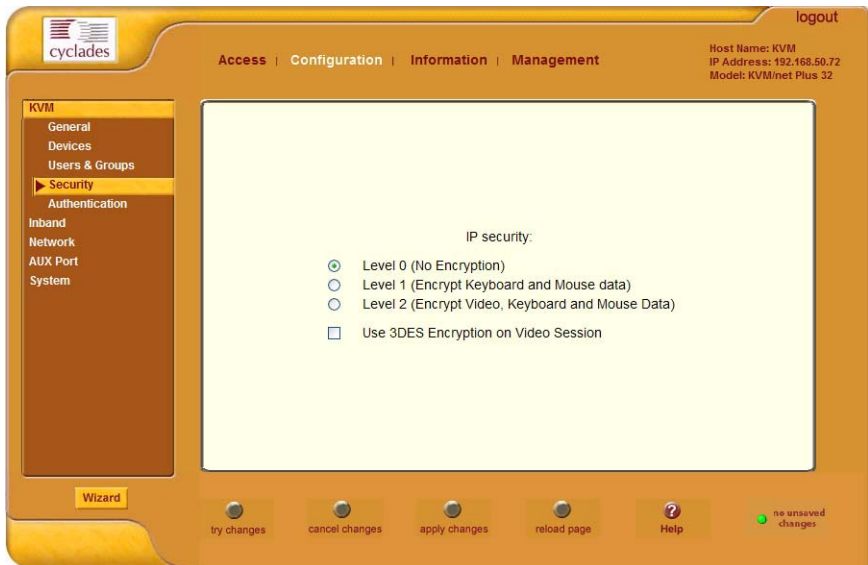
- Level 0 (No Encryption)
- Level 1 (Encrypt Keyboard and Mouse data)
- Level 2 (Encrypt Video, Keyboard and Mouse Data)

In addition, you can select 3DES (Triple Data Encryption Standard) for video sessions in stead of RC4 (Rivest Cipher four), the system default. Though RC4 is faster than 3DES, it is less secure.

### ▼ **To Configure Encryption on Port Connections [Expert]**

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

The Security form appears.



2. Check the appropriate radio buttons.

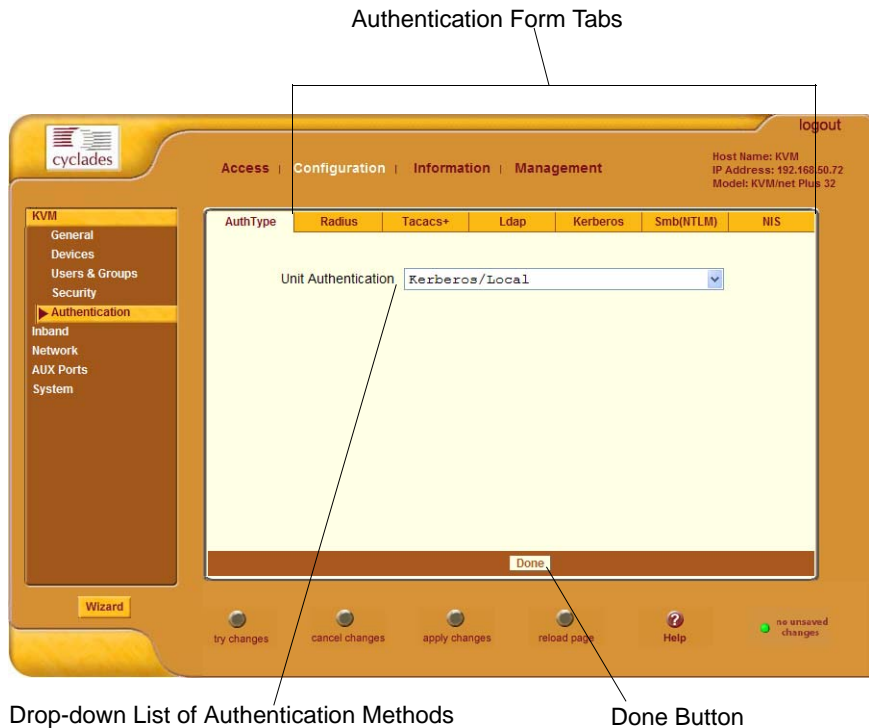
RC4 is the default encryption if 3DES is not selected. See “Security” on page 189, if needed, for more information.

3. Click “apply changes” to complete the procedure.



## Configuring an Authentication Method

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



The administrator uses the Authentication forms for two main purposes:

- To select an authentication method for the KVM/net Plus *only*.  
The default authentication method for the KVM/net Plus is Local. The administrator can either accept the default or select one of the other authentication methods from the drop-down list on the AuthType form. See “To Configure an Authentication Method for KVM/net Plus Logins” on page 192 for the procedure.  
Any authentication method chosen for the KVM/net Plus is used for authentication of any users attempting access through telnet, ssh, or the Web Manager.

See “Authentication” on page 48 for more details.

- To configure all authentication servers for the KVM/net Plus ports.

The administrator fills out one of the tabbed forms to set up an authentication server for each authentication method to be used by the KVM/net Plus and by any of its ports: RADIUS, TACACS+, LDAP, Kerberos, SMB (ports only), NIS. See “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194.

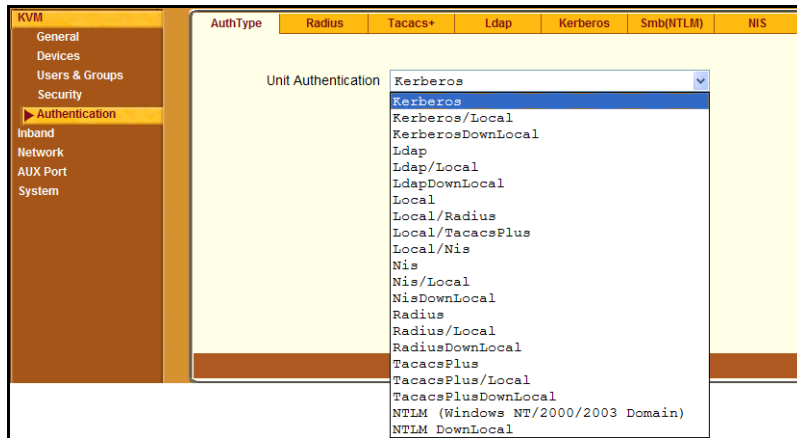
See “To Configure an Authentication Method for Logins Through KVM Ports” on page 193 for instruction on how to specify an authentication method for ports.

### ▼ **To Configure an Authentication Method for KVM/net Plus Logins**

See “Configuring an Authentication Method” on page 191, if needed, for background information.

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

The AuthType form displays, as shown in the following figure.



2. To specify an authentication method for logins to the KVM/net Plus, select a method from the Authentication drop-down list.
3. Make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194.

### ▼ **To Configure an Authentication Method for Logins Through KVM Ports**

By default, all users can log into all ports. This procedure configures a single authentication method that applies whenever anyone attempts to log into a device connected to any KVM port.

1. Go to Expert>Configuration>General.

The General form appears.

2. Select an Authentication Type from the drop-down list.

The default option is None.

3. Make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices” on page 194.

## ***Configuring Authentication Servers for Logins to the KVM/net Plus and Connected Devices***

The administrator fills out the appropriate form to set up an authentication server for every authentication method to be used by the KVM/net Plus and by any of its ports: Kerberos, LDAP, NIS, NTLM/SMB (ports only), RADIUS, TACACS+.

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

<b>Method</b>	<b>Variations</b>	<b>Procedures</b>
Kerberos	Kerberos, Local/Kerberos, Kerberos/Local, or Kerberos/DownLocal	“To Identify a Kerberos Authentication Server” on page 195
LDAP	LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal	“To Identify an LDAP Authentication Server” on page 197
NIS	NIS, Local/NIS, NIS/Local, or NIS/DownLocal	“To Configure a NIS Authentication Server” on page 200
NTLM (Windows NT/ 2000/2003 Domain)	NTLM (Windows NT/2000/2003 Domain), or NTLM/DownLocal	“To Configure an SMB(NTLM) Authentication Server” on page 199
RADIUS	RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal	“To Identify a RADIUS Authentication Server” on page 201
TACACS+	TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal	“To Identify a TACACS+ Authentication Server” on page 202

## ▼ **To Identify a Kerberos Authentication Server**

Perform this procedure to identify the authentication server when the KVM/net Plus or any of its ports is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local, or KerberosDownLocal.)

Before starting this procedure, find out the following information from the Kerberos server's administrator:

- Realm name and KDC address
- Host name and IP address for the Kerberos server

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the KVM/net Plus and connected devices know the passwords assigned to the accounts:

- An account for "admin"
- If Kerberos authentication is specified for the KVM/net Plus, accounts for all users who need to log into the KVM/net Plus to administer connected devices.
- If Kerberos authentication is specified for KVM ports, accounts for users who need administrative access to connected devices

**1.** Make sure an entry for the KVM/net Plus and the Kerberos server exist in the KVM/net Plus' `/etc/hosts` file.

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

The "Host Table" form appears.

b. Add an entry for KVM/net Plus if none exists and an entry for the Kerberos server.

i. Click "Add."

The "New/Modify Host" dialog appears.

ii. Enter the address in the "IP Address" field.

iii. Enter the name in the "Name" field.

iv. If desired, enter an optional alias in the "Alias" field.

**2.** Make sure that timezone and time and date settings are synchronized on the KVM/net Plus and on the Kerberos server.

Time and date synchronization is most easily achieved by setting both to use the same NTP server.

- a. To specify an NTP server, follow the procedure under “To Set The Time and Date With NTP” on page 255.
  - b. To manually set the time and date on the KVM/net Plus, follow “To Set the KVM/net Plus’ Date and Time Manually” on page 254.
  - c. Work with the authentication server’s administrator to synchronize the time and date between the KVM/net Plus and the server.
- 3.** If the KVM/net Plus is not located in the PST time zone, set the timezone on the KVM/net Plus.
- a. Make a console connection to the KVM/net Plus and log in as root,

```
KVM login: root
Password: *****
```

The root prompt appears.

```
[root@kvm root]#
```

- b. Enter **set\_timezone**.

A list of timezones appears followed by a prompt asking you to enter a number of a timezone.

```
[root@kvm root]# set_timezone
Please choose the time zone where this machine is located.
0) GMT
1) 1h West GMT
2)10h West GMT
...
26) 9h East GMT
Enter your option:
```

- c. Enter the number of the timezone where the KVM/net Plus is located.

```
Enter your option: 10
```

- d. Logout from the console session and close the terminal.

4. In the Web Manager Expert mode, go to Configuration>Authentication>Kerberos.

The Kerberos form displays as shown in the following figure.

5. Fill in the form according to your local setup of the Kerberos server.
6. Click “Done.”
7. Click “apply changes.”

### ▼ **To Identify an LDAP Authentication Server**

Perform this procedure to identify the authentication server when the KVM/net Plus or any of its ports is configured to use the LDAP authentication method or any of its variations (LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal).

Before starting this procedure, find out the following information from the LDAP server’s administrator:

- The distinguished name of the search base
- The LDAP domain name
- Whether to use secure LDAP
- The authentication server’s IP address

You can enter information in the following two fields, but an entry is not required:

- The LDAP password
- The LDAP user name

Work with the LDAP server's administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the KVM/net Plus and connected devices know the passwords assigned to the accounts:

- An account for “admin”
  - If LDAP authentication is specified for the KVM/net Plus, accounts for all users who need to log into the KVM/net Plus to administer connected devices.
  - If LDAP authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.
1. Go to Configuration>Authentication>LDAP in Expert mode.

The “LDAP” form displays with “LDAP Server” and “LDAP Search Base” fields filled in from the current values in the `/etc/ldap.conf` file.

The screenshot shows a configuration window with a yellow background and a brown header bar. The header bar contains several tabs: AuthType, Radius, Tacacs+, Ldap, Kerberos, Smb(NTLM), and NIS. The 'Ldap' tab is currently selected. Below the tabs, there are several input fields and a checkbox. The 'Ldap Server' field contains the text '127.0.0.1'. The 'Ldap Base' field contains 'dc=padl,dc=com'. There is a checkbox labeled 'Secure Ldap' which is currently unchecked. Below that are two empty input fields for 'Ldap User Name' and 'Ldap Password'. At the bottom of the form, there is a brown bar with a white button labeled 'Done'.

2. Supply the IP address of the LDAP server in the “LDAP Server” field.
3. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the “LDAP” Base field, change the base definition.

The default distinguished name is “dc,” as in `dc=value,dc=value`. If the distinguished name on the LDAP server is “o,” then replace `dc` in the base field with `o`, as in `o=value,o=value`.

4. Replace the default base name with the name of your LDAP domain.



For example, for the LDAP domain name cyclades.com, the correct entry is: `dc=cyclades,dc=com`.

5. Click “Done.”
6. Click “apply changes.”

The changes are stored in `/etc/ldap.conf` on the KVM/net Plus.

### ▼ **To Configure an SMB(NTLM) Authentication Server**

Perform the following to identify the authentication server if any of the ports is configured to use the NTLM (Windows NT/2000/2003 Domain) authentication method or NTLM/Downlocal.

1. Go to Configuration>Authentication>SMB(NTLM) in Expert mode.

The SMB(NTLM) form displays as shown in the following figure.

AuthType	Radius	Tacacs+	Ldap	Kerberos	Smb(NTLM)	NIS
<p>Domain: <input type="text"/></p> <p>Primary Domain Controller: <input type="text"/></p> <p>Secondary Domain Controller <input type="text"/></p> <p style="text-align: right;"><b>Done</b></p>						

2. Fill in the form according to your configuration of the SMB server.
3. Click “Done.”
4. Click “apply changes.”

### ▼ **To Configure a NIS Authentication Server**

Perform this procedure to identify the authentication server when the KVM/net Plus or any of its ports is configured to use the NIS authentication method or any of its variations (Local/NIS, NIS/Local, or NIS/DownLocal).

1. Go to Configuration>Authentication>NIS in Expert mode.

The NIS form displays as shown in the following figure.



The screenshot shows a web-based configuration form for NIS authentication. At the top, there is a horizontal menu with tabs for different authentication methods: AuthType, Radius, Tacacs+, Ldap, Kerberos, Smb(NTLM), and NIS. The NIS tab is currently selected. Below the menu, the form contains two input fields: "NIS Domain Name" and "NIS Server IP". At the bottom of the form, there is a "Done" button.

2. Fill in the form according to your configuration of the NIS server.
3. Click “Done.”
4. Click “apply changes.”

### ▼ To Identify a RADIUS Authentication Server

Perform this procedure to identify the authentication server when the KVM/net Plus or any of its ports is configured to use the RADIUS authentication method or any of its variations (Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal).

1. Go to Configuration>Authentication>RADIUS in Expert mode.

The RADIUS form displays as shown in the following figure.



The screenshot shows a configuration window with a yellow background and a brown header. The header contains several tabs: AuthType, Radius, Tacacs+, Ldap, Kerberos, Smb(NTLM), and NIS. The 'Radius' tab is currently selected. Below the header, there are four text input fields arranged vertically, each with a label to its left: 'First Authentication Server', 'Second Authentication Server', 'First Accounting Server', and 'Second Accounting Server'. At the bottom of the window, there is a brown bar containing a 'Done' button.

2. Fill in the form according to your local setup of the RADIUS server or servers.
3. Click “Done.”
4. Click “apply changes.”

The changes are stored in `/etc/raddb/server` on the KVM/net Plus.

### ▼ **To Identify a TACACS+ Authentication Server**

Perform this procedure to identify the authentication server when the KVM/net Plus or any of its ports is configured to use the TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal).

1. Go to Configuration>Authentication>TACACS+ in Expert mode.

The TACACS+ form appears.

AuthType	Radius	Tacacs+	Ldap	Kerberos	Smb(NTLM)	NIS
		First Authentication Server				
		Second Authentication Server				
		First Accounting Server				
		Second Accounting Server				
<b>Done</b>						

2. Fill in the form according to your local setup of the TACACS+ server or servers.
3. Click “Done.”
4. Click “apply changes.”
5. The changes are stored in `/etc/tacplus.conf` on the KVM/net Plus.

## Configuring In-band (RDP) Servers

Selecting Configuration>Inband in Expert mode brings up the form displayed in the following figure.



You can use the Add, Modify, and Delete buttons to configure in-band server connections to Windows Terminal Servers using RDP. Up to either 16 or 32 in-band servers can be configured on a KVM/net Plus depending on the model ordered.

If secondary KVM/net Plus units are cascaded to the master KVM/net Plus, administrators can configure additional in-band servers. The total number of in-band servers configured is the same as the total number of KVM ports in the whole infrastructure (master and cascaded devices). Even though it is possible to configure a KVM port on the master or on any cascaded device for each in-band server, all in-band configuration and connections are done through the master KVM/net Plus.

For more complete access and as a backup to in-band connection failures, in-band servers can also be connected to KVM ports on the KVM/net Plus. This enables out-of-band access to the in-band server so that if the in-band connection fails, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

See “Server Access: In-band and Out of Band” on page 34, for a description of the differences between in-band and KVM connections.

## ***Prerequisites for In-band Access to RDP Servers***

The following prerequisites must be met in order for a KVM/net Plus in-band connection to work:

- The connected server must be a Windows (Win2000, 2003, XP, and NT) Terminal Server with RDP enabled.  
Windows Terminal Servers do not have RDP enabled by default: The administrator of these servers must enable RDP on the server in order for the KVM/net Plus in-band connection to work.
- A KVM/net Plus user who needs to access any in-band server must have the following:
  - A valid account created on the in-band server.  
The KVM/net Plus does not authenticate or offer permissions configuration for in-band connections.
  - Internet access and Microsoft Internet Explorer 6 on a remote Windows client machine.
- The Windows Terminal Server must be configured on the Inband page of the Web Manager. See “To Add or Modify an In-band (RDP) Server” on page 205 for configuration instructions.
- If you want to enable an out-of-band, KVM connection as back up for an in-band connection failure or if you want to view the BIOS, POST, and boot messages on the server, the RDP server must be connected to a KVM port on the master KVM/net Plus or on a cascaded and configured KVM unit.  
See “To Connect Computers to KVM Ports” on page 82 for instructions on physically connecting a server to a KVM/net Plus port.

## ▼ To Add or Modify an In-band (RDP) Server

See the previous section “Prerequisites for In-band Access to RDP Servers” on page 204 for prerequisite information to this procedure.

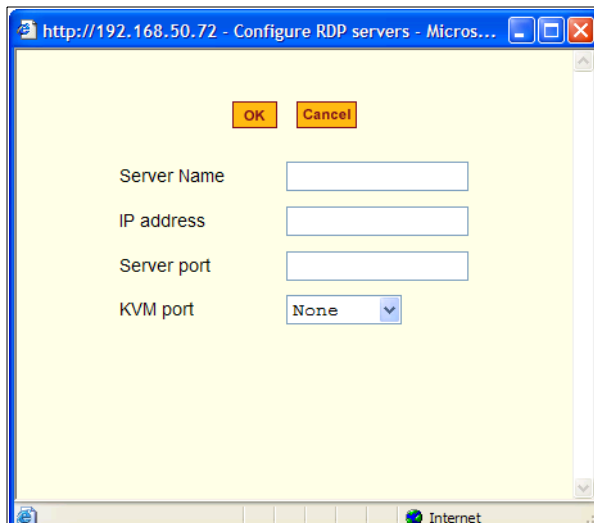
1. In Expert mode, go to: Configuration>Inband.

The Inband form appears.



2. To add a server to the list, click Add.

The Configure RDP Servers dialog box appears.



The connected server must be a Windows (Win2000 or NT) Terminal Server with RDP enabled.

3. To modify a server, select the server on the list and click Modify.
4. In the Server Name field, specify a unique name for the in-band server.  
This name will appear in the drop-down list on the Connect to Server form.

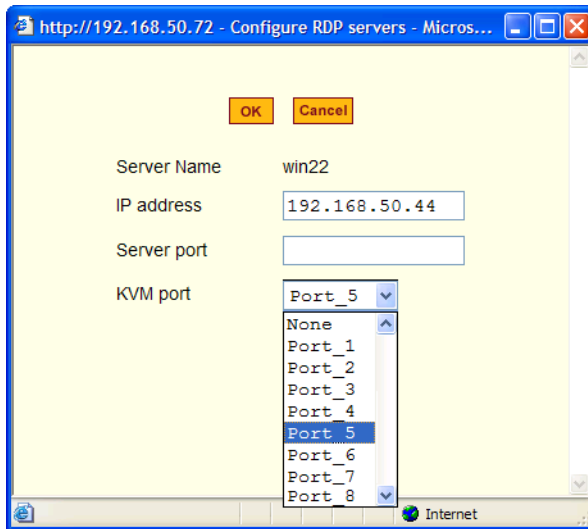
---

**Note:** Once a name is given to an in-band server, it cannot be modified. In order to change the name of an in-band server, you must delete the server configuration and add the server again to the KVM/net Plus.

---

5. In the IP Address field, enter the IP address of the in-band server.
6. (Optional) In the Server Port field, specify a port to be used if it differs from the default which is 3389.  
All servers with RDP enabled are configured with 3389 as the default port unless the administrator of the RDP server changes it.
7. To enable a back up KVM connection for the in-band server, from the KVM Port drop-down list, select the KVM port to which the in-band server is connected.





This enables both in-band and out-of-band access to the connected server. If the in-band connection fails or if an RDP session already exists, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

8. Click OK to close the dialog box.
9. Specify the TCP ports or a range of TCP ports to be used in the RDP Viewer Ports field.

You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the KVM/net Plus.

For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”.

You can request valid TCP ports from your network administrator.

10. Click “apply changes.”
11. Repeat steps 1-9 for every in-band server connection required.

The KVM/net Plus supports the configuration of up to 16 or 32 in-band servers depending on the number of KVM ports on the KVM/net Plus model ordered.

12. To connect to the in-band server, in Expert mode, go to Access>Connect to Server.

See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 304.

## ▼ **To Delete an In-band (RDP) Server**

1. In Expert mode, go to: Configuration>Inband.

The Inband form appears.



2. Select the in-band server from the list and click Delete.

3. Click “apply changes.”

## Network

Selecting Configuration>Network in Expert mode brings up the following form.

Network configuration comprises eight forms:

**Table 4-1: Network Forms**

Form	Use this form to:	Where Documented
<b>Host Settings</b>	Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.	“Host Settings” on page 211
<b>Syslog</b>	Define the Syslog Servers to enable system logging.	“Syslog” on page 214
<b>PCMCIA Management</b>	Configure one of the PCMCIA card slots for use with a modem card.	“Configuring a Modem (PCMCIA) Card” on page 216

**Table 4-1: Network Forms (Continued)**

<b>Form</b>	<b>Use this form to:</b>	<b>Where Documented</b>
<b>Services</b>	Define or activate the method of access (for example, Telnet, SSH, SNMP, Client, or NTP).	“Services” on page 220
<b>IP Filtering</b>	Configure the selective filtering of packets that may potentially crack your network system or generate unnecessary traffic.	“IP Filtering” on page 221
<b>VPN</b>	Configure IPsec tunnels to establish a secure connection between KVM/net Plus and a security gateway machine.	“VPN” on page 238
<b>SNMP</b>	Configure the SNMP server to manage complex networks.	“SNMP” on page 242
<b>Host Table</b>	View hosts list and add, edit, and delete hosts.	“Host Tables” on page 246
<b>Static Routes</b>	View, create, and delete routes from the table.	“Static Routes” on page 248

## Host Settings

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.

The screenshot shows the Host Settings configuration form. The left sidebar contains a tree view with the following items: KVM, Inband, Network (expanded), Host Settings (selected), Syslog, PCMCIA Management, Services, IP Filtering, VPN, SNMP, Host Tables, Static Routes, AUX Ports, and System. The main content area has a yellow background and contains the following fields:

- DHCP
- Host Name:
- Console Banner:

If the “DHCP” check box is not checked, then other options appear on the form as shown in the following example.

The screenshot shows the Host Settings configuration form with the DHCP checkbox unchecked. The left sidebar is identical to the previous screenshot. The main content area has a yellow background and contains the following fields:

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

## ▼ **To Configure Host Settings [Expert]**

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

1. Go to Expert>Network>Host Settings.

The Host Settings form appears.

2. By default, the DHCP is enabled. To disable DHCP, clear the DHCP check box.

The system adds the Ethernet Port and DNS Service sections.

3. Complete or edit the fields described in the following table as necessary.

**Table 4-2:** Host Settings Configuration Fields

<b>Field Name</b>	<b>Definition</b>
<b>Host Name</b>	The fully qualified domain name identifying the specific host computer within the Internet.
<b>Console Banner</b>	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.
<b>Ethernet Port</b>	
<b>Primary IP</b>	The 32-bit numeric IP address of the KVM/net Plus unit on the Internet.
<b>Network Mask</b>	The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for this IP network/subnet/supernet.
<b>Secondary IP</b>	The 32-bit numeric, secondary IP address of the KVM/net Plus unit on the Internet.
<b>Secondary Network Mask</b>	The network mask of the secondary IP.

**Table 4-2: Host Settings Configuration Fields (Continued)**

<b>Field Name</b>	<b>Definition</b>
<b>MTU</b>	Maximum Transmission Unit used by the TCP protocol.
<b>DNS Service</b>	
<b>Primary DNS Server</b>	Address of the Domain Name Server.
<b>Secondary DNS Server</b>	Address of the backup Domain Name Server.
<b>Domain Name</b>	The name that identifies the domain (for example, domainname.com).
<b>Gateway IP</b>	The gateway numeric identification number.

4. Select “apply changes” when done to save your configuration to flash.

## Syslog

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.

The screenshot shows the Syslog configuration interface. At the top, there are two dropdown menus for 'CAS/AUX Ports Facility' (set to 'Local17') and 'KVM Ports Facility' (set to 'Local13'). Below these are the 'Syslog Destination' options: 'Console' (unchecked), 'Root User' (checked), and 'Server' (unchecked). A 'New Syslog Server' section includes an input field and an 'Add >>' button. A 'Syslog Servers' table lists the server '168.192.50.5' with a 'Delete' button. The bottom half of the form contains five filter sections, each with checkboxes for log levels: Emergency, Warning, Alert, Notice, Critical, Info, and Debug. The 'Alert', 'Notice', 'Critical', and 'Info' levels are checked in all filter sections.

You can use the Syslog form to configure how the KVM/net Plus handles syslog messages. The Syslog form allows you to do the following:

- Specify one or more syslog servers to receive syslog messages related to ports.
- Specify rules for filtering messages.



The top of the form is used to tell the KVM/net Plus where to send syslog messages:

- You can specify one facility number for messages from AUX ports and another facility number for messages from KVM ports.  
Obtain the facility numbers to use from the syslog server's administrator. See "To Add a Syslog Server [Wizard]" on page 150 for how syslogging is configured for the KVM/net Plus under the Configuration>General form. You can specify the same or different syslog servers and the same or duplicate facility numbers according to your site's configuration.
- You can send syslog messages to the console port (for logging the messages even if no user is logged in); to all sessions where the root user is logged in, or to one or more syslog servers.
- You can add or delete entries for syslog servers.

The bottom of the form has check boxes for specifying which types of messages are forwarded based on the following criteria:

- Their severity level: "Emergency," "Alert," "Critical," "Error," "Warning," "Notice," "Info," "Debug"
- Their category "CAS/AUX log;" "KVM log;" "Data Buffering log;" "Web log;" or "System log."

### ▼ **To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]**

1. Go to Configuration>Network>Syslog in Expert mode.

The Syslog form appears.

2. Select a destination for the Syslog messages by clicking the check box next to one or all of the options: "Console," "Root User," or "Server."
3. Add a syslog server to the Syslog Servers list, by entering its IP address in the "New Syslog Server" field, and clicking the "Add>>" button.
4. Select a facility number for messages generated by KVM or AUX ports by selecting the number from the "CAS/AUX Ports Facility" drop-down list.
5. Select a facility number for messages generated by KVM ports by selecting the number from the "KVM Ports Facility" drop-down list.
6. Click "apply changes."

## Configuring a Modem (PCMCIA) Card

The PCMCIA Management page allows you to configure a local user to login to the KVM/net Plus through an installed and configured modem card. See “PCMCIA Card Slots on the Front” on page 16, for background information on the PCMCIA slots.

Before configuring a PCMCIA card you must have a card inserted in the PCMCIA card slot on the front of the KVM/net Plus. See “Installing PCMCIA Cards in the Front Card Slots” on page 114, for instructions on installing a PCMCIA card.

### ▼ To Configure a Modem Card

1. Insert a modem card into the slot on the front of the KVM/net Plus.  
See “Installing PCMCIA Cards in the Front Card Slots” on page 114 if needed.
2. In Expert Mode, go to: Configuration>Network>PCMCIA Management.

The PCMCIA Management page appears with the card type displayed under the Card Type column.

The KVM/net Plus supports only modem cards.

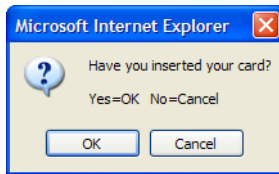
The screenshot shows the Web Manager interface for KVM/net Plus. The top navigation bar includes 'Access | Configuration | Information | Management'. The left sidebar shows a menu with 'PCMCIA Management' selected. The main content area displays a table titled 'PCMCIA' with the following data:

Slot #	Card Type	Action		
1	no card	Insert	Eject	Configure
2	Zoom, V92 PC Card	Insert	Eject	Configure

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

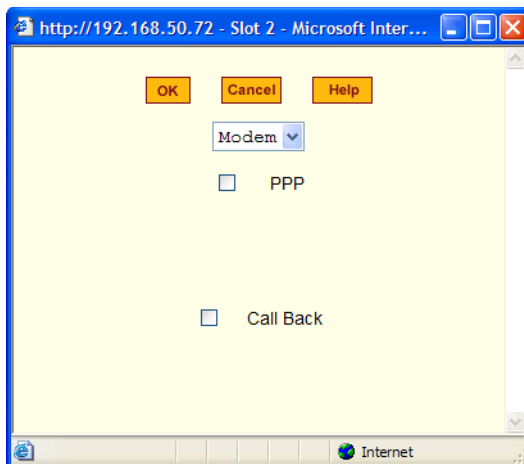
3. Click the Insert button next to the slot in which you installed the PCMCIA card.

The following prompt appears.



4. If the card is inserted, select OK.
5. If the card is not inserted, insert it and select OK.
6. Click the Configure button.

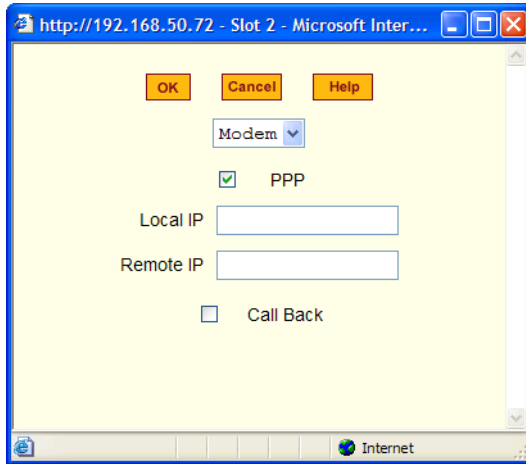
The Slot dialog box appears.



7. To enable PPP, do the following:

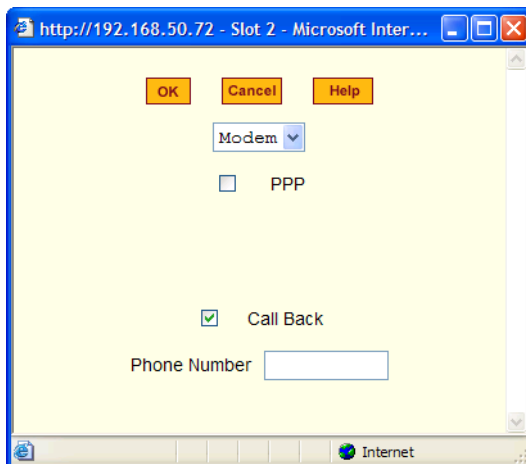
- a. Select the PPP check box.

The Local IP and Remote IP fields appear on the Slot dialog box.



- b. In the Local IP field, specify the IP address of the KVM/net Plus.
  - c. In the Remote IP field, specify the IP address of the user station or other device that is connecting to the KVM/net Plus.
- 8.** To enable call back, do the following:
- a. Select the Call Back check box.

The Phone Number field appears on the Slot dialog box.



- b. Type a callback number in the Phone Number field.
- 9.** Click the OK button.

10. Click “apply changes.”

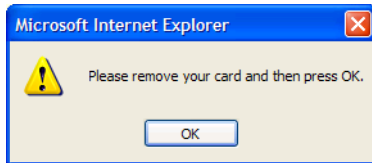
### ▼ To Eject a PCMCIA Card From the Card Slot

1. In Expert Mode, go to: Configuration>Network>PCMCIA Management.

The PCMCIA Management page appears.

2. Click the Eject button adjacent to the card you want to remove.

A prompt appears instructing you to remove the card.



3. Physically remove the card from the slot and click OK.

See “To Remove a PCMCIA Card from the Front Card Slot” on page 115 if needed.

The card type clears under the Card Type column.

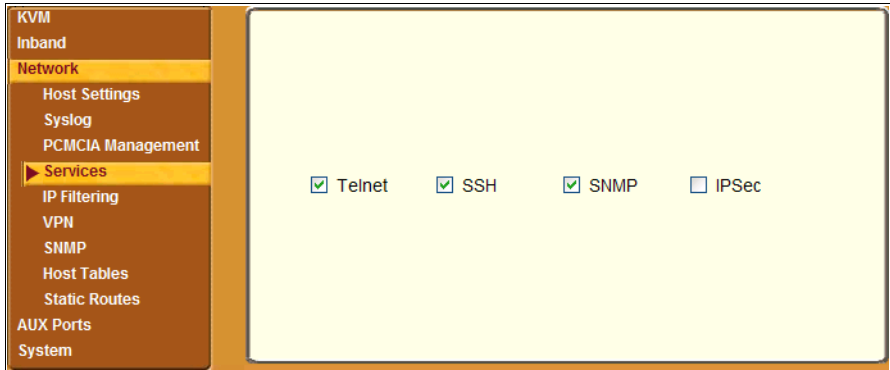
PCMCIA		
Slot #	Card Type	Action
1	no card	<input type="button" value="Insert"/> <input type="button" value="Eject"/> <input type="button" value="Configure"/>
2	no card	<input type="button" value="Insert"/> <input type="button" value="Eject"/> <input type="button" value="Configure"/>

4. Click Apply changes.

5. Physically remove the card from the PCMCIA slot on the front of the KVM/net Plus.

## Services

Selecting Configuration>Network>Services in Expert Mode, brings up the following form.



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

---

**Note:** If you plan on using VPN, make sure to enable IPsec.

---

Depending on the security requirements of your site, you may want to enable or disable the daemons that support the following types of connections:

- telnet [enabled by default]
- SSH [enabled by default]
- SNMP [enabled by default]
- IPsec

Each of these services is required when telnet, ssh, SNMP, or VPN are configured, as described in the following table.

Service Name	Notes and Where Documented
Telnet	Enable telnet if users need to access the KVM/net Plus through telnet.
SNMP	Enable “SNMP” if you configure SNMP in “To Configure SNMP” on page 243.
IPsec	Enable “IPsec” if you configure VPN in “To Configure VPN” on page 239.

## ▼ To Select the Daemons Used for Incoming Connections

1. In Expert mode got to: Configuration>Network>Services.

The Services form appears.

2. Select or clear the check boxes next to the desired service(s) to enable or disable the service.
3. Select “apply changes” when done.

## IP Filtering

Selecting Configure>Network>IP Filtering in Expert mode brings up the IP Filtering form as shown in the following figure.

Name	Policy	Packets	Bytes
INPUT	ACCEPT	5212	990K
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	1586	593K

You can use the IP Filtering form to filter traffic to and from the KVM/net Plus and block traffic according to rules you define.

The KVM/net Plus uses chains and rules for filtering packets like a firewall. Each entry in the list represents a chain with a set of rules.

The form by default has three built-in chains, as shown in the previous figure. The chains accept all INPUT, FORWARD, and OUTPUT packets. You can use the form to do the following to specify packet filtering:

- Add a new chain and specify rules for that chain
- Add new rules
- Delete existing chains and rules.

## Add Rule and Edit Rule Options

The Add Rule and Edit Rule dialog boxes have the fields and options shown in the following figure.

OK Cancel Help

Target  
ACCEPT

Source IP [ ] Mask [ ]  Inverted

Destination IP [ ] Mask [ ]  Inverted

Protocol All  Inverted

Input Interface [ ]  Inverted

Output Interface [ ]  Inverted

Fragments All packets

## Inverted Check Boxes

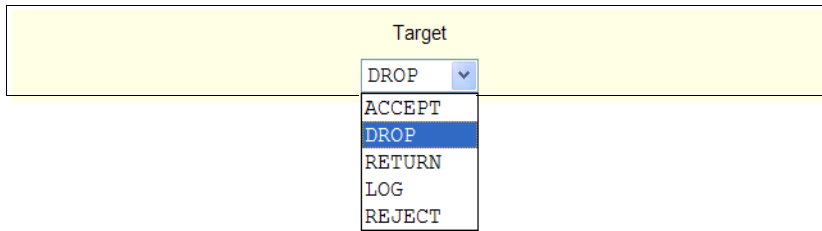
If you check the “Inverted” check box on any line, the target action is performed on packets that do not match any of the criteria specified in that line when any other specified criteria are also met.

For example, if you select DROP as the target action, check “Inverted” on the line with a source IP address specified, and do not specify any other criteria in the rule, any packets arriving from any other source IP address than the one specified are dropped.

## Target Drop-down List Options

The “Target” is the action to be performed on an IP packet that matches all the criteria specified in a rule. The target drop-down list is shown in the following figure.





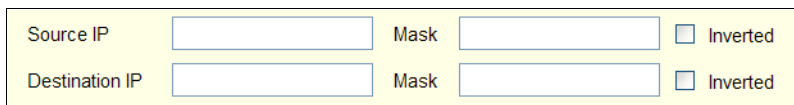
If the “LOG” and “REJECT” targets are selected, additional fields appear as described under “LOG Target” on page 227 and “REJECT Target” on page 228.

### Source or Destination IP and Mask

If you fill in the “Source IP” field, incoming packets are filtered for the specified IP address. If you fill in the “Destination IP” field, outgoing packets are filtered for the specified IP address.

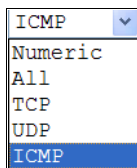
If you fill in either “Mask” field, incoming or outgoing packets are filtered for IP addresses from the network in the specified netmask.

The source and destination IP and related fields are shown in the following figure.



### Protocol

You can select a protocol for filtering from the “Protocol” drop-down list, which is shown in the following figure.



The additional fields that appear for each protocol are explained in the following sections.

### Numeric Protocol Fields

If you select Numeric as the protocol when specifying a rule, a text field appears to the right of the menu for you to enter the desired number, as shown in the following figure.

The screenshot shows a form with a 'Protocol' dropdown menu set to 'Numeric'. To the right of the dropdown is a text input field containing the number '0'. Further to the right is an unchecked checkbox labeled 'Inverted'.

### TCP Protocol Fields

If you select TCP as the protocol when specifying a rule, the additional fields shown in the following figure appear for you to fill out at the bottom of the form.

The screenshot shows a section titled 'TCP Options Section'. It contains two rows of port fields: 'Source Port' and 'Destination Port', each with a 'to' field and an unchecked 'Inverted' checkbox. Below these are 'TCP Flags' with dropdown menus for SYN, ACK, FIN, RST, URG, and PSH, all set to 'Any'. There is also an unchecked 'Inverted' checkbox at the bottom.

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

Field/Menu Option	Definition
<b>Source Port</b> - OR - <b>Destination Port</b> -AND- <b>to</b>	You can specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.
<b>TCP Flags</b>	You can select the check box next to any of the TCP flags: “SYN” (synchronize), “ACK” (acknowledge), “FIN” (finish), “RST” (reset), “URG” (urgent), or “PSH” (push) and select either “Any,” “Set,” or “Unset,” TCP packets are filtered for the specified flag and the selected condition.

## UDP Protocol Fields

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

**UDP Options Section**

Source Port  to   Inverted

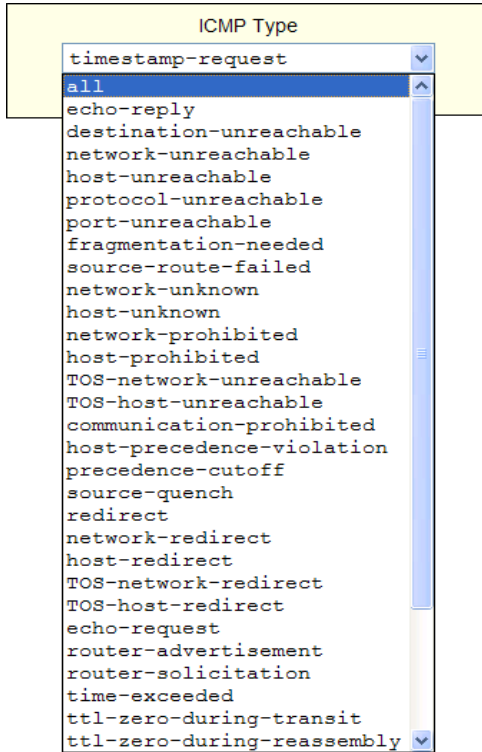
Destination Port  to   Inverted

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

Field	Definition
<b>Source Port</b> - OR - <b>Destination Port</b> -AND- <b>to</b>	<p>Specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field.</p> <p>You can specify a source or destination port number for filtering in the “Source Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.</p>

## ICMP Protocol Fields

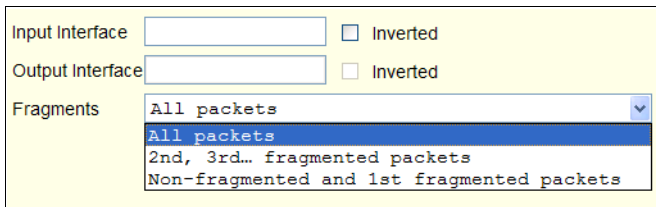
If you select ICMP as a protocol when specifying a rule, the ICMP Type drop-down list appears in the ICMP Options Section at the bottom of the IP Filtering form. The following figure shows the options.



### Input Interface, Output Interface, and Fragments

If you enter an interface (such as eth0 or eth1) in the “Input Interface” field, incoming packets are filtered for the specified interface. If you enter an interface in the “Output Interface” field, outgoing packets are filtered for the specified interface.

These fields are shown in the following figure.



The following table defines the fields in the previous figure.

Field	Definition
<b>Input Interface</b>	The input interface (eth <i>N</i> ) for the packet
<b>Output Interface</b>	The output interface (eth <i>N</i> ) for the packet
<b>Fragments</b>	The types of packets to be filtered: All packets 2nd, 3rd... fragmented packets Non-fragmented and 1st fragmented packets

### LOG Target

If you select “LOG” from the “Target” field, the following fields and menus appear in the “LOG Options Section” at the bottom of the form.

**LOG Options Section**

Log Level:  (dropdown arrow)

Log Prefix:

TCP sequence       TCP options       IP options

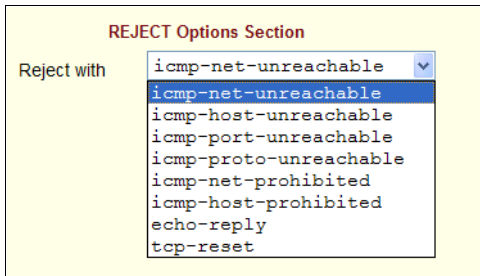
The following table defines the menu options, field, and check boxes in the “LOG Options Section.”

Field or Menu Name	Definition
<b>Log Level</b>	One of the options in the drop-down list: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <span style="float: right;">▼</span> <span style="float: left;">emerg</span> <hr/> <span>emerg</span> <span>alert</span> <span>crit</span> <span>err</span> <span>warning</span> <span>notice</span> <span>info</span> <span>debug</span> </div>
<b>Log Prefix</b>	The prefix to use in the log entry.

Field or Menu Name	Definition
<b>TCP Sequence</b>	Checking the box includes the TCP sequence in the log.
<b>TCP Options</b>	Checking the box includes TCP options in the log.
<b>IP Options</b>	Checking the box includes IP options in the log.

### REJECT Target

If you select REJECT from the Target drop-down list, the following drop-down list appears



Any “Reject with” option causes the input packet to be dropped and a reply packet of the specified type to be sent.

### Firewall Configuration Procedures

The following table has links to the procedures for defining packet filtering:

To Add a Chain	Page 229
To Edit a Chain	Page 229
To Edit a Rule for IP Filtering	Page 230
To Add a Packet Filtering Rule	Page 231

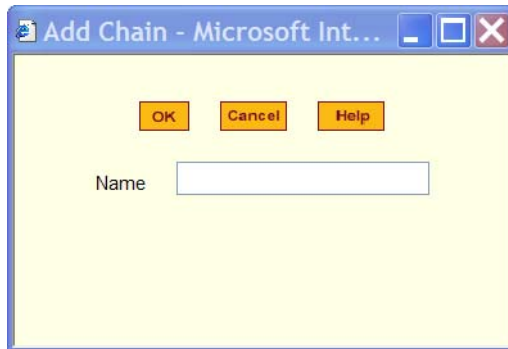
### ▼ **To Add a Chain**

1. Go to Configuration>Network>Firewall Configuration in Expert Mode.

The IP Filtering form appears.

2. Click “Add.”

The “Add Chain” dialog box appears.



3. Enter the name of the chain to be added in the “Name” field and then click OK.

Spaces are not allowed in the chain name.

The name of the new chain appears in the list.

4. Finish defining the chain by adding one or more rules, as described in to “To Add a Rule for IP Filtering” on page 233.

### ▼ **To Edit a Chain**

Perform this procedure if you want to change the policy for a default chain.

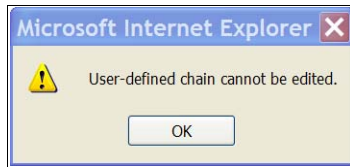
---

Note: User-defined chains cannot be edited.

---

1. Go to Configuration>Network>Firewall Configuration in Expert Mode.
2. Select one of the default chains from Chain list, and then click the “Edit” button.

If you select a user-defined chain, the following dialog box appears.



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



3. Select the desired policy from the Policy drop-down list, and then click OK.
4. Click “apply changes.”
5. To edit any rules for this chain, go to “To Edit a Rule.”

### ▼ **To Edit a Rule for IP Filtering**

1. In Expert mode go to: Configuration>Network>IP Filtering.

The IP Filtering configuration form appears.

See “To Add a Rule for IP Filtering” on page 233 procedure section for a definition of the user input fields.

2. Select a chain whose rule you want to edit.
3. Click the Edit Rule button.

The Edit Rules form appears. Each line represents a rule for the selected chain.

4. Select the Chain you wish to edit from the Chain list, and click the Edit Rule button.

The Edit Rules form appears.



5. Specify the rule as desired.  
See “IP Filtering” on page 221 for a definition of the input fields, if needed.
6. Click on the “apply changes” button to complete the procedure.

### ▼ **To Add a Packet Filtering Rule**

1. Go to Configuration>Network>Firewall Configuration in Expert Mode.
2. Select the chain whose rule you want to edit from Chain list, and then and then click the “Edit Rules” button.
3. Click the “Edit Rule” button.

The “Edit Rule for Chain” dialog box appears.

4. Specify the rule as desired.
5. Click the “Add” button.

The “Add Rule” dialog box appears.

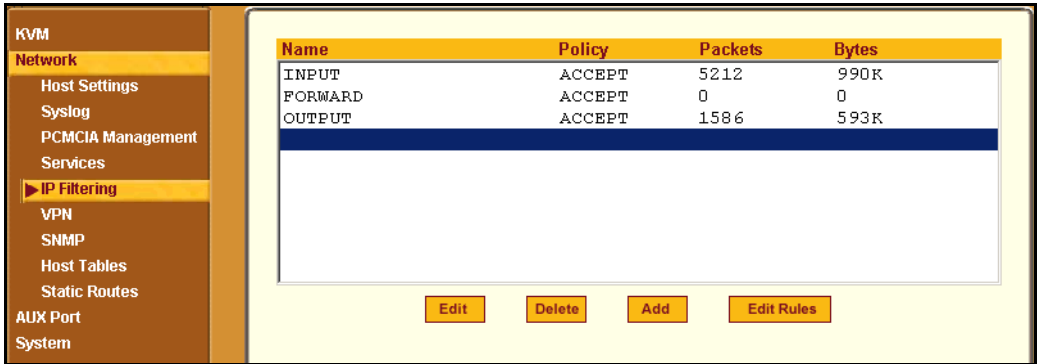
6. Complete the Add Rule dialog box.
7. Click “apply changes.”

You can perform the following task from the IP Filtering Form:

- “To Add a Chain for IP Filtering” on page 231
- “To Edit A Chain for IP Filtering” on page 233
- “To Add a Rule for IP Filtering” on page 233
- “To Edit a Rule for IP Filtering” on page 230

### ▼ **To Add a Chain for IP Filtering**

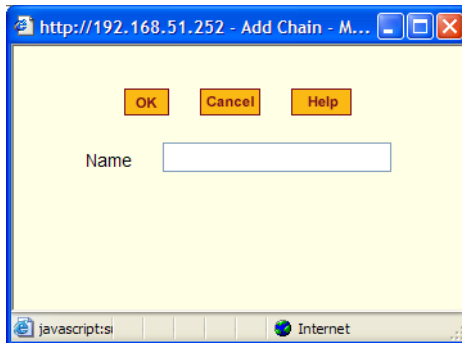
1. In Expert mode go to: Configuration>Network>IP Filtering.  
The IP Filtering configuration form appears.



Each line in the list box represents a chain. For a definition or explanation of the field columns, refer to the introductory section of this procedure or to the field definitions for the Edit Rule dialog box, next section.

2. To add a chain, select the Add button.

The Add Chain dialog box appears.



3. Enter the name of the chain that you are adding to the filter table, and then select OK. (Spaces are not allowed in the chain name.)
4. After entering a new chain name, click on the Edit Rules button to enter the rules for that chain.
5. Select OK to commit your changes.
6. To add rules to your new chain, see “To Add a Rule for IP Filtering” on page 233.

### ▼ **To Edit A Chain for IP Filtering**

1. In Expert mode go to: Configuration>Network>IP Filtering.

The IP Filtering configuration form appears.

2. Select the Chain you wish to edit from the Chain list box (or filter table), and select the Edit button.

The Edit Chain dialog box appears.

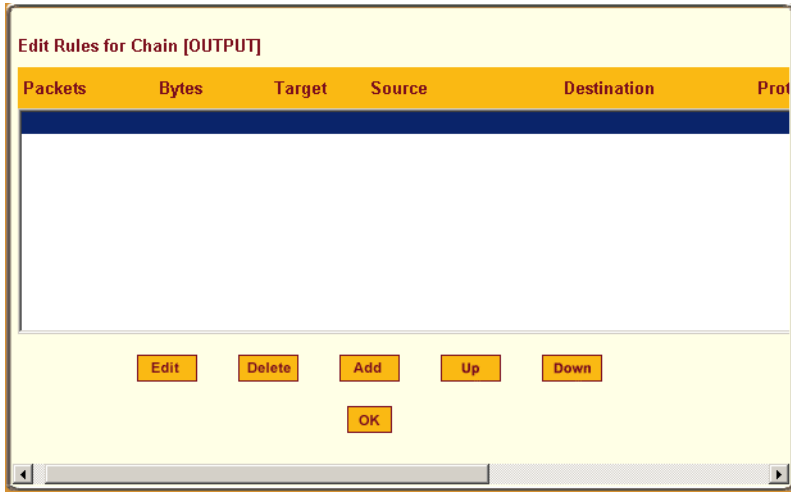


3. Modify the Policy field, as needed, and select OK.
4. Verify your entry from the main form and click “apply changes” to save your changes.
5. If you need to add any rules for this chain, go to “To Add a Rule for IP Filtering” on page 233.

### ▼ **To Add a Rule for IP Filtering**

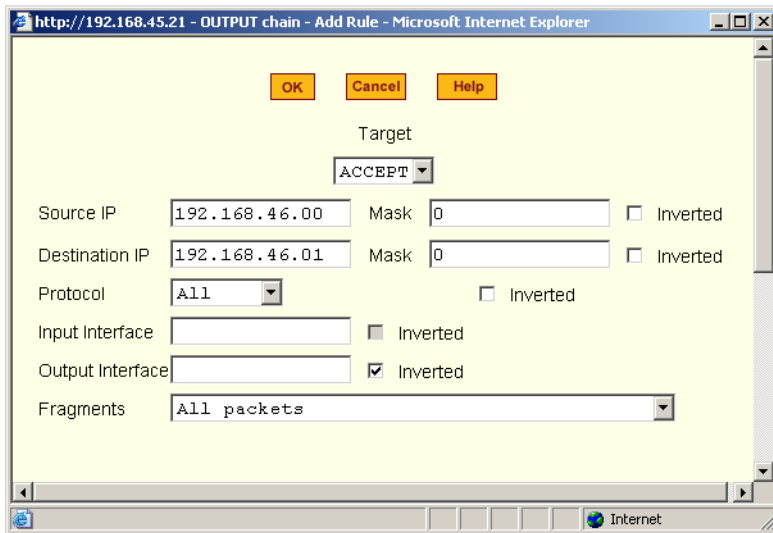
1. In Expert mode go to: Configuration>Network>IP Filtering.

The IP Filtering configuration form appears.



2. Click the Add button.

The Add Rule dialog box appears.



3. Complete the following data fields as necessary:

Field Name	Definition
<b>Target</b>	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.
<b>Source IP</b>	The source IP address.
<b>Mask</b>	Source network mask. Required when a network should be included in the rule.
<b>Inverted</b>	Select the check box adjacent to Source IP to invert the target action. For example, the action assigned to the target will be performed to all source IPs/Masks except to the one just defined.
<b>Destination IP</b>	Destination IP address.
<b>Mask</b>	Destination network mask.
<b>Inverted</b>	Select the check box adjacent to Destination IP to invert the target action. For example, the action assigned to the target will be performed to all Destination/Mask IPs except to the one just defined.
<b>Protocol</b>	The transport protocol to check. If the numeric value is available, select Numeric and type the value in the adjacent field; otherwise, select one of the other options.

Field Name	Definition
<b>Inverted</b>	Select the check box adjacent to Protocol to invert the target action. For example, the action assigned to the target will be performed to all protocols except to the one just defined.
<b>Input Interface</b>	The interface where the IP packet should pass. The Input Interface option appears only for the INPUT and FORWARD chains.
<b>Inverted</b>	Select the check box adjacent to Input Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.
<b>Output Interface</b>	The interface where the IP packet should pass. The Output interface option will appear for the chains FORWARD and OUTPUT.
<b>Inverted</b>	Select box adjacent to Output Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.
<b>Fragments</b>	Indicates the fragments or unfragmented packets to be checked. The IP Tables can check for: <ul style="list-style-type: none"> <li data-bbox="628 1237 786 1263">• All Packets</li> <li data-bbox="628 1289 1005 1315">• 2nd, 3rd... fragmented packets</li> <li data-bbox="628 1341 1076 1402">• Non-fragmented and 1st fragmented packets</li> </ul>
<b>ICMP Type</b>	This dropdown list box contains all the ICMP types that may be applied to the current rule.

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

4. Complete the following additional fields as necessary:

- If you selected Log from the Target field, the following options also appear.

**LOG Options Section**

Log Level  Log Prefix

TCP sequence     
  TCP options     
  IP options

Field Name	Definition
<b>Log Level</b>	The log level classification to be used based on the type of error message (such as, alert, warning, info, debug, and so on.).
<b>Log Prefix</b>	The prefix that will identify the log.
<b>TCP Sequence</b>	Check box to include TCP sequence in the log.
<b>TCP Options</b>	Check box to include TCP options in the log.
<b>IP Options</b>	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

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

“Reject with” means that the filter drops the input packet and sends back a reply packet according to any of the reject types listed below.

Using tcp flags and appropriate reject type, the packets are matched with the REJECT target. The following options are available:

- icmp-net-unreachable – ICMP network unreachable alias
- icmp-host-unreachable – ICMP host unreachable alias
- icmp-port-unreachable – ICMP port unreachable alias
- icmp-proto-unreachable – ICMP protocol unreachable alias
- icmp-net-prohibited – ICMP network prohibited alias
- icmp-host-prohibited – ICMP host prohibited alias
- echo-reply – Echo reply alias
- tcp-reset – TCP RST packet alias

5. Click on the OK button when done.

6. Click on “apply changes.”

## **VPN**

When VPN Connections is selected under Configuration>Network in Expert mode, you can configure one or more VPN connections.

Selecting one of the existing VPN connections and clicking the edit button or the add button launches a dialog box to prompt for the details of the connection. Complete the fields in the dialog box. The RSA keys may be entered using the Copy and Paste feature of your Browser.

If needed, see “VPN and the KVM/net Plus” on page 54 for background information.



## ▼ To Configure VPN

For the VPN to function properly, ensure that you have also enabled IPsec on the Services form. See “To Select the Daemons Used for Incoming Connections” on page 221 for instructions on configuring IPsec.

1. In Expert mode, go to: Configure>Network>VPN.

The VPN form appears.

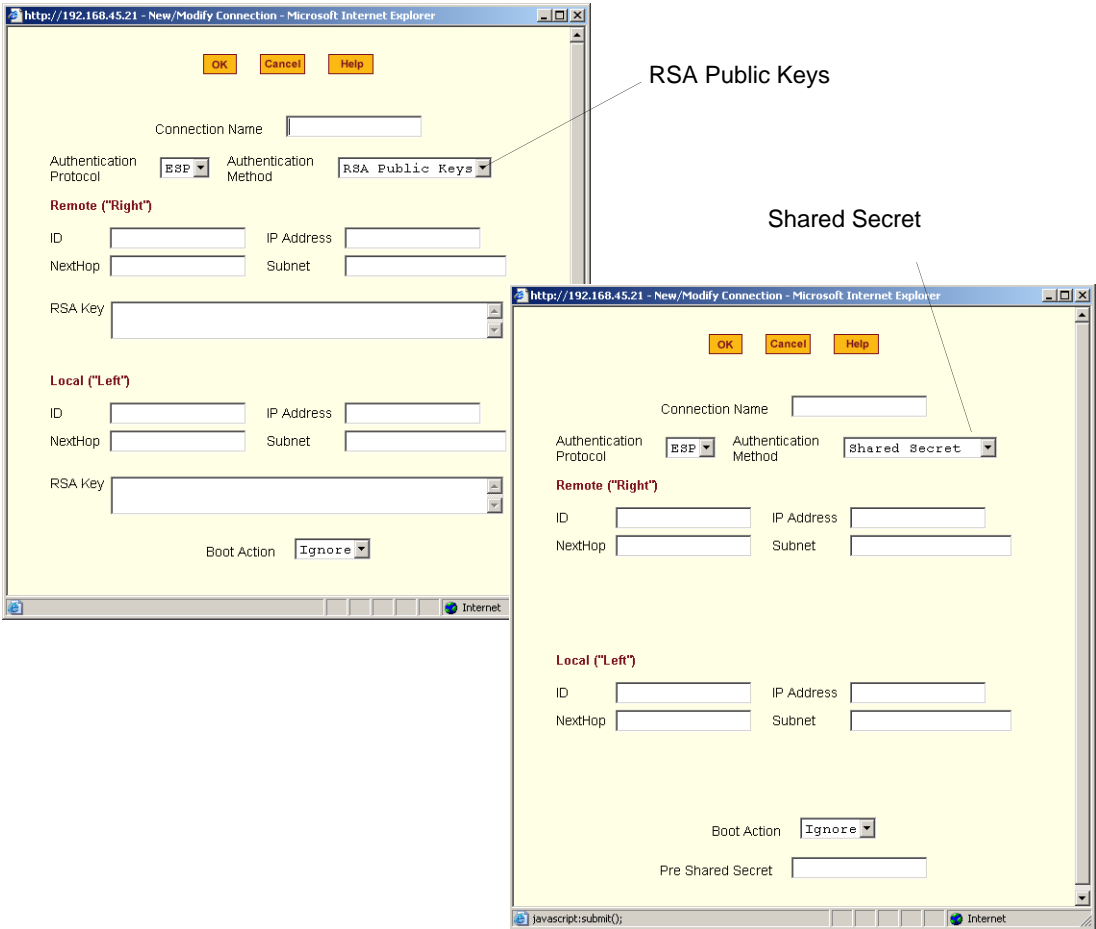


2. To edit a VPN connection, select the VPN connection that you wish to edit from the form, and then select the Edit button.

- OR -

To add a VPN Connection, select the Add button.

The New/Modify Connection dialog box appears.



**Note:** If the selected authentication method is RSA Public Keys, the dialog box on the left of the previous figure is used; if the authentication method is Shared Secret, the dialog box on the right is used.

3. Edit or complete the appropriate fields as follows.

Field Name	Definition
Connector Name	Name of the VPN connection.

<b>Field Name</b>	<b>Definition</b>
<b>Authentication Protocol</b>	Authentication protocol used to establish a VPN connection.
<b>Authentication Method</b>	Authentication method used to establish a VPN connection.
<b>Remote (“Right”)</b>	
<b>ID</b>	The identification name of the remote host, commonly referred to as the “right” host.
<b>IP Address</b>	Remote IP address.
<b>NextHop</b>	The router to which the Console Server sends packets in order to deliver them to the left.
<b>Subnet Mask</b>	As indicated.
<b>RSA Key</b>	You may use the copy and paste feature of your browser to enter the RSA key.
<b>Local (“Left”)</b>	
<b>ID</b>	The identification name of the local host, commonly referred to as the “left” host.
<b>IP Address</b>	The IP address of the local or left host.
<b>NextHop</b>	The router to which the Console Server sends packets in order to deliver them to the right.
<b>Subnet Mask</b>	As indicated
<b>RSA Key</b>	You may use the copy and paste feature of your browser to enter the RSA key.
<b>Boot Action</b>	The boot action configured for the local host.

---

Field Name	Definition
<b>Pre-Shared Secret</b>	Pre-shared password between left and right users.

---

4. Select the OK button when done.
5. Select the “apply changes” button to save your configuration.

## **SNMP**

Short for Simple Network Management Protocol, SNMP is a set of protocols for managing network devices. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices (*agents*), store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The KVM/net Plus 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 Plus supports SNMP v1, v2, and v3. The two versions require different configurations. SNMP v1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

**Important:** Check the SNMP configuration before gathering information about KVM/net Plus by SNMP. An unauthorized user can implement different types of attacks to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in KVM/net Plus cannot permit the public community to read SNMP information.

▼ **To Configure SNMP**

1. In Expert Mode go to: Configuration>Networks>SNMP.

The SNMP form appears.

To activate the snmpd services, you should go to the Network Services section.

**System Information Settings**

SysContact:

SysLocation:

**Access Control**

**SNMPv1/SNMPv2 Configuration**

Community	Source	OID	Permission
-----------	--------	-----	------------

Add Delete Edit

**SNMPv3 Configuration**

User name	Permission	OID
-----------	------------	-----

Add Delete Edit

2. Enter the following system information, as necessary:

Field Name	Definition
<b>Community</b>	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.

Field Name	Definition
<b>SysContact</b>	The email of the person to contact regarding the host on which the agent is running (for example, me@mymachine.mydomain)
<b>SysLocation</b>	The physical location of the system (for example, mydomain).

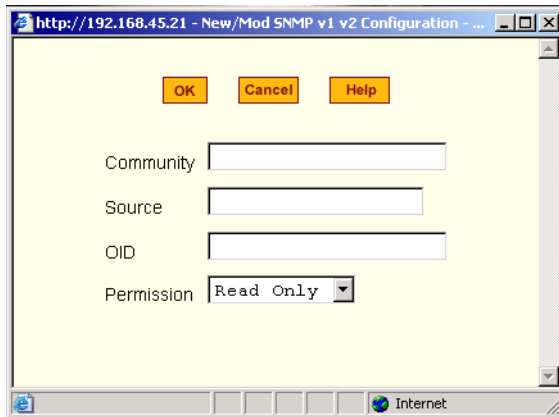
If you are using SNMPv3, skip to Step 6.

- To Add an SNMP agent using SNMPv1/SNMP2 Configuration, select the Add button located at the bottom of this view table.

OR

To edit an SNMP agent, select the Edit button.

The New/Modify SNMP Daemon Configuration dialog box appears.



- Complete the dialog box as follows:

Field Name	Definition
<b>Community</b>	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.

Field Name	Definition
<b>Source</b>	The source IP address or range of IP address.
<b>OID</b>	Object Identifier.
<b>Permission</b>	Select the permission type: <ul style="list-style-type: none"> <li>• Read Only – Read-only access to the entire MIB except for SNMP configuration objects.</li> <li>• Read/Write – Read-write access to the entire MIB except for SNMP configuration objects.</li> <li>• Admin – Read-write access to the entire MIB.</li> </ul>

5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form and select the Add button located at the bottom of this view table

The screenshot shows a web-based configuration interface titled "SNMPv3 Configuration". It features a table with three columns: "User name", "Permission", and "OID". The table is currently empty. Below the table, there are three buttons: "Add", "Delete", and "Edit".

6. To add an SNMP agent using SNMPv3, click Add.
7. To edit an SNMP agent using SNMPv3, click Edit.

The New/Modify SNMP Daemon Configuration dialog box.

The screenshot shows a dialog box titled "http://192.168.45.21 - New/Mod SNMPv3 Config...". It contains the following fields and controls:

- OK, Cancel, and Help buttons at the top.
- User name:
- Password:
- OID:
- Permission:  (dropdown menu)

8. Complete the form and when done.

---

<b>Field Name</b>	<b>Definition</b>
<b>Username</b>	Name of user account accessing the KVM/net Plus.
<b>Source</b>	The source IP address or range of IP address.
<b>OID</b>	Object Identifier.
<b>Permission</b>	Select the permission type: <ul style="list-style-type: none"><li>• Read Only – Read-only access to the entire MIB except for SNMP configuration objects.</li><li>• Read/Write – Read-write access to the entire MIB except for SNMP configuration objects.</li></ul>

---

9. Click the OK button.

10. Verify your entry or modification on the SNMP form.

11. Click “apply changes” to complete the procedure.

### ***Host Tables***

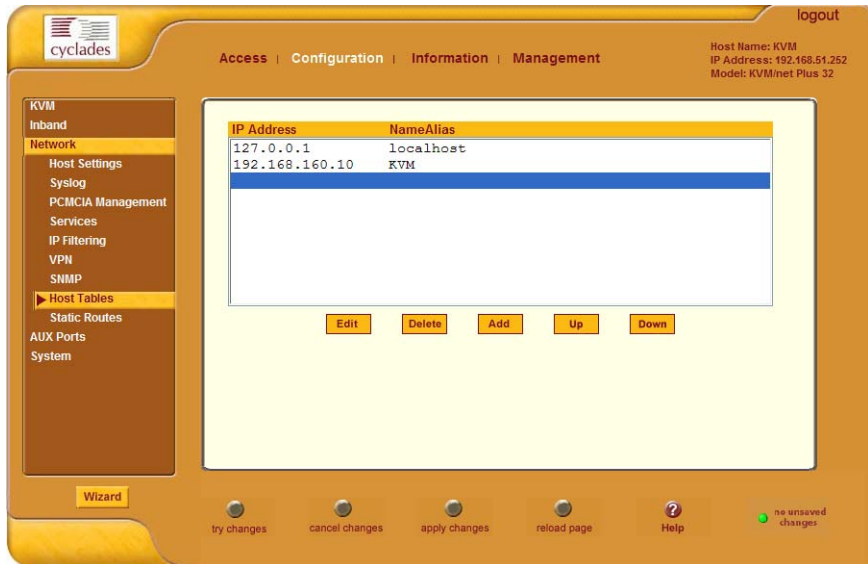
The Host Tables form enables you to keep a table of host names and IP addresses that comprise your local network, and thus provide information about your network environment.

#### **▼ To Configure Hosts**

1. In Expert Mode, go to: Configuration>Network>Host Tables.

The Host Tables form appears.





2. Do on of the following:

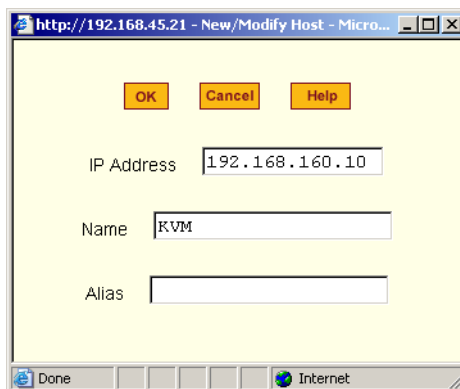
- To edit a host, select the host IP address from the Host Table and then click the Edit button.

If the list is long, use the Up and Down buttons to go through each item in the list.

- OR -

- To add a host, click the Add button.

The New/Modify Host dialog box appears.



3. Enter the new or modified host address in the IP Address field and the host name in the Name field.
4. Click the OK button.
5. To delete a host, select the host you wish to delete from the Host Table form, and select the Delete button on the form.
6. Select “apply changes” to save your configuration to Flash.

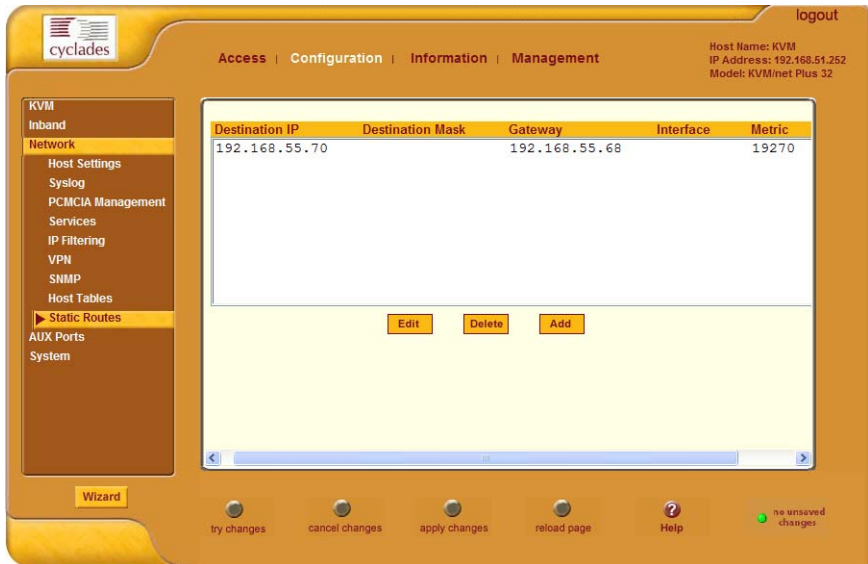
### **Static Routes**

The Static Routes form allows you to manually add routes. The Routing Table defines which interface should transmit an IP packet based on destination IP information. Static routes are a quick and effective way to route data from one subnet to another.

#### **▼ To Add, Edit, or Delete a Static Route**

1. In Expert mode, go to: Configure>Network>>Static Routes.

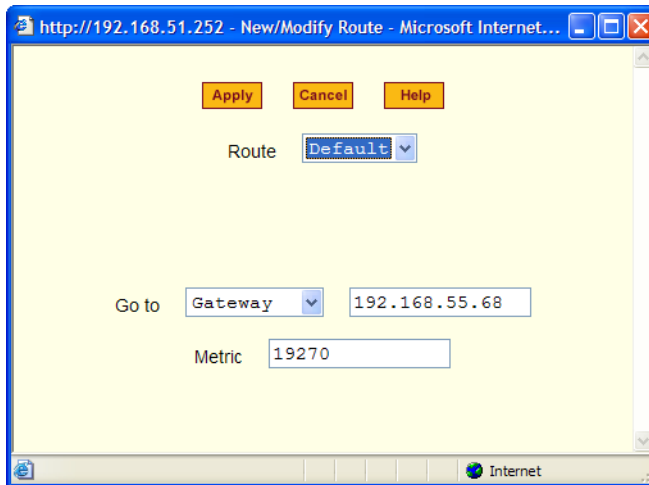
The Static Routes table form appears.



2. Do one of the following:

- To edit a static route, select a route from the Static Routes form, and click the Edit button.

- To add a static route, select the Add button from the form.  
The New/Modify Route dialog box appears.



3. Complete the dialog box as follows:

**Table 4-3: Add/Modify Static Routes Fields**

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

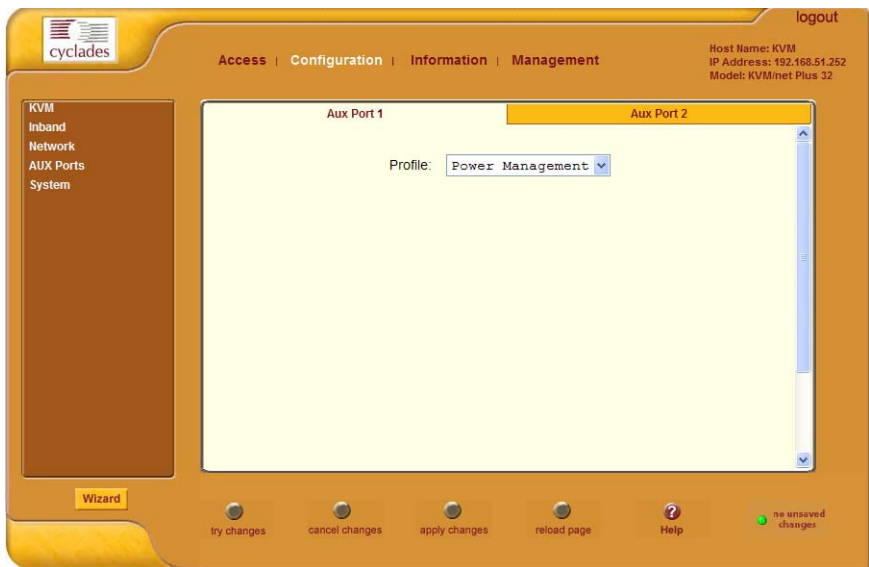
**Table 4-3:** Add/Modify Static Routes Fields

Field Name	Definition
Metric	The number of hops.

4. Click the Apply button to close the dialog box.  
The new or modified route appears in the list.
5. To delete a static route, select a route from the list and click Delete.
6. Click “apply changes.”

## AUX Ports

Selecting Configuration>AUX Ports in Expert mode brings up the following form.



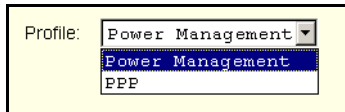
The AUX Port 1 form is used to configure the AUX 1 port for use with an AlterPath PM or an external modem. The AUX Port 2 form is used to configure an external modem.

## ▼ **To Configure the AUX 1 Port for Use With a PM**

1. In Expert mode go to: Configuration>AUX Ports.

The Aux Port 1 form appears.

2. To configure the AUX 1 port for Power Management, make sure that Power Management is selected in the Profile drop-down list.



The image shows a screenshot of a web form. On the left, the label 'Profile:' is followed by a drop-down menu. The menu is currently open, showing three options: 'Power Management' (which is highlighted in blue), 'Power Management', and 'PPP'. The background of the form is light yellow.

3. Click “apply changes.”

See “Power Management” on page 44 for background information on power management and lists of related tasks.

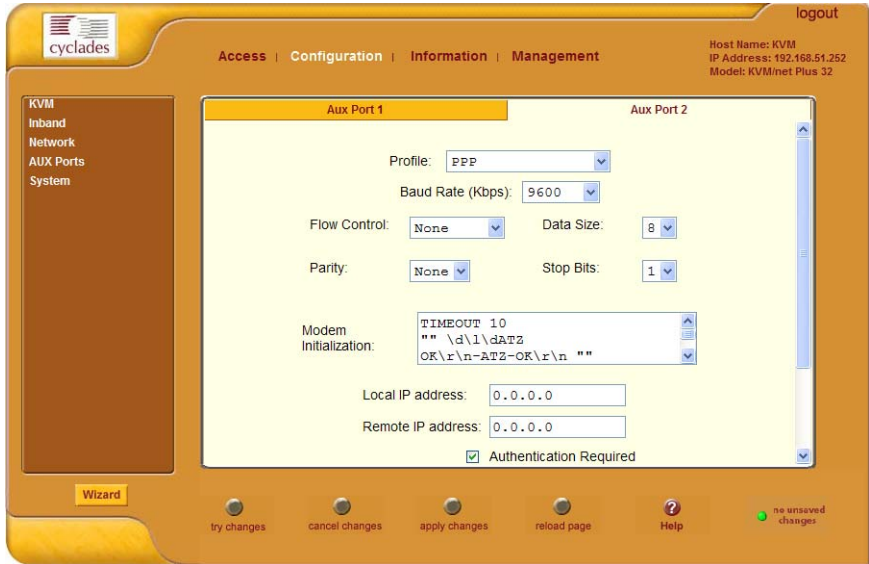
## ▼ **To Configure the AUX 2 Port for Use With an External Modem**

1. In Expert mode go to: Configuration>AUX Ports.

The Aux Port 1 form appears.

2. Select the Aux Port 2 tab.

The Aux Port 2 form appears.



3. Make sure that PPP is selected in the Profile field.
4. Complete the fields as shown below.

**Table 4-4:** PPP Fields for Configuring the AUX Port

Field Name	Definition
<b>Profile</b>	Select the device to be connected. For <b>PPP</b> , the following input fields are used:
<b>Baud Rate</b>	The port speed.
<b>Flow Control</b>	Gateway or interface address used for the route.
<b>Data Size</b>	The number of data bits.
<b>Parity</b>	None, even or odd.
<b>Stop Bits</b>	The number of stop bits.
<b>Modem Initialization</b>	The modem initialization string.
<b>Local IP Address</b>	The IP address of the KVM/net Plus.

**Table 4-4: PPP Fields for Configuring the AUX Port (Continued)**

Field Name	Definition
<b>Remote IP Address</b>	The remote IP address
<b>Authentication Required</b>	Select check box if authentication is required.
<b>MTU/MRU</b>	The maximum transmission unit / maximum receive units for the PPP.
<b>PPP Options</b>	The options for this protocol.

5. Click “apply changes.”

## System

Selecting Configuration>System in Expert mode brings up the System form as shown in the following figure.

The screenshot shows the Cyclades KVM configuration interface. The top navigation bar includes 'Access | Configuration | Information | Management'. The sidebar on the left lists 'KVM', 'Inband', 'Network', 'AUX Ports', 'System', 'Time / Date', and 'Boot Configuration'. The main content area displays the following configuration fields:

- Timezone: GMT
- Network Time Protocol: Disable
- Date:
  - Month: 6
  - Day: 15
  - Year: 2005
- Time:
  - Hour: 19
  - Minute: 55
  - Second: 46

The bottom toolbar contains buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and a status indicator for 'no unsaved changes'.

With the System form administrators can set the time and date on the KVM/net Plus and reboot the KVM/net Plus if necessary. The following procedures are available on the System form:

- “To Set the KVM/net Plus’ Date and Time Manually” on page 254
- “To Set The Time and Date With NTP” on page 255
- “To Set the Time and Date to the KVM/net Plus’ Local GMT” on page 255
- “To Configure KVM/net Plus Boot” on page 259

### ***Time/Date***

With the Time/Date form, you have three options for setting the time and date of your KVM/net Plus system:

- “To Set the KVM/net Plus’ Date and Time Manually” on page 254
- “To Set The Time and Date With NTP” on page 255
- “To Set the Time and Date to the KVM/net Plus’ Local GMT” on page 255

#### **▼ To Set the KVM/net Plus’ Date and Time Manually**

1. In Expert Mode, go to: Configuration>System>Time/Date.  
The Date/Time form appears.
2. Make sure that Disabled is selected in the Network Time Protocol dropdown list.



Network Time Protocol:

**Date**

Month:  Day:  Year:

**Time**

Hour:  Minute:  Second:

3. Fill in the date and time fields by selecting the appropriate numbers from the drop-down lists.
4. Click “apply changes.”

### ▼ **To Set The Time and Date With NTP**

1. In Expert Mode, go to: Configuration>System>Time/Date.  
The Date/Time form appears.
2. Choose Enable from the Network Time Protocol drop-down list.  
The NTP Server field appears.

Enable Timezone:

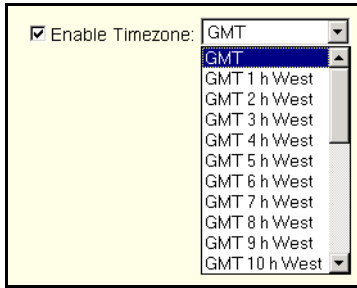
Network Time Protocol:

NTP Server:

3. Enter the address of the NTP server in the NTP Server field.
4. Click the “apply changes” button.

### ▼ **To Set the Time and Date to the KVM/net Plus' Local GMT**

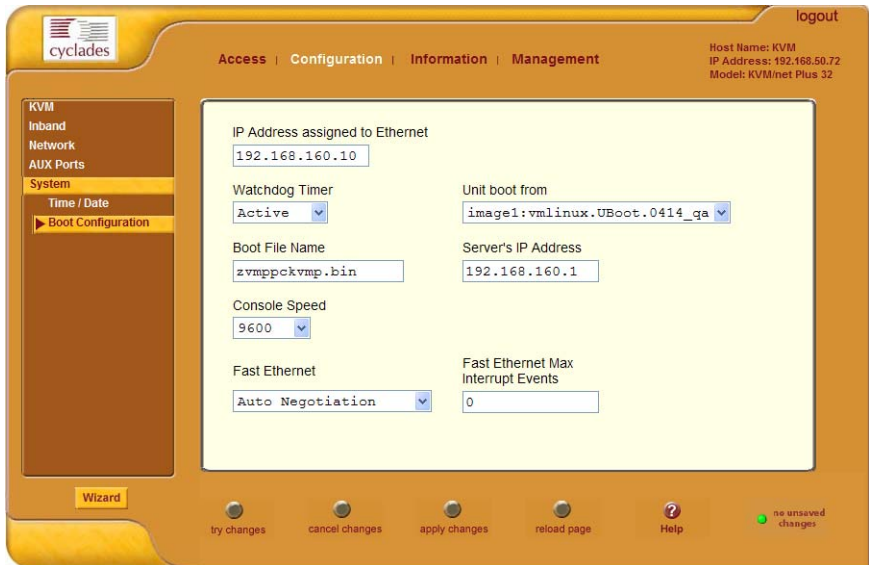
1. Select Administration from the top menu bar.
2. Select Time/Date from the left menu panel.  
The Time/Date form appears.
3. Select the appropriate GMT from the Timezone drop-down list. Only official time zones are available.



4. Click “apply changes.”

## Boot Configuration

Selecting Configuration>System>Boot Configuration brings up the following form.



On the Boot Configuration form, you can redefine the location from which the KVM/net Plus boots.

By default, the KVM/net Plus boots from a boot file in the on-board Flash memory. To understand the “Unit boot from” options, you need to understand how the KVM/net Plus handles software upgrades:

- The KVM/net Plus initially boots from a software image referred to as “image1.”
- The first time you download and install a new software version from Cyclades, the new image is stored as “image2” in the Flash memory and the configuration is changed to boot the KVM/net Plus from “image 2.”
- The second time you download a new software version, the latest image is stored as “image 1,” and the KVM/net Plus configuration is changed to boot from “image1.”
- Subsequent downloads are stored following the same pattern, alternating “image1” with “image2.”

In the “Unit boot from” drop-down list, an entry showing the number of the *current* image and the name of the boot file are selected by default. The word “image” is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. In the initial configuration, the menu item appears as follows:

```
image1: zvmppcons.vversion_number
```

For the first version the filename would be:

```
image1: zvmppcons.v100
```

After one or more software upgrades have been performed, a second image is also listed in the menu, for example:

```
image1: zvmppcons.v100
```

```
image2: zvmppcons.v101
```

If, for any reason, you want to boot from another image than the one currently selected, you can select that image from the “Unit boot from” menu. You can select “Network” and configure a boot server to boot from the network instead, if desired.

A network boot has the following prerequisites:

- A TFTP or BOOTP server must be available to the KVM/net Plus on the network.
- An upgraded KVM/net Plus boot image file must be downloaded from Cyclades and available on the boot server.

- The KVM/net Plus must have a fixed IP address and you must know the address.
- You must know the boot filename and the IP address of the TFTP server.

These and other boot related options are described in the following table.

**Table 4-5: Boot Configuration Fields and Options**

<b>Field or Value Name</b>	<b>Description</b>
<b>IP Address assigned to Ethernet</b>	A new IP address for the KVM/net Plus.
<b>Watchdog Timer</b>	Whether the watchdog timer is active. If the watchdog timer is active the KVM/net Plus reboots if the software crashes. See “Boot Configuration” on page 256 for how the watchdog timer can be activated or deactivated.
<b>Unit boot from</b>	Choose one or more images and “Network” from the list.
<b>Boot File Name</b>	An alternative name for the boot file.
<b>Server’s IP Address</b>	An IP address for a boot server.
<b>Console Speed</b>	An alternative console speed from 4800 to 115200 (9600 is the default).
<b>Fast Ethernet</b>	The speed of the Ethernet connection: Auto Negotiation, 100 BaseT Half-Duplex, 100 BaseT Full-Duplex, 10 BaseT Half-Duplex, 10 BaseT Full-Duplex
<b>Fast Ethernet Max Interrupt Events</b>	An alternate number of maximum interrupt events to improve performance (0 is the default)

## ▼ **To Configure KVM/net Plus Boot**

For more information about the fields in the “Boot Configuration” form, see Table 4-5 on page 258, if desired.

1. Go to Configuration>System>Boot Configuration in Expert mode.

The Boot Configuration form appears.

2. Enter the IP address of the KVM/net Plus in the “IP Address assigned to Ethernet” field.
3. Accept or change the selected option in the “Watchdog Timer” field.
4. Choose the desired image or “Network” from the “Unit boot from” menu.
5. Accept or change the filename of the boot program in the “Boot File Name” field.
6. If specifying network boot, do the following steps.
  - a. Enter the IP address of the tftp server in the “Server’s IP Address” field.
  - b. Select a console speed to match the speed of the tftp server from the “Console Speed” drop-down list.
  - c. Choose an Ethernet speed from the “Fast Ethernet” drop-down list.
  - d. Specify the maximum number of packets that the CPU handles before an interrupt in the “Fast Ethernet Max. Interrupt Events” field.
7. Click “apply changes.”

## Viewing System Information

The Information menu provides three forms for viewing information about your KVM/net Plus:

- General
- Port Status
- Read Sensor

### General

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

- System – Kernel version, date, uptime, power supply
- CPU – CPU, clock, revision, Bogomips
- Memory – Total, free, cached, active/inactive, and so on.
- Ram Disk Usage – 1k-blocks, used/available, percent used, and mounted
- Fan Status – Rotations per minute

### ▼ To View General Information for Your KVM/net Plus

1. In Expert mode, go to: Information>General.

The General information form appears.



## Port Status

Use the Port Status form to view the system status of each KVM/net Plus port. The Port Status form displays information for six ports—two local and four remote.

---

**Note:** Remote port status does not appear on the Port Status form unless one or more remote ports is configured in the system.

---

### ▼ To View Port Status

1. In Expert mode, go to: Information>Port Status.

The Port Status form appears.



The following table describes the information displayed for each port on the Port Status form.

**Table 4-6:** Port Status Information

<b>Field</b>	<b>Information</b>
<b>Station</b>	Displays whether the station is Local, Remote, or Inactive and lists the microcontroller version used. This field also displays whether the KVM/net Plus is a Master or Slave and lists the model number of the master KVM/net Plus.
<b>Connection mode</b>	Displays whether the connection is <b>Network</b> or <b>Physical</b> or if the system is <b>Trying to connect</b> (if the cable is disconnected).
<b>Current status</b>	Displays the name of the current active page for that session.
<b>Login</b>	If a user is logged in, displays the user name and duration of the session in seconds.
<b>Current server</b>	When connected to a port, displays the server name.
<b>Connection status</b>	When connected to a port, displays the type of switch, expander, and version number used.
<b>Current permissions</b>	When connected to a port, displays the permissions the current user has on that port.
<b>Cycle</b>	When connected to a port and in Cycle Mode, this field displays the time in seconds that the system has been cycling.



## ***Temperature Sensor***

The Temperature Sensor graph displays readings from the KVM/net Plus' three temperature sensors located at the power supply, at the fan, and at the field programmable gate array (FPGA). The graph displays a new reading every five seconds for the selected temperature sensor. Administrators can modify the format of the display and save the format in a profile for later use.

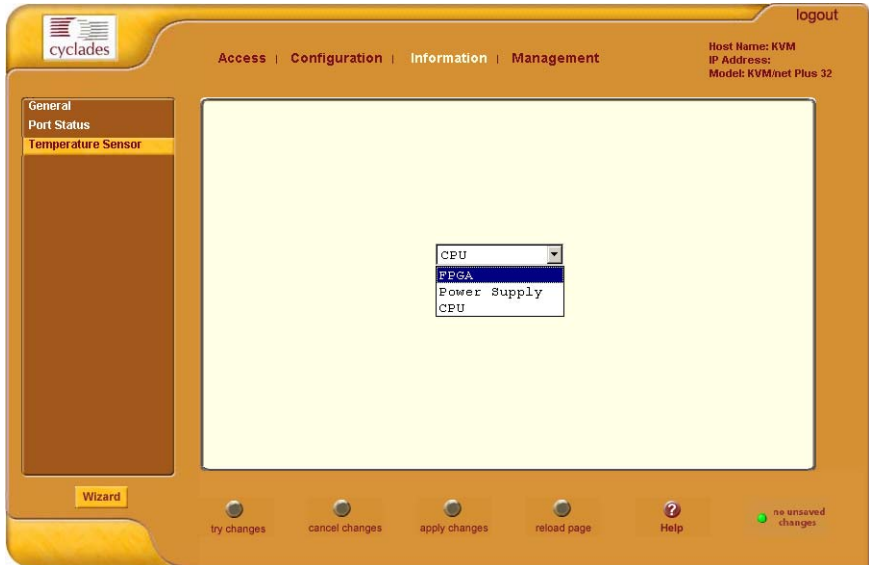
Selectable graph features include the following:

- Number of cells (Grid Boxes)
- Background color
- Line color
- Type of graph: bar or line graph
- Temperature range
- Mean temperature

**Caution!** The temperature should not exceed 115°F nor fall below 50°F.

### **▼ *To Monitor the Temperature of Your KVM/net Plus***

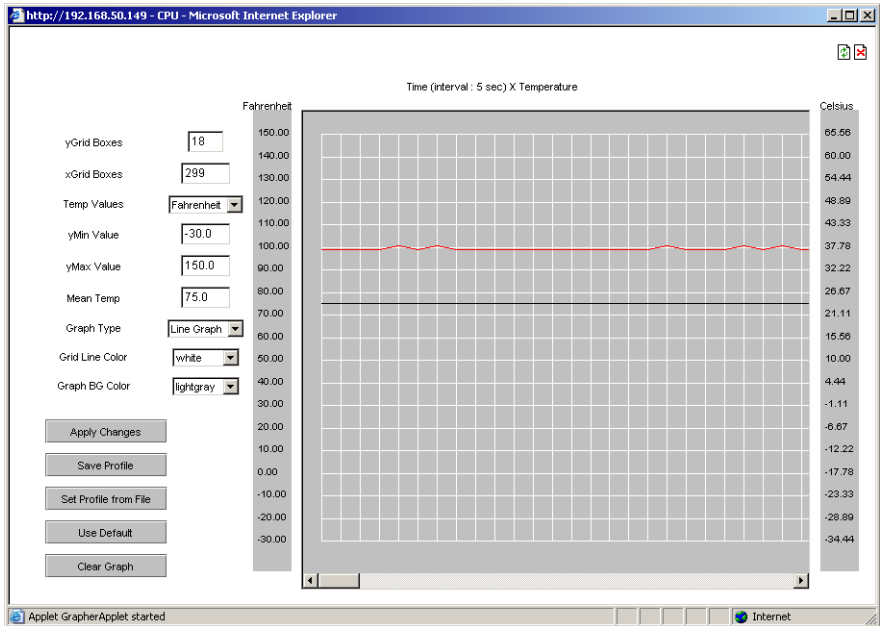
1. In Expert Mode, go to: Information>Temperature Sensor.  
The Temperature Sensor form appears.



2. Select the temperature sensor you wish to read from the drop-down list and click Connect.

You can choose the temperature sensor located near the power supply, the fan, or the field programmable gate array (FPGA).

The Time (seconds) X Temperature (degrees Fahrenheit) dialog box appears for the specified temperature sensor.



### 3. Choose a display format.

- To use the default graph profile, do nothing.
- or
- Specify another display format.

The following table describes the fields and menu options for changing the display.

<b>Field</b>	<b>Used to</b>	<b>Default</b>
<b>yGrid Boxes</b>	Specify the number of rows. Valid values include whole numbers between 1 and 55.	29
<b>xGrid Boxes</b>	Specify the number of columns. Each graph cell represents five seconds. Valid values include whole numbers between 1 and 999.	299
<b>yMin Value</b>	Specify the minimum value in degrees Fahrenheit to be displayed on the y-axis. Valid values include whole numbers between -100 and 300.	-40°F
<b>yMax Value</b>	Specify the maximum value in degrees Fahrenheit to be displayed on the y-axis. Valid values include whole numbers between -100 and 300.	250°F
<b>Mean Temp</b>	Specify the temperature to use as a basis for comparing the actual temperature. In line graphs, the Mean Temp is indicated by a red, horizontal line. In bar graphs, the colors of the bars indicate the following: <ul style="list-style-type: none"> <li>• Blue bars – Less than mean temperature.</li> <li>• Red bars – Greater than mean temperature.</li> <li>• Black bars – Equal to the mean temperature.</li> </ul>	75°F
<b>Graph Type</b>	Select graph type, either line or bar.	Line Graph
<b>Grid Line Color</b>	Select the color of the grid lines.	White
<b>Graph BG Color</b>	Select the background color.	Light Gray

4. To apply any changes to the graph, click “apply changes.”
5. To save any changes in a profile file, do the following:

- a. Click Save Profile.
    - A Save Profile dialog box appears.
  - b. Enter a name for the profile and click OK.
6. To apply a previously defined profile, do the following:
    - a. Select Set Profile from File.
      - The file chooser dialog box appears.
    - b. Select the desired profile's file name.
      - The temperature graph display changes to the profile's values.
  7. To clear the temperature display and start the plotting again at zero seconds, select Clear Graph.
  8. To exit the Temperature Sensor form, click the X box at the upper right hand corner of the applet window.

## Management

Selecting Management in Expert mode brings up the Management form as displayed in the following figure.

The screenshot shows the Management form in the cyclades interface. The form is titled "Management" and contains the following elements:

- Header:** "cyclades" logo on the left, "Access | Configuration | Information | Management" navigation tabs in the center, and "logout" on the right. System information on the far right includes "Host Name: KVM", "IP Address: 192.168.50.72", and "Model: KVM/net Plus 32".
- Left Sidebar:** A vertical menu with options: Backup Configuration, Firmware Upgrade, Microcode Upgrade, Microcode Reset, Active Sessions, and Reboot.
- Main Content Area:** A form with a "Type" dropdown menu set to "FTP". Below it are four input fields: "Server IP", "Path and Filename", "Username", and "Password". At the bottom of the form are "Save" and "Load" buttons.
- Bottom Bar:** A "Wizard" button on the left, and a row of five circular buttons: "try changes", "cancel changes", "apply changes", "reload page", and "Help". On the far right, a green indicator and the text "no unsaved changes" are displayed.

Administrators can use the management menu to perform system and software management such as booting, backing up, upgrading firmware, and handling configuration data.

---

<b>Menu Selection</b>	<b>Use this menu to:</b>
<b>Backup Configuration</b>	Use a FTP server to save or retrieve your configuration data.
<b>Firmware Upgrade</b>	Upload firmware from the web to the KVM/net Plus and save the new software version or update.
<b>Microcode Upgrade</b>	Update any of the microcontroller microcodes that are stored in the KVM Terminator, main KVM/net Plus, local KVM/net Plus, and internal KVM/net Plus switch.
<b>Microcode Reset</b>	Reset any of the micro controller microcodes.
<b>Active Sessions</b>	View the status of all active sessions as well as reset or kill sessions.
<b>Reboot</b>	Reboot the system.

---

## ***Backup Configuration***

The Backup Configuration form allows you to set the KVM/net Plus to use an FTP server to save and retrieve its configuration data.

For the backup configuration to work, the FTP server must be on the same subnet as the KVM/net Plus. Ping the FTP server, to ensure that it is accessible from the KVM/net Plus.

Selecting Management>Backup Configuration in Expert mode brings up the form shown in the following figure.

The screenshot shows a web-based configuration interface. On the left is a vertical menu with the following items: Backup Configuration (highlighted), Firmware Upgrade, Microcode Upgrade, Microcode Reset, Active User Sessions, and Reboot. The main area contains a form with the following fields:
 

- Type:** A dropdown menu currently showing 'FTP', with 'Storage Device' also visible in the list.
- Server IP:** A text input field.
- Path and Filename:** A text input field.
- Username:** A text input field.
- Password:** A text input field.

 At the bottom of the form are two buttons: 'Save' and 'Load'.

You can use the form to specify an FTP server for saving the KVM/net Plus configuration, so you can retrieve the configuration if it is ever erased. You can also use the form for retrieving a copy of the backed up configuration file from the FTP server.

The FTP server must be on the same subnet. Ensure that it is accessible by pinging the FTP server.

The following table described the information you need to enter in the fields on the “Backup Configuration” form when FTP is selected from the “Type” drop-down list.

Field	Definition
<b>Server IP</b>	IP address of the FTP server
<b>Path and Filename</b>	Path of a directory on the FTP server where you have write access for saving the backup copy of the configuration file. Specify a filename if you want to save the file under another name. For example, to save the configuration file in a file whose name identifies its origin and date (such as KVM8802config040406) in a directory called “upload” on the FTP server, you would enter the following in the “Path and Filename” field: upload/KVM8802config040406.
<b>Username and Password</b>	Username for accessing FTP server (check with the FTP server’s administrator, if needed to obtain the username and password to use),

## ▼ To Back Up or Retrieve KVM/net Plus Configuration Data

1. In Expert mode, go to: Management>Backup Configuration.

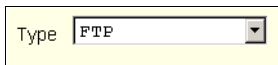
The Backup Configuration form appears.



The screenshot shows the 'Backup Configuration' form in the KVM/net Plus Web Manager. The interface has a yellow and orange theme. At the top left is the 'cyclades' logo. The top navigation bar includes 'Access | Configuration | Information | Management'. The top right corner shows 'logout' and system information: 'Host Name: KVM', 'IP Address: 192.168.50.72', and 'Model: KVMnet Plus 32'. On the left side, there is a sidebar menu with options: 'Backup Configuration', 'Firmware Upgrade', 'Microcode Upgrade', 'Microcode Reset', 'Active Sessions', and 'Reboot'. The main content area contains the 'Backup Configuration' form. It features a 'Type' dropdown menu set to 'FTP'. Below this are four input fields: 'Server IP', 'Path and Filename', 'Username', and 'Password'. At the bottom of the form are two buttons: 'Save' and 'Load'. 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', 'Help', and 'no unsaved changes'.

2. To save or retrieve data from an FTP server, do the following:

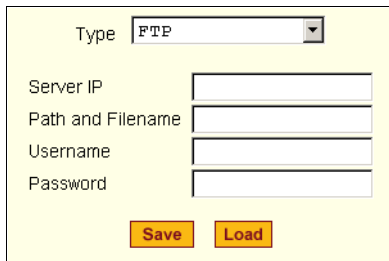
- a. From the Type drop-down list, select FTP.



A close-up of the 'Type' dropdown menu. The word 'Type' is on the left, followed by a dropdown box containing the text 'FTP' and a small downward-pointing arrow.



Selecting FTP (default) brings up the fields displayed in the following figure.

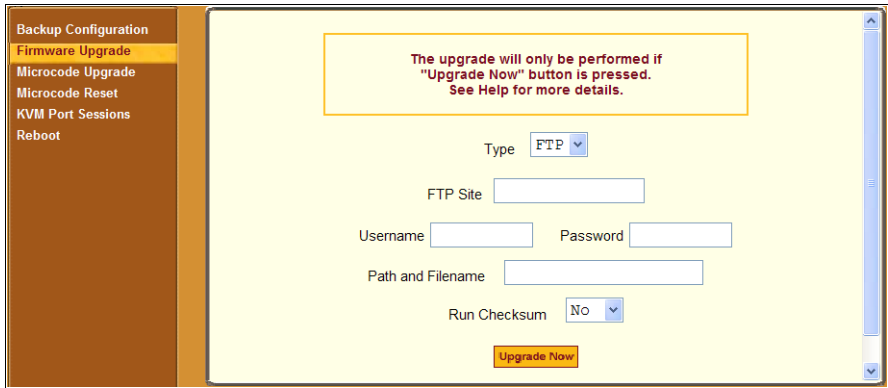


The image shows a configuration form for FTP. At the top, there is a dropdown menu labeled 'Type' with 'FTP' selected. Below this are four text input fields: 'Server IP', 'Path and Filename', 'Username', and 'Password'. At the bottom of the form are two buttons: 'Save' and 'Load'.

- b. Fill in the following fields with appropriate connection information:
  - Server IP
  - Path and Filename
  - Username
  - Password
3. Click Save to save the configuration to the selected location.
4. Click Load to load the configuration from the selected location.
5. Click “apply changes.”
6. To run the loaded configuration, reboot the KVM/net Plus.

## Firmware Upgrade

Selecting Management>Firmware Upgrade in Expert mode brings up the form shown in the following figure.



The screenshot shows a web interface for firmware upgrade. On the left is a vertical navigation menu with the following items: Backup Configuration, Firmware Upgrade (highlighted), Microcode Upgrade, Microcode Reset, KVM Port Sessions, and Reboot. The main content area has a yellow background and contains a warning box at the top: "The upgrade will only be performed if 'Upgrade Now' button is pressed. See Help for more details." Below the warning box are several form fields: a "Type" dropdown menu set to "ETP", an "FTP Site" text input field, "Username" and "Password" text input fields, a "Path and Filename" text input field, and a "Run Checksum" dropdown menu set to "No". At the bottom of the form is an orange "Upgrade Now" button.

You can use the form to set up automatic upgrades of the operating system and files on the KVM/net Plus. The form collects information used to automatically download software from an FTP server and install the software on the KVM/net Plus.

The following table defines the information you need to supply on the form.

Field/Menu Name	Definition
<b>Type</b>	FTP is the only supported type.
<b>FTP Site</b>	The address of the FTP server where the microcode is located. You can use any FTP server if you download the firmware on it first. The Cyclades FTP site address is: <code>ftp.cyclades.com</code> . If desired, see “To Upgrade Firmware” on page 275 for instructions on how to download the firmware for installation on your own local FTP server.
<b>Username</b>	Username recognized by the FTP server. The Cyclades FTP username for microcode downloads is “anonymous.”
<b>Password</b>	Password associated with the Username. An empty password is accepted for anonymous login at the Cyclades FTP server
<b>Path and File Name</b>	<p>The pathname of the software on the FTP server.</p> <p>On the Cyclades FTP server, the directory is under <code>pub/cyclades/alterpath/KVMnetPlus/released/version_number/filename</code>, where <i>version_number</i> is <code>V_N.N.N.</code>, and <i>N.N.N</i> is the most recent version number, for example, <code>1.2.1</code>. The filename includes the version number in the following format: <code>zImage_ons_NNN.bin</code>. The pathname for this example would be:</p> <pre>pub/cyclades/alterpath/KVMnetPlus/released/V_1.2.0/zImage_ons_121.bin</pre> <p>Go to <code>ftp://ftp.cyclades.com/pub/cyclades/alterpath/KVMnetPlus/released</code> in a browser, if needed, to verify the correct pathname and file names for the software (zImage) for the KVM/net Plus.</p>

The following table has links to the related procedures.

---

To Find the Cyclades Pathname for Firmware or Microcode Upgrades	Page 274
To Upgrade Firmware	Page 275
To Download Microcode From an FTP Server	Page 278

---

## ▼ **To Find the Cyclades Pathname for Firmware or Microcode Upgrades**

1. To find the correct filename for the firmware or microcode updates at Cyclades, Corp., enter the following address in a browser:

```
ftp://ftp.cyclades.com/pub/cyclades/alterpath/  
KVMnetPlus/released
```

2. In the `released` directory, go to the directory with the latest version number by clicking on the name of the directory.

For example, if the `released` directory contains directories named `V_1.1.0` and `V_1.2.0`, you would click on the `V_1.2.0` directory name. In the version directory, you would see several files like those shown in the following figure.

```
1.0.5.6-04.10.18.4bin  
KVM_v104.bin  
KVMterm_v104.bin  
KVMUSBterm_v106.bin  
zImage_ons_120.bin  
zImage_ons_120.md5
```

3. If upgrading the KVM/net Plus kernel, applications, and configuration files, take a note of the filename of the file whose name starts with `zImage` and has the `.bin` suffix and go to “To Upgrade Firmware” on page 275.
4. If upgrading the microcode on a KVM PS2 Terminator, take a note of the filename of the file whose name starts with `KVMterm` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server” on page 278.

5. If upgrading the microcode on a KVM USB Terminator, take a note of the filename of the file whose name starts with `KVMUSBterm` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server” on page 278.
6. If upgrading the KVM switch microcode, take a note of the filename of the file whose name starts with `KVM_vXXX` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server” on page 278.
7. If upgrading the microcode on KVM/net Plus IP modules take a note of the filename of the file whose name starts with a series of numbers separated by dots, for example, `1.0.5.6-04.10.18.4.bin`, and go to “To Download Microcode From an FTP Server” on page 278.

## ▼ **To Upgrade Firmware**

1. In the Web Manager, go to Management>Firmware Upgrade in Expert mode.

The Firmware Update form appears.

2. Choose FTP from the Type menu.
3. Enter the name of the FTP server in the “FTP Site” field.  
The Cyclades FTP site address is: `ftp.cyclades.com`.
4. Enter the username recognized by the FTP server in the “Username” field.  
The Cyclades FTP username for firmware downloads is “anonymous.”
5. Enter the password associated with the username on the FTP server in the “Password” field.

The Cyclades FTP server accepts any password for “anonymous” login.

6. Enter the pathname of the file on the FTP server. in the “Path and Filename” field.

On the Cyclades FTP server, the directory is under `pub/cyclades/alterpath/KVMnetPlus/released/version_number/`

See ““To Find the Cyclades Pathname for Firmware or Microcode Upgrades” on page 274, if needed.

7. Press the “Upgrade Now” button.
8. Click “apply changes.”

## Microcode Upgrade

Selecting Management>Microcode Upgrade in Expert mode bring sup the following form.

You can use the form to specify information used to automatically download microcode from an FTP server and install the microcode on various KVM/net Plus components. You can specify either the Cyclades FTP server, `ftp://ftp.cyclades.com`, or a local FTP server where you have previously downloaded the microcode.

The following table shows the terms used on the form, the corresponding component names, and the filename formats uses for each type of microcode.

Target Name Used on Form	Filename Format	Component
KVM Terminator	KVMterm_vNNN.bin	KVM Terminator (PS2)
	KVMUSBterm_vNNN.bin	KVM Terminator (USB)
KVM Switch (internal)	KVM_vNNN.bin	KVM switch (internal)
KVM Video Compression Modules	N.N.N.N-NN.NN.NN.N.bin	IP modules

You need to enter the actual pathname components in the “Directory” and “File Name” fields. If needed, go to: “To Find the Cyclades Pathname for Firmware or Microcode Upgrades” on page 274.

The following table defines the information you need to supply on the form.

Field Name	Definition
<b>Target</b>	The name of the component whose microcode you wish to upgrade.
<b>FTP Server</b>	The address of the FTP server where the microcode is located. You can use any FTP server if you download the firmware on it first. The Cyclades FTP site address is: <code>ftp.cyclades.com</code> .
<b>Username</b>	Username recognized by the FTP server. The Cyclades FTP username for microcode downloads is “anonymous.”
<b>Password</b>	Password associated with the Username. An empty password is accepted for anonymous login at the Cyclades FTP server
<b>Directory</b>	The pathname where the microcode resides on the FTP server. On the Cyclades FTP server, the directory is under <code>pub/cyclades/alterpath/KVMnetPlus/released/version_number/</code> filename. Go to <code>ftp://ftp.cyclades.com/pub/cyclades/alterpath/KVMnetPlus/released</code> in a browser, if needed, to verify the correct pathname and file names for the microcode for the KVM/net Plus.
<b>File Name</b>	The file name of the microcode for the “Target.”

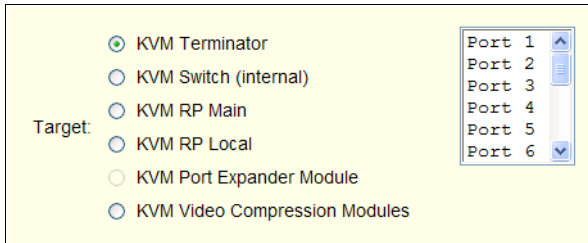
### ▼ **To Download Microcode From an FTP Server**

1. Go to Management>Microcode Upgrade in Expert mode.

The Microcode form appears.

2. Click the radio button next to the “Target” whose microcode you want to update.

If you select the KVM Terminator radio button, a scrollable port list appears next to the Target list.



The screenshot shows a form with a 'Target:' label and a list of radio buttons. The first option, 'KVM Terminator', is selected. To the right of the radio buttons is a scrollable list box containing 'Port 1' through 'Port 6'. The list box has a vertical scrollbar and arrow buttons at the top and bottom.

3. To download microcode for a KVM Terminator, select a port from the scrollable port list.
4. Enter the IP address or name of the FTP server in the “FTP Server” field.  
The Cyclades FTP site address is: `ftp.cyclades.com`.
5. Enter the username recognized by the FTP server in the “User” field.  
The Cyclades FTP username for microcode downloads is “anonymous.”
6. Enter the password associated with the username on the FTP server in the “Password” field.  
The Cyclades FTP server accepts an empty password for “anonymous” login.
7. Enter the pathname to the directory where the microcode resides on the FTP server. in the “Directory” field.  
On the Cyclades FTP server, the directory is `pub/cyclades/alterpath/KVMnetPlus/released/version_number/`
8. Enter the name of the microcode file in the “File Name” field.
9. Click the “Upgrade Now” button.
10. Click “apply changes.”



11. Go to “To Reset the Microcode After Upgrade” on page 279.

## Microcode Reset

Selecting Management>Microcode Reset in Expert mode brings up the form shown in the following figure.

You can use the form to reset the microcode after an upgrade.

### ▼ To Reset the Microcode After Upgrade

Perform this procedure if you have upgraded microcode as described in “To Upgrade Firmware” on page 275.

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

The Microcode Reset form appears.

2. To reset the microcode in a KVM Terminator, do the following steps.
  - a. Click the KVM Terminator radio button.  
A scrollable list of KVM ports appears.
  - b. Select the port to which the KVM Terminator is connected from the port list.
3. To reset another type of microcode, select the radio button next to the target you want to upgrade, either “KVM Switch (internal),” or “KVM Video Compression Modules.”
4. Press the “Reset Now” button.

## Active Sessions

The Active Sessions form is designed to provide you quick status and usage information pertaining to all active server sessions. Administrators may also kill sessions from this form.

### ▼ To View Active Sessions Information

1. In Expert mode, go to Management>Active Sessions.

The Active Sessions window appears.



2. Review the session information as described in the following table.

Column	Definition
Uptime	Time the KVM/net Plus has been on in minutes and seconds (mm:ss).
# Users	Number of users connected to server.
User	The user who initiated the session.

Column	Definition
TTY	The name of the KVM port.
From	The network machine to which the port is connected.
Login@	The day and time of the last login.
Idle	The time when the session or server became inactive.
JCPU	The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.
PCPU	The time used by the current process that is named in the What column.
What	The current process attached to the tty.

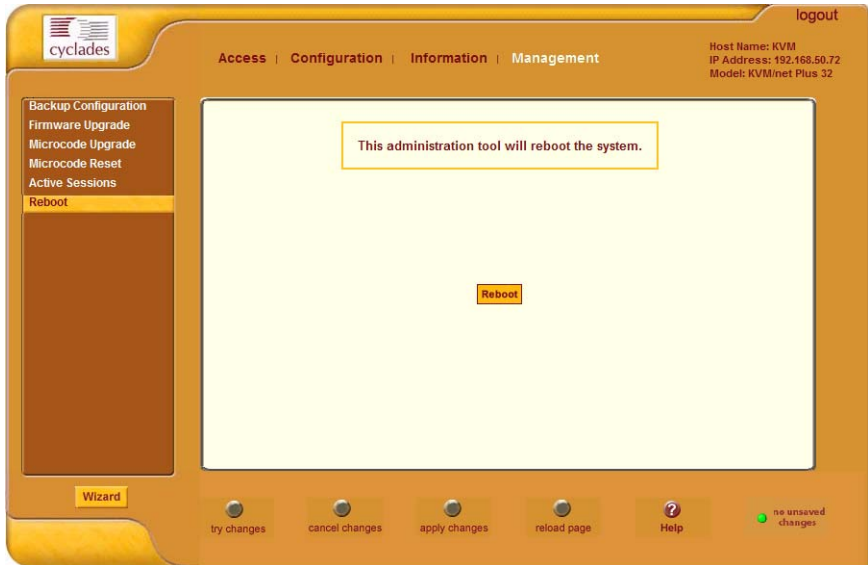
3. Select the Refresh button to update the form with current information.

## ▼ **To Kill an Active Session**

1. In Expert mode, go to Management>Active Sessions.  
The Active Sessions window appears.
2. Select the sessions you wish to kill.
3. Click Kill Session.
4. Click “apply changes.”

## Reboot

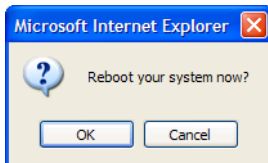
Selecting Management>Reboot in Expert mode, brings up the following form.



Selecting the Reboot button allows you to reboot the system without physically turning off the hardware.

### ▼ **To Reboot the KVM/net Plus From a Remote Location**

1. In Expert mode, go to: Management>Reboot
2. Click the Reboot button.
3. A confirmation page appears.



4. Click OK to reboot the system.

# Chapter 5

## Web Manager for Regular Users

With the KVM/net Plus Web Manager, regular users can connect to PCs with USB or PS/2 connectors or Sun servers with USB connectors through out-of-band, KVM connections and manage power of devices connected to AlterPath PMs from anywhere on a network. Regular users can also connect to Windows Terminal Servers through in-band connections.

For more information on in-band and out-of-band connections see “Server Access: In-band and Out of Band” on page 34.

For more information on power management, see “Power Management for Regular Users” on page 288.

For procedures on how to operate the KVM/net Plus as an administrator, see Chapter 4: Web Manager for Administrators.

## Web Manager for Regular Users

When users without administrative privileges log in to the KVM/net Plus, the Web Manager appears with three menu options:

- **Connect to Server** – Form used to connect to servers with either an in-band or a KVM connection.  
See “Connecting to Servers Remotely Through the Web Manager” on page 304.
- **IPDU Power Management** – Form used to control the power of devices plugged in to AlterPath PM IPDUs.  
See “Power Management for Regular Users” on page 288.
- **Security** – Form used to change your password.  
See “Changing Your KVM/net Plus Password” on page 289.

The IPDU Power Management and Security forms can be accessed by clicking the corresponding menu items.

The Web Manager interface provides you with a static main menu and a user entry form as displayed in Figure 5-1. The content of the user entry form changes based on your menu selection.



**Figure 5-1:** Cyclades KVM/net Plus Web Manager

## Prerequisites for Logging in to the Web Manager

You must collect the following information from your KVM/net Plus administrator before accessing and logging into the KVM/net Plus:

- KVM/net Plus IP address
- Username
- Password

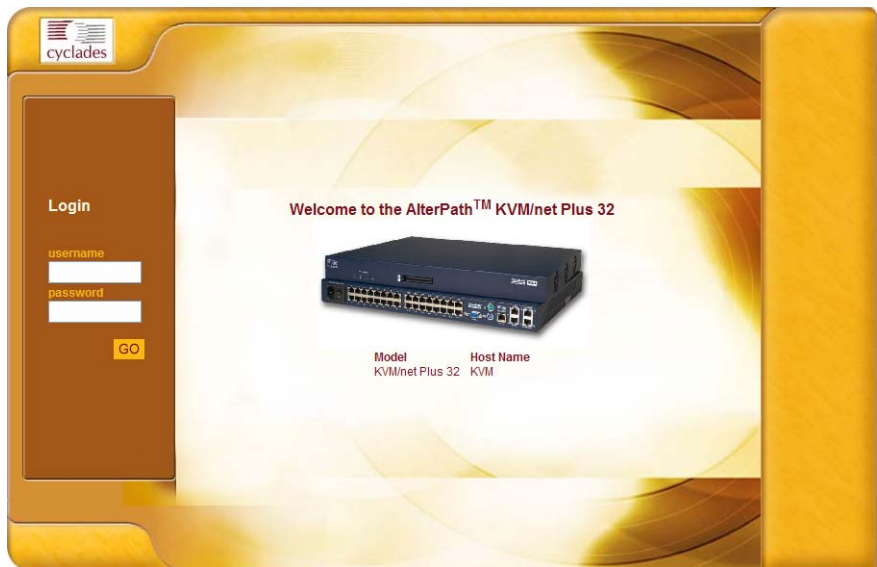
See the following sections for prerequisites for accessing servers with KVM and in-band connections:

- “Prerequisites for Accessing Servers With In-band Connections” on page 296
- “Prerequisites for Accessing Servers With KVM Connections” on page 297

### ▼ **To Log Into the KVM/net Plus Web Manager as a Regular User**

1. Launch a supported browser and type the KVM/net Plus IP address (for example `http://10.0.0.1/`) into the browser’s URL field.

The AlterPath KVM/net Plus log in screen appears.





2. Enter your username and password as provided to you by your KVM/net Plus administrator
3. Click Go.

The Connect form appears.



See “Web Manager for Regular Users” on page 284 for an introduction to using the Web Manager and links to more detailed information.

## Power Management for Regular Users

The KVM/net Plus offers two modes of controlling power:

- Power control of any device plugged into a PM that is configured on the KVM/net Plus.  
See “Power Control of Any Device Plugged Into a PM on the KVM/net Plus” on page 288.
- Power control of a server while connected to that server through a KVM port.  
See “Controlling Power of a KVM-connected Server” on page 329.

### ***Power Control of Any Device Plugged Into a PM on the KVM/net Plus***

Depending on your access rights, the KVM/net Plus allows you to remotely view and manage all PMs connected to the KVM/net Plus. Regular users can go to the IPDUs Power Management menu on the Web Manager and use the Outlets Manager and the View IPDUs Info forms to manage and view the status of PMs and the devices plugged into them. The following table lists the power management tasks available to regular users through the Web Manager and links to the associated procedures.

**Table 5-1:** Power Management Tasks Available to Regular Users

Task	Where Documented
Switch on/off and lock/unlock outlets; reboot network devices.	<ul style="list-style-type: none"> <li>• “Outlets Manager” on page 155</li> <li>• “To View Status, Lock, Unlock, and Cycle Power Outlets” on page 156</li> </ul>
View IPDU information by ports and slaves.	<ul style="list-style-type: none"> <li>• “View IPDUs Info” on page 156</li> <li>• “To View and Reset IPDU Information” on page 157</li> </ul>
Switch on/off and lock/unlock outlets; reboot servers connected to KVM ports.	<ul style="list-style-type: none"> <li>• “To Power On, Power Off, or Reboot the Connected Server [KVM]” on page 318</li> </ul>

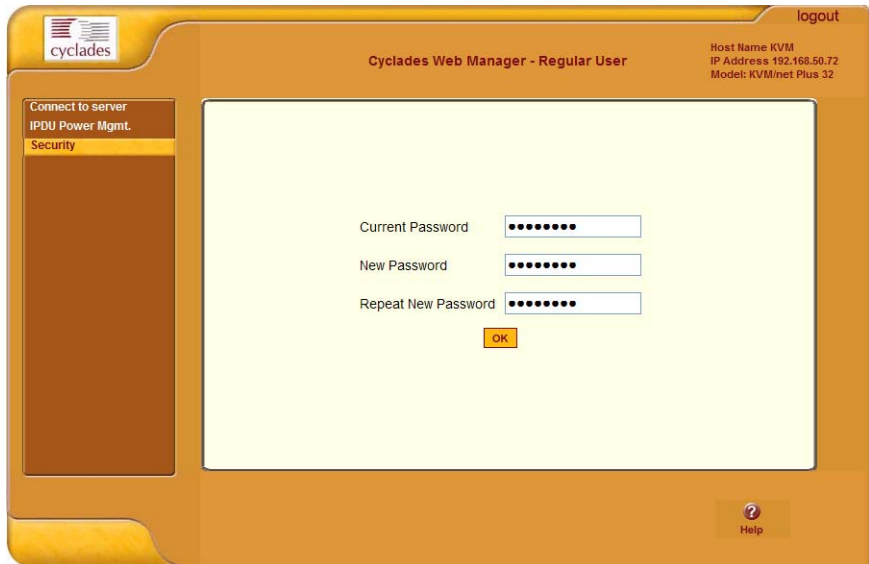
# Changing Your KVM/net Plus Password

On the Security form on the KVM/net Plus Web Manager, you can change your old password to a new password.

## ▼ *To Change Your KVM/net Plus Password*

1. Log in to the Web Manager.
2. Select Security in the Main Menu.

The Security Form appears.



The screenshot shows the Cyclades Web Manager interface. The top navigation bar includes the 'cyclades' logo, the text 'Cyclades Web Manager - Regular User', and a 'logout' link. On the right side of the header, system information is displayed: 'Host Name KVM', 'IP Address 192.168.50.72', and 'Model: KVMnet Plus 32'. A left-hand sidebar menu contains the following items: 'Connect to server', 'IPDU Power Mgmt.', and 'Security'. The 'Security' item is highlighted in orange. The main content area is a light yellow box containing three password input fields: 'Current Password', 'New Password', and 'Repeat New Password'. Each field is filled with black dots. Below the fields is an orange 'OK' button. A 'Help' icon is located in the bottom right corner of the interface.

3. Type your current password in the Current Password field.
4. Type your new password in the New Password field and again in the Repeat New Password field.
5. Click OK.



# Chapter 6

## Accessing Connected Devices

With the KVM/net Plus, users and administrators can connect to any PC or USB Sun servers through out-of-band, KVM connections and manage power of devices connected to AlterPath PMs from anywhere on a network with the Web Manager or locally with the OSD. Users and administrators can also connect to Windows Terminal Servers through in-band connections. .

This chapter gives an overview of the options for accessing servers that are connected to ports on the KVM/net Plus.

The following table lists the procedures in this chapter.

---

To View Connected Port Information	Page 325
To Connect to Another Port Using the Current AlterPath Viewer and Access Window Tab	Page 310
To Initiate Cycle by Server	Page 326
To Stop Cycling Between Ports	Page 311
To Connect to the Next Authorized Server from the Current Server	Page 327
To Adjust Screen Brightness and Contrast	Page 327
To Reset Your Keyboard and Mouse	Page 314
To Refresh the Information Displayed on the Access Window	Page 314
To Resume Your Port Connection After an Idle Timeout	Page 315
To Quit the Port Connection	Page 315
To Share a Server Connection	Page 317
To Power On, Power Off, or Reboot the Connected Server	Page 329
To Configure a PPP Connection on a Remote Computer	Page 340
To Make a PPP Connection From a Remote Computer	Page 342

---

---

To Set Up a Terminal Emulator Dial Up Connection Page 342

To Dial Into the KVM/net Plus Using a Terminal Emulator Page 343

---

## Who Can Access Connected Devices

Authorized users have the permissions they need to access one or more servers or other devices that are connected to ports on the KVM/net Plus. See “Types of Users” on page 20 and “KVM/net Plus Port Permissions” on page 29 for more information.

Authorized users and KVM/net Plus administrators have the following options for accessing connected devices:

- Use the Web Manager for most connections to devices.  
See “Cyclades Web Manager” on page 24 and “Prerequisites for Using the Web Manager” on page 25 for background information about the Web Manager, if needed.  
See “Connecting to Servers Remotely Through the Web Manager” on page 304 for instructions on how to log into the Web Manager and connect to devices.
- Use the on-screen display (OSD) to access devices that are connected to the KVM/net Plus’ KVM ports.  
Local users and administrators who have access to a directly connected Local User station can use the OSD Connect menu.  
Chapter 7: “On Screen Display” describes how to access connected devices through the OSD.
- Dial into the KVM/net Plus through a modem  
See “Modem Connections” on page 339.

## Server Connections: What You See

Once connected to a server, one or two windows appear depending on the type of server connection being made:

- KVM connections
  - AlterPath Viewer is launched with the same interface as if you were directly logging into the connected server.
  - The Access Window with an interface for managing up to four server connections.

See “Viewing KVM Connections” on page 294.

- In-band connections

An ActiveX viewer is launched with the same interface as if you were directly logging into the connected server.

See “Viewing In-band Connections” on page 296.

## Viewing KVM Connections

The AlterPath Viewer is the interface you use to manage servers over KVM over IP connections. Logins persist across connection sessions. If you close a connection without logging out, you are still logged in the next time you connect, unless the system has closed your session. If you are not currently logged in, you see a login screen or prompt.

The connected servers's login prompt appears. The following example shows a login prompt for a Windows 2000 server displayed by the AlterPath Viewer. If you are connected to a Linux server without a graphical display, you see a "Login:" prompt.

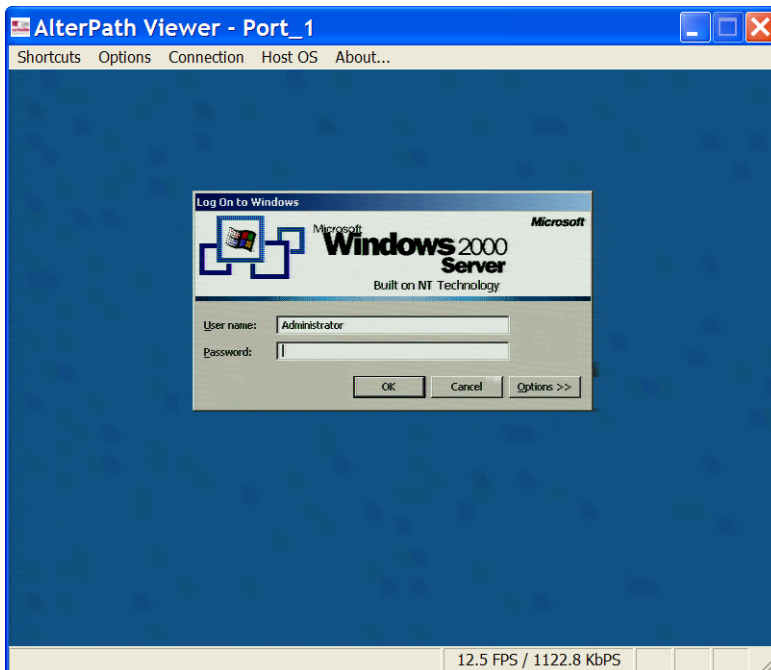


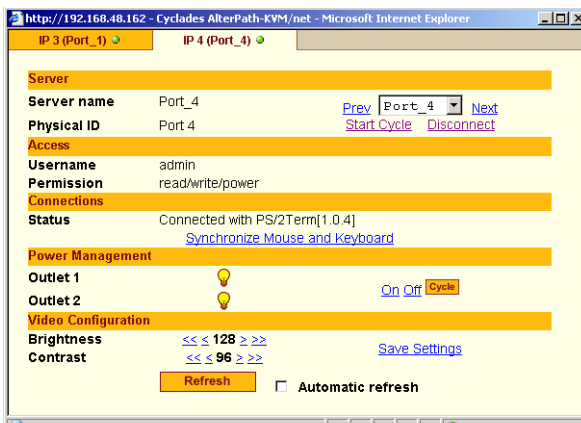
Figure 6-1: AlterPath Viewer for KVM Connections



See “AlterPath Viewer Settings” on page 332 for more detailed information about using the AlterPath Viewer.

Local KVM connections through the OSD do not use the AlterPath Viewer. Instead, the view of the connected server takes up the entire screen of local work station. See “Controlling Local KVM Port Connections Through the OSD” on page 322 for more information on local KVM connections.

The Access Window, displayed in the following figure, is a separate pop-up window that contains up to four tabs—one for each active KVM device connection made through the Web Manager. The tabs of the Access Window dynamically change status information and viewer event messages as the connection information changes.



**Figure 6-2:** Access Window

See “Managing Multiple Server Connections with the Access Window” on page 308 for more detailed information about the Access Window.

## Viewing In-band Connections

The ActiveX viewer is the interface you use to manage servers over an in-band connection.

The following graphic displays the login screen of a server running Windows 2003 in the ActiveX viewer for in-band connections.

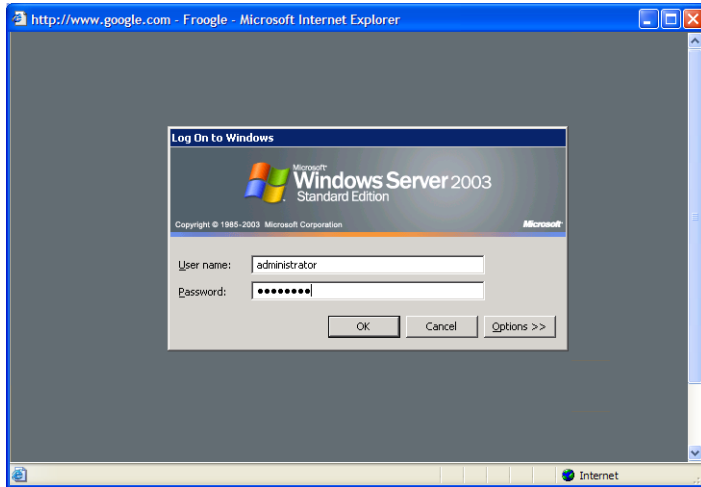


Figure 6-3: ActiveX Viewer for In-band Connections

## Prerequisites for Accessing Servers With In-band Connections

A KVM/net Plus user who needs to access any RDP server must have the following:

- The username and password of a valid account on the RDP server.
- Internet access and Microsoft Internet Explorer on a remote Windows client machine.

# Prerequisites for Accessing Servers With KVM Connections

The following prerequisites must be met before you can access a KVM-connected server:

- Know the KVM Port(s) to which you have access (especially if direct access to a port is configured)
- Have the username and password of a valid account on the connected server
- If you are connecting through the Web Manager, have the following:
  - A remote computer running a Windows operating system with Internet access and a supported browser installed
  - The IP address of the KVM/net Plus
- If you are making a local connection, have a direct connection made to the User 1 or User 2 ports of the KVM

## Web Manager Login Screen

The following table list the sections that describe the three different possible views of the Web Manager login screen that can appear under various conditions.

**Table 6-1:** Web Manager Login Screen Options

Conditions	Where Documented
Direct logins to KVM ports not enabled: <ul style="list-style-type: none"> <li>• You enter the KVM/net Plus' IP address in a browser to bring up the Web Manager login screen.</li> <li>• You can log into the Web Manager and perform administration.</li> <li>• If you want to access a server connected to a KVM port after logging into the Web Manager, you can connect to the KVM port from the Connect to Server form.</li> </ul>	“Login Screen: Direct Logins Not Enabled” on page 299

**Table 6-1:** Web Manager Login Screen Options (Continued)

Conditions	Where Documented
<p>Direct logins to KVM ports enabled (option 1):</p> <ul style="list-style-type: none"> <li>• You enter the KVM/net Plus' IP address in a browser to bring up the Web Manager login screen.</li> <li>• You enter your username and password and the desired KVM port number on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first.</li> </ul>	<p>“Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 301</p>
<p>Direct logins to KVM ports enabled (option 2):</p> <ul style="list-style-type: none"> <li>• You enter the KVM/net Plus' IP address along with the port name in a browser to bring up the Web Manager login screen.</li> <li>• The port field is already filled in when the Web Manager appears.</li> <li>• You save the URL that includes the port in a favorites file to save time when logging into the same port in the future.</li> <li>• You enter your username and password on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first, as in the previous row.</li> </ul>	<p>“Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 302</p>

---

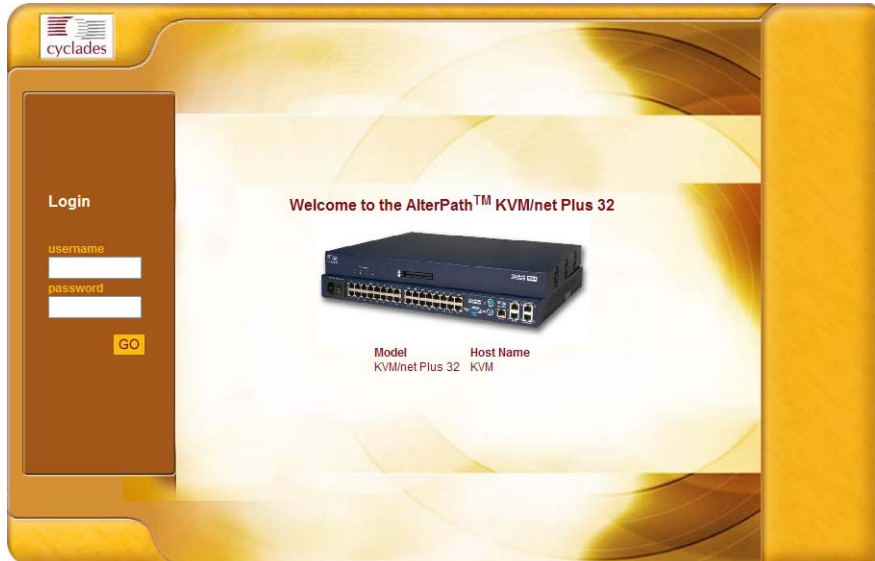
**Note:** The direct access method allows users to access servers that are connected to KVM ports only or servers that are connected to KVM ports and are available for in-band access as well. This method is particularly useful for users who may need direct KVM access to a server that has both KVM and in-band access enabled.

---

## Login Screen: Direct Logins Not Enabled

The following screen shows an example of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the KVM/net Plus is entered in the browser.
- Direct logins to KVM ports is not enabled.

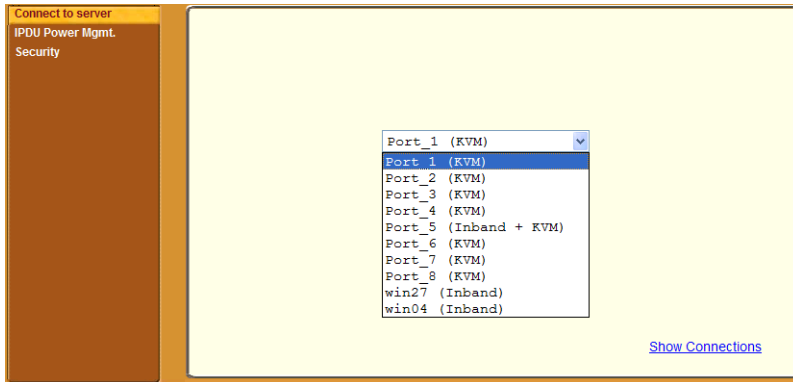


**Figure 6-4:** Web Manager Login Screen Without KVM Direct Logins Enabled

As shown in Figure 3-1, the Web Manager login screen displays two fields in the “Login” section: “username” and “password.” The product name appears in the “Welcome” line, and the model and the administrator-specified hostname are listed below images of the front and back of the product.

## Connect to Server Drop-down List

With the connect to server drop-down list, you can select the in-band or KVM server you want to connect to.



**Figure 6-5:** Connect To Server Drop-down List

The following sections can help you to identify whether a server has an in-band connection, KVM connection, or both and whether it is connected to a cascaded KVM device.

### ***Servers and Connection Types in the Connect to Server Drop-down List***

There are two levels of identifying servers in the Connect to Server drop-down list:

- **Connection Type** – The types of connections that can be made to each server is displayed in parenthesis at the end of each server entry in the list. An entry with “(KVM)” at the end of it can be accessed with a KVM connection only. An entry with “(Inband)” at the end of it can be accessed with an in-band connection only. An entry with “KVM + Inband”) can be accessed with both connection methods. See “Determining the Connection Type and its Supported Functionality” on page 36 for more detailed information.
- **Server Name or Port Name/Number** – The type of connection determines the type of name applied:
  - Individual KVM ports are either labelled by the port number in the form Port\_# or by an administrator-defined alias, which should describe the

type of computer connected to the port or be the actual name of the connected server.

- Individual in-band connections are labelled by an administrator-defined server name, which should identify the type of computer being accessed or be the actual name of the server.

---

**Note:** A server that is configured for both in-band and KVM connections can have two different aliases configured: one for the KVM port and one for the in-band connection. In this case, the alias that appears in the Connect to Server drop-down list is the alias assigned to the KVM port.

---

### ***Port Numbers of Cascaded KVM Devices in the Connect to Server Drop-down List***

In the Connect to Server drop-down list on the Connect to Server form, a name and a number connected by a period (.) indicate the alias or name of the cascaded KVM unit followed by its physical port.

For example, in the port name kvm2.4, kvm2 is the name of the cascaded device, and 4 is the physical port on the device named kvm2.

## ***Login Screen: Direct Logins Enabled, Only IP Address Entered***

The following screen shows an example of the format of the Login portion of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the KVM/net Plus is entered in a browser.
- Direct logins to KVM ports is enabled.



The screenshot shows a login form with a dark blue background. At the top, the word "Login" is displayed in white. Below it, there are three input fields, each with a label in yellow text: "username" (containing "ana"), "password" (containing three black dots), and "port" (containing "2"). A yellow "GO" button is located at the bottom right of the form.

## ***Login Screen: Direct Logins Enabled, IP Address and Port Entered***

This section describes how the Web Manager login screen appears if the following two conditions are true:

- Direct logins to KVM ports is enabled,
- The IP address of the KVM/net Plus is entered along with a port ID (in the required format) in a browser

The required format is:

*IP\_address/login.asp?portname=portnumber*

where *IP\_address* is the IP address of the KVM/net Plus and *portnumber* is the portnumber or alias assigned to the KVM port.

Entering the port number along with the IP address makes it possible to connect directly to a KVM port without going to the Web Manager's Access page first. You can save the URL as a bookmark or in your browser's favorites list and go directly to the port login later without typing in the entire URL. The "port" field is filled in with the port number when the Web Manager login window appears.

The example in the following figure shows `http://192.168.46.169/login.asp?portname=Port_1` entered in the Address field of a Microsoft Internet Explorer browser. The login screen displays empty "username" and "password" fields and a port field filled with the name of the port from the URL, in this case "Port\_1."





**Figure 6-6:** Example: Web Manager with Direct Logins Enabled, IP Address and Port Entered

# Connecting to Servers Remotely Through the Web Manager

KVM/net Plus administrators who are logging into the Web Manager to perform KVM/net Plus configuration can use any modern browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla, or Firefox).

See “Web Manager Login Screen” on page 297 for a description of the ways authorized users can connect to servers from the Web Manager.

See the following procedures for connecting to servers:

---

To Connect to a KVM Port Through the Web Manager Login Screen	Page 306
To Connect to Servers Through The Web Manager’s Connect To Server Form	Page 304

---

If needed, see one of the following login procedures.

---

To Log Into the Web Manager as Admin	Page 138
To Log Into the KVM/net Plus Web Manager as a Regular User	Page 286

---

## ▼ **To Connect to Servers Through The Web Manager’s Connect To Server Form**

1. Log in to the KVM/net Plus using your username and password.

See “To Log Into the KVM/net Plus Web Manager as a Regular User” on page 286 or “To Log Into the Web Manager as Admin” on page 138 for detailed instructions on logging in to the Web Manager.

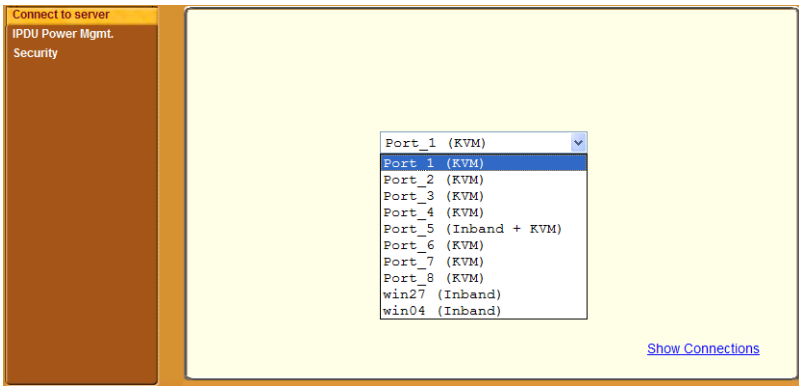
2. From the left menu panel, select Connect to Server.

The Port Connection form appears.



- 3. From the drop-down menu, select the server or port to which you want to connect.

A list similar to the list in the following graphic appears.



See “Determining the Connection Type and its Supported Functionality” on page 36 for a description of each type of connection method and what happens once connected.

- 4. Click on the Connect button.

The system may launch one or two browser windows: the AlterPath viewer and the Access Window for KVM connections, or an ActiveX

viewer for RDP connections. See “Server Connections: What You See” on page 293 for a description of each window.

---

**Note:** The first time the system invokes the AlterPath Viewer, it prompts you to accept a security certificate. Click Accept.

---

## ▼ **To Connect to a KVM Port Through the Web Manager Login Screen**

This procedure assumes that the KVM/net Plus administrator has enabled direct logins to KVM ports.

1. Enter the IP address of the KVM/net Plus alone or the IP address of the KVM/net Plus followed by the KVM port number (in the required format) in the address field of a browser.

The required format for entering a KVM port number in the URL is:

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

where *IP\_address* is the IP address of the KVM/net Plus and *portnumber* is the portnumber or alias assigned to the KVM port.

---

**Note:** Check with the administrator who configured the basic network parameters on the KVM/net Plus, for help finding the IP address and the “admin” password, if needed. Also if needed, see an example of the proper format for entering the port number in “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 302.

---

- If DHCP is not enabled, use a fixed IP address assigned by the network administrator to the KVM/net Plus.
- If DHCP is enabled, enter the dynamically assigned IP address.

The Web Manager login screen appears. If you entered a KVM port ID in the URL, the “port field” is filled in with the port ID you entered.

2. If you entered a KVM port ID in the URL, save the URL as a bookmark or in your favorites list in the browser.

For future connections to that port, you can click on the bookmark or item in favorites list to easily bring up the Web Manager login screen again with the port number filled in.

3. Enter your account name in “username” field and the account’s password in the “password” field.
4. If no port is listed in the “port” field, enter a port alias or number.
5. Press “Go.”

If the Web Manager Access “Connect to Server” form appears, you are finished logging in.

6. For administrators, if a dialog box prompts you to verify whether you want to proceed by logging the other admin out or by cancelling your login attempt, click the appropriate radio button and then click Apply.

---

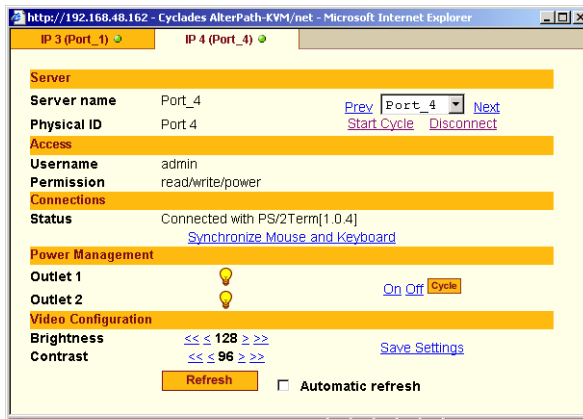
**Note:** Only one admin can be logged in at a time.

---

# Managing Multiple Server Connections with the Access Window

One KVM over IP user can make up to four KVM server connections from one work station, can control servers through separate AlterPath Viewer windows, and can use the Access window to manage each active KVM connection. The tabs of the Access Window dynamically change status information and viewer event messages as the connection information changes.

For example, if a regular user is connected to two ports, two tabs are activated on the Access Window: These tabs are labeled with the name of the port. The following figure displays an example of what the Access Window looks like when two port connections are made, to Port\_1 and Port\_4.



**Figure 6-7:** Access Pop-up Window with Two Active Port Connections

Once connected to a server through a KVM port, you may want to do one or more of the tasks listed in the following table with links to more detailed information.

**Table 6-2:** Tasks Available During KVM Connections

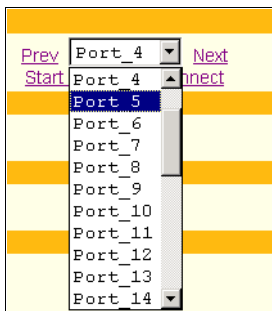
Task	Where Documented
Review information about the connected port.	“To View Connected Port Information” on page 325
Make direct connections to other servers without returning to the Web Manager Port Connection form.	<ul style="list-style-type: none"> <li>• “To Connect to Another Port Using the Current AlterPath Viewer and Access Window Tab” on page 310</li> <li>• “To Initiate Cycle by Server” on page 326</li> <li>• “To Connect to the Next Authorized Server from the Current Server” on page 327</li> </ul>
Adjust the color and brightness of the server window.	“To Adjust Screen Brightness and Contrast” on page 327
Reset your keyboard and mouse.	“To Reset Your Keyboard and Mouse” on page 314
Refresh the port information on the port tab.	“To Refresh the Information Displayed on the Access Window” on page 314
Resume a Web Manager connection after an idle timeout.	“To Resume Your Port Connection After an Idle Timeout” on page 315
Quit the port connection and close the AlterPath Viewer for the selected session.	“To Quit the Port Connection” on page 315
Access a KVM port that is already in use by another user.	“To Share a Server Connection” on page 317
Power on, power off, or reboot the connected server.	“To Power On, Power Off, or Reboot the Connected Server” on page 329

## ▼ **To View Connected Port Information**

1. On the Access window, select the tab that corresponds to the desired port connection.
2. Review the contents of each row:
  - Server Name – The alias of the port to which the connection is made
  - Administrators configure port aliases on the
  - Physical ID – The name of the port
  - Username – Name of user connected to the port
  - Permission – The permissions that user has on the current port
  - Connections – Hardware and software version of the Cyclades Terminator used to connected the server to the KVM/net Plus
  - Outlets – The power status of the outlets on an AlterPath PM that the connected server is plugged into
  - Brightness – The brightness level of the AlterPath Viewer
  - Contrast – The contrast level of the AlterPath Viewer

## ▼ **To Connect to Another Port Using the Current AlterPath Viewer and Access Window Tab**

1. On the Access window, select the Tab that corresponds to the desired port connection.
2. Select a port from the drop-down list.





This changes the port connection of the selected session; changes the contents of the Viewer; and updates the Port Information and tab identification to correspond with the newly selected port.

## ▼ *To Cycle Between Ports*



Initiating a server cycle changes the contents of the AlterPath Viewer so that the server connected to each available port is viewed for a fixed period of time.

1. On the Access window, select the Tab that corresponds to the desired port connection.
2. Click Start Cycle.

Server	
Server name	Port_4 <a href="#">Prev</a> Port_4 <a href="#">Next</a>
Physical ID	Port 4 <a href="#">Start Cycle</a> <a href="#">Disconnect</a>

The system initiates the cycle from the first authorized server, and the servers connected to all authorized ports appear for a few moments in the AlterPath Viewer.



Once the cycling begins, the Stop Cycle option appears on the Access Window.

IP 3 (Port_4)  	
Event	Cycle started.
Server	
Server name	Port_4 <a href="#">Stop Cycle</a>
Physical ID	Port 4

Talk to the KVM/net Plus administrator if you want to change the period of time that each server appears during the cycle.

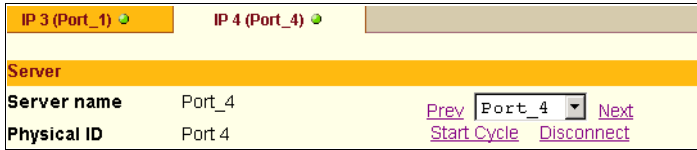
## ▼ *To Stop Cycling Between Ports*

Click Stop Cycle on the Access Window.

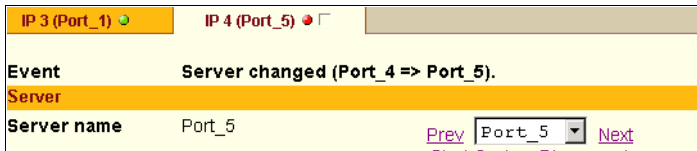
IP 3 (Port_4)  	
Event	Cycle started.
Server	
Server name	Port_4 <a href="#">Stop Cycle</a>
Physical ID	Port 4

## ▼ **To Connect to the Previous or Next Authorized Port Without Opening a New AlterPath Viewer**

1. On the Access window under Server, click Previous or Next adjacent to the port drop-down list.



The display in the AlterPath Viewer and the active tab changes from the currently connected port to the next or previous authorized port in the ports list.



2. Repeat Step 1 to move up or down in the port list.

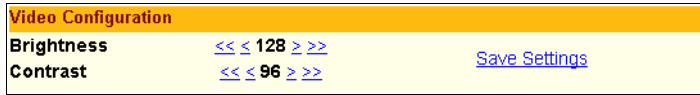
## **Adjusting Screen Brightness and Contrast**

The Video Configuration section on the Access window allows you to control the screen brightness and contrast of your KVM connection session.

These values are used to compensate for cable length from the KVM/net Plus to the server. The longer the cable used, the lower the values for brightness and contrast should be. For example, if you use a 500-foot-long cable, the setting should 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.

## ▼ **To Adjust Screen Brightness and Contrast**

1. On the Access window, select the Tab that corresponds to the desired server connection.



2. Under the Video Configuration section, click one of the following Brightness or Contrast arrows:

**Table 6-3:** Access Window Brightness and Contrast Arrows

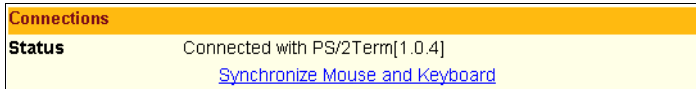
Button	Description
<<	Double arrow left decreases the screen brightness or contrast by 16 units.
<	Single arrow left decreases the screen brightness or contrast by 1 unit.
>>	Double arrow right increases the screen brightness or contrast by 16 units.
>	Single arrow right increases the screen brightness or contrast by 1 unit.

3. Optionally click Save Settings to save the brightness and contrast values for other KVM sessions.

## ▼ **To Reset Your Keyboard and Mouse**

Use this feature if the keyboard or mouse stop responding during a KVM connection.

1. On the Access window, select the Tab that corresponds to the desired port connection.

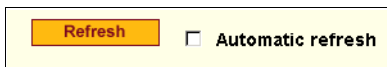


2. Under the Connections row, click the Synchronize Mouse and Keyboard button.

The mouse reappears and the keyboard regains functionality.

## ▼ **To Refresh the Information Displayed on the Access Window**

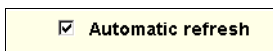
1. On the Access window, select the Tab that corresponds to the desired port connection.
2. Click the Refresh button.



The page is refreshed with current information.

3. To have the access window automatically refreshed every 10 second, check the Automatic Refresh check box.

The Refresh button is removed from the Access window and only the Automatic refresh check box appears.



4. To revert to refreshing the window only when the Refresh button is clicked, clear the Automatic Refresh check box.

## ▼ **To Resume Your Port Connection After an Idle Timeout**

On the Access window, click Reconnect.

## ▼ **To Quit the Port Connection**

Do one of the following:

- On the Access window, select the tab that corresponds to the desired port connection and click Disconnect.
- On the AlterPath Viewer menu bar, go to: Shortcuts > Exit Viewer Client. Performing any one of the previous actions closes the viewer for the selected session, quits the KVM connection, and inactivates the tab.

# Sharing a Server Connection

The KVM/net Plus supports shared connections to a server. 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. Depending on the action selected by the connecting user, notifications are also presented to the current user.

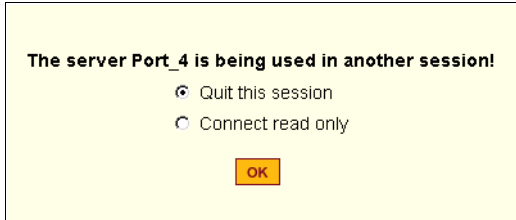
Options available under this menu vary depending on the connecting user's access permissions. When accessing a KVM port that is already in use by another user, two connection options may be displayed depending on the connecting user's access privileges for that port:

**Table 6-4:** Connection Option According to Port Access Permissions

<b>Connection Option</b>	<b>Permission needed to connect to port</b>
Connect read only	Read-only Read-write Read-write-power (full access)
Connect read write	Read-write Read-write-power (full access)

As displayed in Figure 6-8, the following two options are always presented in the menu to the connecting user:

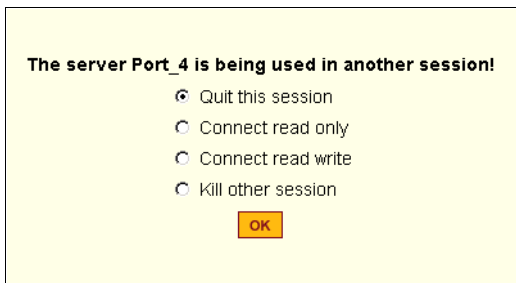
- Quit – Quits the connection attempt and returns to the Connect to Server form.
- Connect read only – Connects the user in read-only mode, and the Access Window displays an event notification to the current user.



**Figure 6-8:** Connection Options for Users with Read Only Permission

As displayed in Figure 6-9, if the connecting user has either read-write or read-write-power (full access) permission to the port, the following additional options are presented in the menu:

- Connect read write – Connects the connecting user in read-write mode. If the current user is in read-write mode, that user’s access is changed to read-only, and an event notification appears in the Access window.
- Kill the other session – Kills the existing session and connects the connecting user in read-write mode. The previous user is disconnected from the server port, and an event message appears in the Access window.



**Figure 6-9:** Connection Options for Users with Read-Write or Read-Write-Power Permissions

---

**Note:** When the currently connected user is in read-only mode, the connecting user is always granted the highest access privilege based on his or her permission rights.

---

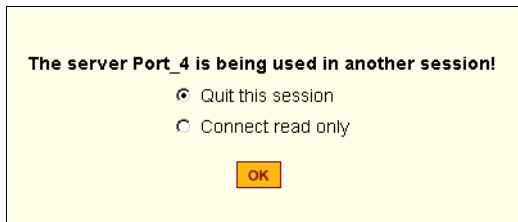
Once two users are connected to a server port, either user may choose at any time to change his/her access mode (or disconnect from the session by issuing a escape sequence command)

## ▼ **To Share a Server Connection**

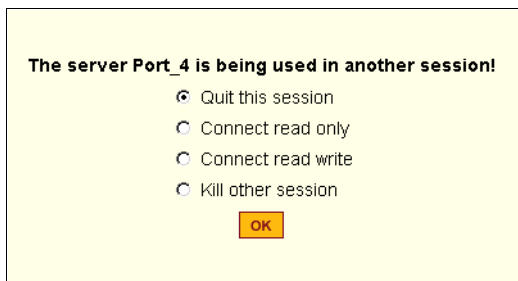
1. Connect to a port that is in use by another KVM/net Plus user.

A message indicating that another user is connected to the port appears. The message changes depending on your access privilege to that port:

- If you have read only access, the following window appears with the Quit and Connect read only options.



- If you have either read-write or read-write-power access permission to the server port, the following window appears with these additional options:



2. Select one of the following options:

- To quit the connection attempt and return to the Connection Menu, select Quit this session.

- To connect to the server in read-only mode, select Connect read-only.
- To connect to the server in read-write mode and notify the previous user, select Connect read write.

If the current user is connected in read-write mode, his or her access mode is changed to read-only, and the a message appears on the Access Window.

- To kill the existing session and connect in read-write mode, select Kill other session.

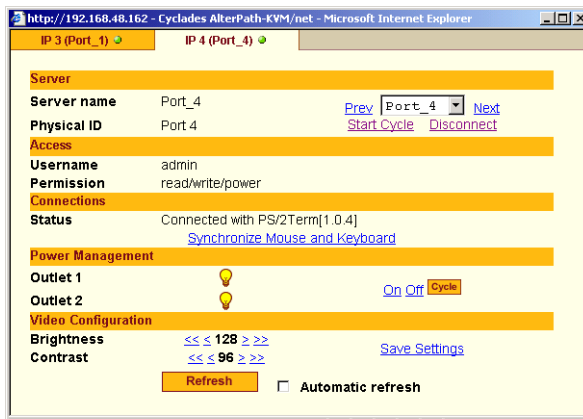
The current user is disconnected from the server port. The AlterPath Viewer closes, and a message is displayed in the active tab. After the next refresh occurs, the tab disappears.

Once at least two users and up to four users are connected to a server port, any user may choose at any time to change his/her access mode by reconnecting to the server port, or the users can disconnect from the session.

## ▼ **To Power On, Power Off, or Reboot the Connected Server [KVM]**

Make sure all the prerequisites for controlling power on KVM-connected servers are met before attempting this procedure.

1. Connect to a server through a KVM port.
2. On the Access window, select the Tab that corresponds to the desired server connection.







3. To view the status of the connected outlets, view the light bulb icons adjacent to the outlet numbers under the Power Management field.

The icons are described in the following table:

**Table 6-5: Power Status Icons**

Icon	Description
	A yellow light bulb indicates that the power is on.
	A grey light bulb indicates that the power is off.

4. To turn the power on, click On
5. To turn the power off, click Off.
6. To cycle the power (turn the power off then on), click Cycle.

Once you make a selection, the page is reloaded with the updated power status.

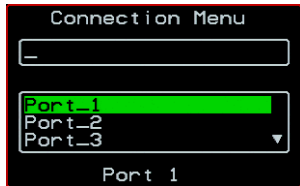
7. To lock or unlock outlets, you must go to the Power Management menu on the Web Manager.

See “Power Management for Regular Users” on page 288 for more information.

By default, regular users have no access to all outlets, and admin users have full access.

## Connecting to Servers Locally Through the OSD

Administrators and authorized regular users who have local access to the KVM/net Plus can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are connected to KVM ports on the master KVM/net Plus or on any cascaded KVM device.



Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the KVM/net Plus. See “To Connect to the User 1 Management Port” on page 85 for instructions on connecting to the User 1 port, or see “To Connect the RP to the KVM/net Plus” on page 131 for instructions on connecting to the User 2 port.

Connections made through the OSD are to physically connected devices only. Use the Web Manager to connect to a remote device. See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 304 for instructions.

---

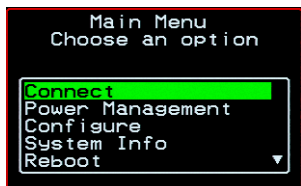
**Note:** The OSD cannot be used to access in-band servers. See “Connecting to Servers Remotely Through the Web Manager” on page 304 for information and instructions on accessing in-band servers.

---

## ▼ To Connect to Servers Through the OSD Connection Menu

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

The OSD Main Menu appears.



2. From the OSD Main Menu, select Connect.

The Connection Menu appears.



3. To select the port you wish to connect to, do one of the following procedures:
  - Type the first letters of the port name in the quick search box until the desired port is highlighted in the port list box.
 

This field is case-sensitive.
  - Select the desired port using the port list box.
4. Press Enter.

Your monitor displays the work station of the connected server.

See Table 6-6, “Tasks Available While Connected to KVM Ports Through the OSD,” on page 322 for a complete lists of the tasks available while connected to KVM ports through the OSD and references to the related instructions.

# Controlling Local KVM Port Connections Through the OSD

Once connected to a server through the OSD, you may want to do one or more of the procedures listed in the following table.

**Table 6-6:** Tasks Available While Connected to KVM Ports Through the OSD

Task	Where Documented
Return to the OSD Connection menu after connecting to a port.	“To Return to the Connection Menu After Connecting to a Port” on page 325.
Access a port that is already in use by another user.	“Sharing KVM Port Connections” on page 330
Make direct connections to other servers without returning to the OSD Connection Menu.	<ul style="list-style-type: none"> <li>• “To Initiate Cycle by Server” on page 326</li> <li>• “To Connect to the Next Authorized Server from the Current Server” on page 327</li> <li>• “To Connect to the Previous Authorized Server from the Current Server” on page 327</li> </ul>
Reset your keyboard and mouse.	“To Reset the Keyboard and Mouse” on page 328
Adjust the color and brightness of the server window.	“To Adjust Screen Brightness and Contrast” on page 327
Power on, power off, or reboot the connected server.	“To Power On, Power Off, or Reboot the Connected Server” on page 329
View information about the currently selected port.	“To View Connected Port Information” on page 325

## Hot Keys for Local

Predefined keyboard shortcuts (also called hot keys) allow you to perform common actions and launch management windows while connected through a KVM port.

The default hot keys are described in the following table. A plus (+) between two keys indicates that both keys must be pressed at once. When two keys are separated by a space, each key must be pressed separately. For example, “Ctrl+k p” means to press the Ctrl and “k” keys together followed by the “p” key, and “Ctrl Shift+i” means press the Ctrl key followed by the Shift and “i” keys pressed together.

**Table 6-7:** Default Local Keyboard Shortcuts Through the OSD

Key Combination	Action
Ctrl+k q	Quit. Closes the connection to the current KVM port and ends the local.
Ctrl+k p	Power management. Brings a power management menu with the options to turn on, off, or cycle the power for outlets to which the current server is connected.
Ctrl+k .	Next Port. Goes to the next authorized port.
Ctrl+k ,	Previous Port. Returns to the previous authorized port.
Ctrl+k v	Video. Brings up a menu that allows you to change between “Automatic control” (which compensates for the length of the cable running from the KVM/net Plus to the KVM Terminator that is connected to the server) and “Manual control” for adjusting screen brightness and contrast.
Ctrl+k s	Reset keyboard and mouse. Allows you to reset the keyboard and mouse if either of them stops responding.

The KVM/net Plus administrator may redefine the keyboard shortcuts, as described in “Redefining KVM Connection Hot Keys” on page 40. If the defaults shown in the previous table do not work, check with your KVM/net Plus administrator for the site-specified keys to use.

## Hot Keys for Emulating Sun Keyboard Keys

The KVM/net Plus provides a default set of hot keys for use while connected to Sun servers. You can use the Sun hot keys to emulate keys that are present on Sun keyboards but are not present on Windows keyboards.

The hot keys are made up of an escape key followed by a function key. The default escape key is the Windows key, which is labeled with the Windows logo. The Windows key usually appears on the Windows keyboard between the `Ctrl` and `Alt` keys. The following table shows function keys and keys from the numeric keypad that emulate Sun equivalent keys when you enter them at the same time as the hot key. For example, to use the Sun `Find` key, you would press the Windows key at the same time you press the `F9` function key.

**Table 6-8:** Default Sun Key Emulation Hot Keys

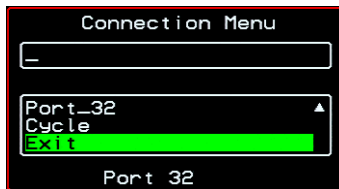
	Win Key	Sun Key
<b>Function Keys</b>	F2	Again
	F3	Props
	F4	Undo
	F5	Front
	F6	Copy
	F7	Open
	F8	Paste
	F9	Find
	F10	Cut
	F11	Help
	F12	Mute
	<b>Numeric Keypad Keys</b>	*
+		Vol +
-		Vol -

KVM/net Plus administrators can change the default escape key portion of the Sun keyboard emulation hot keys from the Windows key to any of the following: `Ctrl`, `Shift`, or `Alt`. See “Redefining Sun Keyboard Equivalent Hot Keys” on page 40 for details and links to procedures.

## ▼ **To Return to the Connection Menu After Connecting to a Port**

1. Press `Ctrl+k q` to display the OSD Connect Menu.

The Connection Menu appears.



2. Do one of the following:

- To make a new server connection, select another port from the list.
- To return to the Main Menu, select Exit.
- To cycle through all servers, select Cycle.

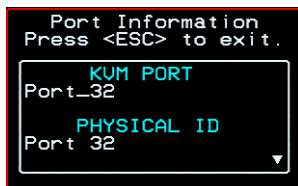
The cycle option does not appear when you are connected through the Web Manager.

## ▼ **To View Connected Port Information**

1. Use the information keyboard shortcut.

The default is `Ctrl+k i`.

The following window appears.



2. Press `Esc` to exit the Port Information window and return to the connected server.

## ***Cycling Between Servers***

Cycle refers to the capability to connect to one or more authorized servers from the server to which you are currently connected. Through the OSD menus or by using a keyboard shortcut, you have immediate access to all configured and authorized servers.

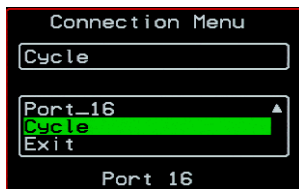
There are two types of cycle commands:

- Cycle by Server – View all authorized servers on a continuous basis until all servers have been exhausted and then start over again.
- Cycle by Key Sequence – View or access the server connected to the next or previous port in the Connection Menu list.

The servers are cycled in the order in which their ports are listed in the Server Connection form.

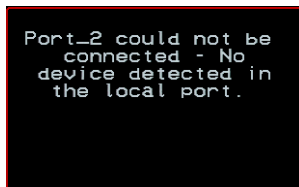
### **▼ *To Initiate Cycle by Server***

1. From the Connection Menu, choose Cycle.



2. Select Cycle at the bottom of the list.

The system initiates the cycle from the first authorized server, and the servers connected to all authorized ports appear for a few moments. If there is no device attached to the port associated with the next logical port, a message appears to indicate that there is no device connected.



3. To abort the process and close the session, press the escape sequence.

The default is Ctrl+k q.



## ▼ **To Connect to the Next Authorized Server from the Current Server**

- Use the Next keyboard shortcut.  
The default is **Ctrl+k .**  
The next authorized server appears. Repeat this step to move to the next server.

## ▼ **To Connect to the Previous Authorized Server from the Current Server**

- Use the Previous keyboard shortcut.  
The default is **Ctrl+k ,**.  
The previous authorized server appears. Repeat this step to move to the previous server.

## ▼ **To Adjust Screen Brightness and Contrast**

1. Press the video control keyboard shortcut.

The default is **Ctrl+k v**.

Depending on which window was accessed last, one of the following windows appears.

- Automatic Control



- Manual Control



2. To switch to the Auto control window or the Manual control window select Auto or Manual respectively.
3. To adjust screen brightness and contrast on the Automatic Control window, select the right or left arrows to set the desired adjustment value.

The Automatic Control window is used to compensate for cable length. For example, if you use a 500-foot cable, the setting might be 10 or 20. If a shorter cable such as 6 or 3 feet is used, a value of 128 or 150 is more appropriate. If this setting is not adjusted properly, the video quality may be poor.

4. To adjust screen brightness and contrast on the Manual control page, select the arrow keys to increase or decrease the contrast and brightness.

The Manual Control window is used to control the levels of video brightness and contrast. The higher the value, the greater the brightness and contrast will be.

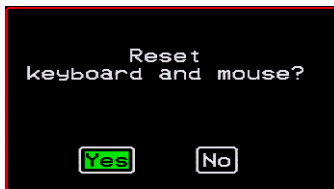
## ***Resetting the Keyboard and Mouse***

You can use the “Keyboard/Mouse Reset” hot key to bring up the “Reset keyboard and mouse?” screen if the keyboard and mouse is not working properly when accessing a server through a KVM port. This command is equivalent to unplugging and plugging in again the keyboard and mouse.

### **▼ *To Reset the Keyboard and Mouse***

1. Type the “Keyboard/Mouse Reset” hot key.

The default is Ctrl-k s. The following confirmation window appears.



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

---

**Note:** See also the “Avoiding Conflicting Mouse Settings” on page 107.

---

## Controlling Power of a KVM-connected Server

In order to control power of a server while connected to the server, the following conditions must be met:

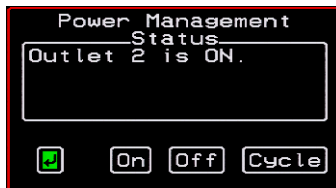
- The server must have at least one power cord plugged into an AlterPath PM that is properly configured and connected to the AUX 1 port.
- The power outlet(s) that the server is connected to must be configured to the port.
- If a regular user is accessing this device, the user must have the following permissions:
  - Full control (read, write, power) permission on the port,
  - Permission to control power on the PM outlet that the device is plugged into.

### ▼ To Power On, Power Off, or Reboot the Connected Server

1. While connected to a server, use the power management keyboard shortcut.

The default is **Ctrl+k p**.

A window similar to the following appears.



2. Select the configured outlet.
3. Do one of the following:
  - To turn the power on, select On.
  - To turn the power off, select Off.
  - To reboot, select Cycle.

To lock or unlock outlets, you must go to the Power Management menu. See “Power Management” on page 336 for more information.

## ***Closing a Local KVM Connection***

The ways you can close a KVM connection are listed below:

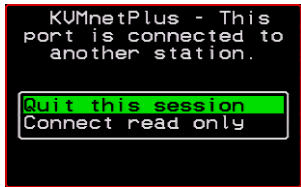
- Use a hot key sequence (Ctrl+k q) to bring up the Connection menu, then select the Exit option.
- Let the session time out.

### **▼ To Close a KVM Connection**

## ***Sharing KVM Port Connections***

Two authorized users can connect simultaneously to a single KVM port.

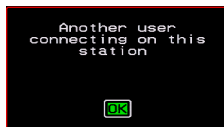
When a user connects to a KVM port that is already in use, the software presents a menu to the connecting user. The options on the menu depend on the connecting user's access permissions. The following figure shows two options that are always presented on the menu to the connecting user.



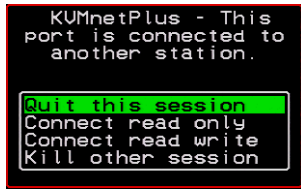
The two menu options are described in the following table.

---

<b>Quit this session</b>	Ends the connection attempt and returns the user to the Connection Menu
<b>Connect read only</b>	Connects the user in read-only mode and sends this notice to the current user:



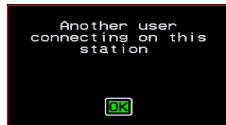
If the connecting user has either read-write, or full access permissions for the KVM port, additional menu options appear, as shown in the following figure.



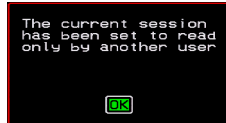
The two menu options are described in the following table.

---

<b>Connect read write</b>	Connects the new user in read-write mode and sends this notice to the current user.
---------------------------	---

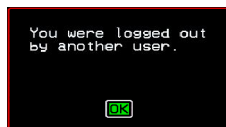


If the previous user is in read-write mode, that user's mode is changed to read-only and the user sees the following notice:




---

<b>Kill other session</b>	Kills the existing session and connects the new user in read-write mode. Sends the following notice to the current user and disconnects that user:
---------------------------	--




---

When the current user is in read only mode, the connecting user is always granted the highest level of access for which the connecting user is authorized.

If two users are connected to a KVM port, either user may choose at any time to change the access mode or disconnect from the session by issuing a hot key or Esc.

## AlterPath Viewer Settings

You can configure the AlterPath viewer settings from the top menu.

[Shortcuts](#) [Options](#) [Connection](#) [Host OS](#) [About...](#)

For a definition of the menu settings, refer to the tables below. A T1 connection is recommended for best performance when using the AlterPath Viewer.

### *Recommended Settings*

The recommended AlterPath Viewer settings are listed in the following table. The connection you set must reflect your actual Internet connection method.

<b>Menu</b>	<b>Select the following option(s):</b>
<b>Options</b>	Auto Sync Mouse
<b>Connection</b>	T1 (preferred), No Encryption, High Color
<b>Host OS</b>	Auto/Other

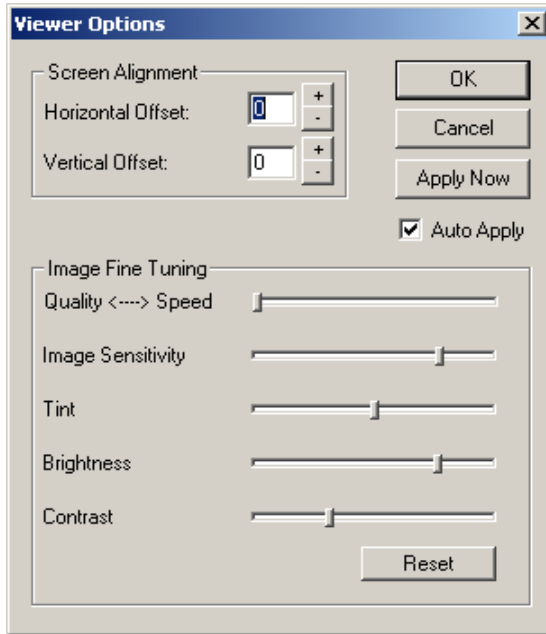
## Options Menu

The following table describes the items in the AlterPath Viewer's Options menu, which you can change as needed for your own requirements.

Menu Selection	Description
<b>Force Screen Refresh</b>	Refreshes the viewer.
<b>Force Screen Auto Alignment</b>	Switches to Auto Alignment mode, which may change the position of the viewer. (You can manually configure Screen Alignment by going to Options>Viewer Options>Screen Alignment.)
<b>Toggle Full Screen</b>	Switches the viewer's display from window to full-screen mode or from full-screen to window mode.
<b>Viewer Options</b>	See Setting the Viewer Options
<b>Show Frames/sec and Network bits/sec</b>	Specify as needed.
<b>Auto Sync Mouse</b>	Make sure this is selected for KVM/net Plus compatibility
<b>Show Startup Dialog</b>	Causes a menu to appear when the viewer is launched.

## Setting the Viewer Options

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



**Figure 6-10:**AlterPath Viewer Options Screen

The following table defines the fields and menu items.

**Table 6-9:** AlterPath Viewer>Options>Viewer Options Menu

Field or Menu Item	Function
<b>Horizontal Offset</b>	The horizontal coordinate for positioning the AlterPath Viewer on the screen (default = 0).
<b>Vertical Offset</b>	The vertical coordinate for positioning the AlterPath viewer on the screen (default = 0).
<b>Quality &lt;----&gt;Speed</b>	Move slider to the left to increase image quality; move slider to the right to increase the performance of the viewer.



**Table 6-9:** AlterPath Viewer>Options>Viewer Options Menu (Continued)

<b>Field or Menu Item</b>	<b>Function</b>
<b>Image Sensitivity</b>	Move slider to the right to increase the image sensitivity.
<b>Tint</b>	Move the slider in either direction to achieve the desired color. For a neutral (white) color, keep the slider in the middle.
<b>Brightness</b>	Move the slider to the right to increase screen brightness.
<b>Contrast</b>	Move the slider to the right to increase screen contrast.

## ***Connection Menu***

The following table describes the Connection menu options.

<b>Menu Selection</b>	<b>Function</b>
<b>56K</b>	For when your network connection method is a 56K modem
<b>DSL</b>	For when your network connection method is a DSL line
<b>T1</b>	Recommended connection type. For when your network connection method is a dedicated T1 line
<b>Low BW LAN</b>	For when you are connecting through a low bandwidth local area network
<b>LAN</b>	For when you are connecting through a standard speed local area network.
<b>Auto</b>	For setting the connection mode automatically
<b>Encrypt Everything</b>	For encrypting everything
<b>Encrypt Keyboard and Mouse</b>	For encrypting only keyboard and mouse input
<b>Encryption Type</b>	For either RC4 or Triple DES encryption

Menu Selection	Function
<b>No Encryption</b>	For no encryption
<b>High Color</b>	For high color resolution screens
<b>Low Color</b>	For low color resolution screens
<b>Grey Scale</b>	For grey scale screens
<b>Low Grey Scale</b>	For low resolution grey scale screens

## Power Management

Administrators and authorized users can access Power Management windows, which allow you to check the status of the master IPDU connected to the AUX port in addition to all cascaded IPDUs, from the Web Manager and the OSD. Any user who has administration privileges can turn on, turn off, cycle (reboot), lock, and unlock the outlets. See “Options for Managing Power” on page 44 for a detailed description of how authorized users can manage power. See “Setting Up and Configuring Power Management” on page 46 for a list of the administrative tasks involved in setting up power management.

The following section gives instructions on managing power through the OSD while connected locally to the KVM/net Plus.

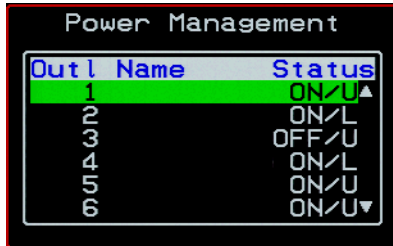
For instructions on how to manage power remotely through the Web Manager, see Table 5-1 on page 288 for a list the power management tasks available to regular users through the Web Manager and links to the associated procedures.

For instructions on managing power servers while connected to them through KVM ports, see “To Power On, Power Off, or Reboot the Connected Server” on page 329.

## ▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets

1. Go to: Configure > Power Management.

The Outlet Status page appears with a list of all configured IPDUs. The status column displays whether the outlet is on or off, locked, or unlocked.

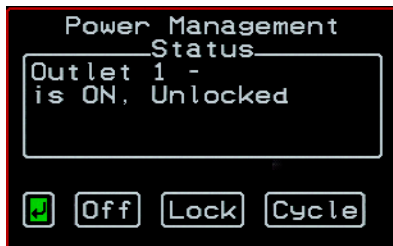


Outl Name	Status
1	ON/U▲
2	ON/L
3	OFF/U
4	ON/L
5	ON/U
6	ON/U▼

The letter U displayed in the status window indicates that the outlet is unlocked; the letter L indicates that the outlet is locked.

2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

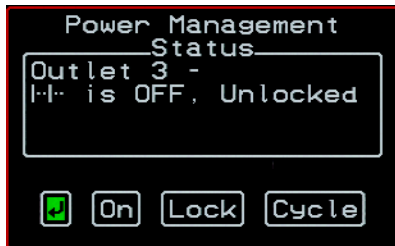
The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.



The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is locked displays only the Unlock option as in the following figure.



An outlet that is turned off and unlocked displays the On, Lock, and Cycle options as in the following figure.



3. Use the arrow keys to select On, Off, Lock, Unlock, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

# Modem Connections

In addition to connecting to the KVM/net Plus through a regular Ethernet connection, you can also access the KVM/net Plus by dialing in through either of the two following modem types:

- An installed external modem
- A modem on a PCMCIA card

You use either of the following methods to dial in:

- Use PPP (when dialing into any of the supported modems)

Once the connection is made, all connections to the specified IP address are made through the PPP connection. For example, if you enter the specified IP address in a browser after making the PPP connection, the browser connects to the KVM/net Plus through the dialup connection. This way you can access the Web Manager through PPP even if the IP connection to the KVM/net Plus is not available.

- Use a terminal emulator (only when dialing into a modem on a PCMCIA card)

On a computer running a Windows operating system, you can use HyperTerminal or another terminal emulator. On a computer running a UNIX-based operating system, such as Solaris or Linux, you can use a compatible terminal emulator such as Kermit or Minicom.

Once the dial in connection is made using the terminal emulator, you get console access to the KVM/net Plus.

The KVM/net Plus administrator performs the procedures to install and configure the modems. Contact your KVM/net Plus administrator for the phone numbers, usernames, and passwords to use, and for questions about how the modems are configured.

Before anyone can use PPP to access the KVM/net Plus, the PPP connection must be configured by the user on the remote computer so the connection can be used for dialing in. Before configuring PPP, you need the following:

- A modem connected to the remote computer.
- The phone number of the line that is dedicated to the KVM/net Plus modem you want to access.
- If authentication is required for the modem, you need a username and password for a user account on the KVM/net Plus.

The following table lists the related procedures and where they are documented.

**Table 6-10:**Tasks for Configuring and Making Dial Up Connections (User)

---

Configure a PPP Connection	“To Configure a PPP Connection on a Remote Computer” on page 340
Connect Using PPP	“To Make a PPP Connection From a Remote Computer” on page 342
Configure a Terminal Connection	“To Set Up a Terminal Emulator Dial Up Connection” on page 342
Connect Through a Terminal Emulator	“To Dial Into the KVM/net Plus Using a Terminal Emulator” on page 343

---

### ▼ ***To Configure a PPP Connection on a Remote Computer***

Perform this procedure on a remote computer with a modem to do the following:

- Create a PPP connection that anyone can use for dialing up the KVM/net Plus
- Optionally configure call back.

See the prerequisites listed in “Modem Connections” on page 339, if needed.

---

**Note:** The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems. You can use this procedure as an example.

---

1. From “My Computer,” go to “My Network Places.”
2. Under “Network Tasks,” click “View network connections.”
3. Under “Network Tasks,” select “Create a new connection.”  
The “New Connection Wizard” appears.
4. Click the “Next” button.
5. Click “Connect to the Internet” and click “Next>.”

The “Getting Ready” form appears.

6. Click “Set up my connection manually” and click “Next>.”

The “Internet Connection” form appears.

7. Click “Connect using a dial-up modem” and click “Next>.”

The “Connection Name” form appears.

Type a name for the connection to the KVM/net Plus in the “ISP Name” field and click “Next>.”

The “Phone Number to Dial” form appears.

8. Type the phone number for the KVM/net Plus’ modem in the “Phone number” field and click “Next>.”

The “Internet Account Information” form appears.

9. Type the username for accessing the KVM/net Plus in the “User name” field.

10. Type the password for accessing the KVM/net Plus in the “Password” and “Confirm Password” field and click “Next>.”

11. Click the “Finish” button.

The “Connect *connection\_name*” dialog appears.

12. Click the “Cancel” button.

The name of the connection appears on the Network Connections” list.

13. To configure call back, do the following steps.

- a. Select the name of the connection from the Network Connections dialog box.

- b. Select “Dial Up Preferences” from the “Advanced” menu.

The “Dial-up Preferences” dialog box appears.

- c. Click the “Callback” tab.

- d. Click “Always call me back at the number(s) below.”

- e. Highlight the name of the modem and click “Edit.”

The “Call Me Back At” dialog box appears.

- f. Enter the phone number of your local modem in the “Phone number:” field, and click OK.

## ▼ **To Make a PPP Connection From a Remote Computer**

Perform this procedure on a remote computer that has a modem to initialize a dial up and optional call back session on the KVM/net Plus. This procedure assumes a PPP connection for dial up or call back has previously been created as described in “To Configure a PPP Connection on a Remote Computer” on page 340.

---

**Note:** The following steps work if you are on a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use these steps as an example.

---

1. From the Start menu, go to My Computer>My Network Places.
2. Under “Network Tasks,” click “View network connections.”
3. Double-click the name of the connection in the list.  
The “Connect *connection\_name*” dialog appears.
4. Type the username and password in the “User Name” and “Password” fields.
5. Click the “Dial” button

## ▼ **To Set Up a Terminal Emulator Dial Up Connection**

Do this procedure on a remote computer that has a modem to create a terminal emulator connection that anyone can use for dialing up a modem that is on a PCMCIA card on the KVM/net Plus. See the prerequisites listed in “Modem Connections” on page 339, if needed.

---

**Note:** The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use this procedure as an example.

---

1. From the Start menu, go to All Programs>Accessories>Communications>Hyperterminal.
2. Select “New Connection” from the “File” menu.



3. Type a name in the “Name” field, select an icon for the connection, and click OK.
4. Enter the phone number assigned to the PCMCIA modem card.
5. Select a country or region from the “Country/region” drop-down list.
6. Fill in the “Area Code” and “Phone number” fields.
7. Select the modem from the “Connect using” drop-down list, and click OK.

The new connection appears in the list of connections appearing on the “Open” menu.

### ▼ **To Dial Into the KVM/net Plus Using a Terminal Emulator**

This procedure requires a PCMCIA modem card installed on the KVM/net Plus. If the KVM/net Plus administrator has configured the PCMCIA modem card for call back, when you dial in, the KVM/net Plus calls you back. Contact your KVM/net Plus administrator if you have questions about the configuration. This procedure also assumes that someone has previously created a connection in the terminal emulator, as described in “To Set Up a Terminal Emulator Dial Up Connection” on page 342.

---

**Note:** The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use this procedure as an example.

---

1. From the Start menu, go to All Programs>Accessories>Communications>Hyperterminal>*connection\_name*.

For example, a previously configured connection named “dialin\_kvm” appears in the HyperTerminal Open list as “dialin\_kvm.ht.”

If the KVM/net Plus administrator has configured the PCMCIA modem card for call back, when you dial in, the KVM/net Plus calls you back.

The terminal emulator appears with console access to the KVM/net Plus.

2. If authorization is required for the modem, log in.



# Chapter 7

## On Screen Display

Administrators and regular users can use the OSD for troubleshooting when a direct connection method is required. However, most configuration and operations tasks are performed through the Web Manager, as described in Chapter 5 and Chapter 4.

Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the KVM/net Plus. See “To Connect to the User 1 Management Port” on page 85 for instructions on connecting to the User 1 port, or see “To Connect the RP to the KVM/net Plus” on page 131 for instructions on connecting to the User 2 port.

Once the connected monitor is turned on, the OSD login window appears.

See the following sections for more information on the OSD screens:

---

Navigating the OSD	Page 346
Logging In Through the OSD	Page 347
OSD Main Menu	Page 348
Connection Menu	Page 349
Power Management Menu	Page 350
Configure Menu Overview	Page 351
System Info Menu	Page 416
Reboot	Page 417
Controlling the OSD Through the AlterPath KVM RP	Page 418

---

## Navigating the OSD

In the OSD you can use keyboard sequences to navigate the windows and make menu selections. The following sections describe:

- Basic Navigation Keys
- Common Navigation Actions

### ***Basic Navigation Keys***

The following table displays a short list of keyboard controls to help you navigate the KVM/net Plus on screen display. The OSD window must be selected and in an *active* state for these keys to work.

**Table 7-1:** Basic Navigation Keys

<b>Key</b>	<b>Action</b>
<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 / Commits changes
<b>Esc</b>	Returns to the previous main menu

## Common Navigation Actions

Table 7-2 shows how to perform common actions used to go to windows, select items, and commit changes in the OSD.

**Table 7-2:** OSD Equivalents for Common Actions

Action	OSD Equivalent
Select OK	Tab to the OK button and press the Enter key on your keyboard.
Save changes	Tab to the Save button and press the Enter key.
Select an option	Tab to the option and press the Enter key.
Go to a specific window, as in: <b>Go to Configure&gt;Users and Groups.</b>	Select the first option from the Main menu. On the next window that comes up select the next option from that menu. Do this until you get to the last option in the menu path.

## Logging In Through the OSD

In order to log in to the KVM/net Plus through the OSD, you need to connect a keyboard, monitor, and mouse to the monitor, keyboard, mouse connectors, labelled User 1, on the KVM/net Plus. See “To Connect to the User 1 Management Port” on page 85 for more information.

Optionally, you can connect to the OSD using an AlterPath KVM RP, which you buy separately. See “Installing the AlterPath KVM RP” on page 129 for instructions on installing the RP. See “Controlling the OSD Through the AlterPath KVM RP” on page 418 for instructions on using the RP.

## ▼ To Log In to the KVM/net Plus Through the OSD

1. Type your username followed by your password.

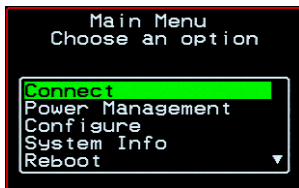


2. Press <Enter>.

The main menu of the KVM/net Plus OSD appears. See the following section, “OSD Main Menu” on page 348 for a description of the OSD Main Menu items.

## OSD Main Menu

The OSD Main Menu provides six menu selections as depicted in the following figure.



**Figure 7-1:** OSD Main Menu

Table 7-5 gives a brief description of each menu item and lists where you can find more information.

**Table 7-3:** OSD Main Menu Items

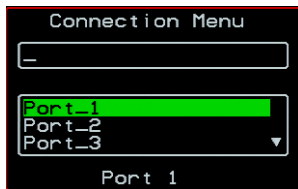
Menu Selection	Select the menu item to:	Where Documented
<b>Connect</b>	View the Server Connection Menu and select the port to which you want to connect.	Page 349

**Table 7-3: OSD Main Menu Items**

<b>Menu Selection</b>	<b>Select the menu item to:</b>	<b>Where Documented</b>
<b>Power Management</b>	View status of all outlets on connected IPDUs and power on, power off, and cycle connected devices.	Page 350
<b>Configure</b>	View the Configuration Menu and perform KVM/net Plus configuration.	Page 351
<b>System Info</b>	View the system information pertaining to the KVM version that you are using.	Page 416
<b>Reboot</b>	Reboot the KVM/net Plus.	Page 417
<b>Exit</b>	Exit from the OSD and close the session.	N/A

## Connection Menu

Administrators and authorized regular users can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are physically connected to KVM ports on the master KVM/net Plus or on any cascaded KVM device.



See “To Connect to Servers Through the OSD Connection Menu” on page 321 for instructions on connecting to servers through the OSD.

## Power Management Menu

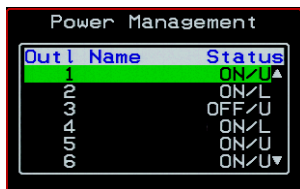
The Power Management windows allow you to check the status of the master IPDU connected to the AUX 1 port in addition to all cascaded IPDUs. Any user who has administration privileges can turn on, turn off, cycle (reboot), lock, and unlock the outlets. See “Connecting AlterPath PMs to the KVM/net Plus” on page 117 for instructions on connecting IPDUs to the KVM/net Plus.

For instructions on managing power through the OSD, see

### ▼ **To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets**

1. Go to: Configure > Power Management.

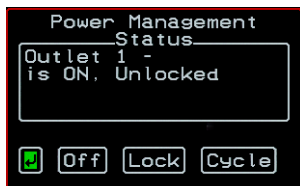
The Outlet Status page appears with a list of all configured IPDUs. The status column displays whether the outlet is on or off, locked, or unlocked.



The letter U displayed in the status window indicates that the outlet is unlocked; the letter L indicates that the outlet is locked.

2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.

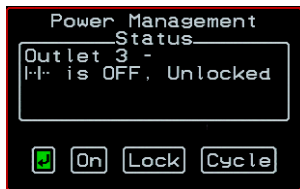




The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is locked displays only the Unlock option as in the following figure.



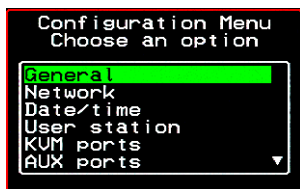
An outlet that is turned off and unlocked displays the On, Lock, and Cycle options as in the following figure.



3. Use the arrow keys to select On, Off, Lock, Unlock, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

## Configure Menu Overview

Selecting “Configure” from the OSD Main Menu brings up the Configuration Menu. The Configuration Menu provides a number of options, as shown in the following screen.



Not all the options are visible. Table 7-4 gives a brief description of all the menu options and lists where you can find more information

**Table 7-4:** Configuration Menu Items

Menu Selection	Select the menu item to:	Where Documented
<b>General</b>	Configure authentication type for direct logins to KVM ports; syslog facility number; KVM connection hot key escape sequence, and Sun Keyboard emulation hot key escape sequence. <b>Note:</b> syslogging also requires configuration of the syslog server using the Syslog option, described later in this table.	“General Configuration Screens [OSD]” on page 355
<b>Network</b>	Configure DHCP or assign an IP address and configure other basic network parameters; configure SNMP, VPN, IP filtering, hosts, and static routes	“Network Configuration Menu Options [OSD]” on page 358
<b>Date/Time</b>	Enable/disable NTP or manually configure the system date and time.	“Date/time Configuration Screens” on page 381
<b>User Station</b>	Configure the Local User station’s idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current work station.	“User Station Screens” on page 382
<b>KVM Ports</b>	Activate KVM ports, assign aliases, and enable power management.	“KVM Ports Screens” on page 386
<b>AUX Ports</b>	Configure the AUX ports for PPP or power management.	“AUX Ports Screens” on page 388
<b>Users and Groups</b>	Configure users and groups, user passwords, and KVM port access permissions.	“Users and Groups Screens” on page 394
<b>Cascade Devices</b>	Add, edit, or delete configurations of cascaded (slave) KVM units.	

**Table 7-4: Configuration Menu Items (Continued)**

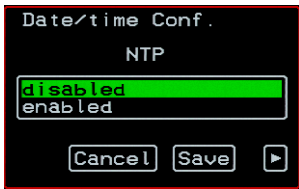
<b>Menu Selection</b>	<b>Select the menu item to:</b>	<b>Where Documented</b>
<b>Syslog</b>	Configure the IP address of the syslog server. <b>Note:</b> syslogging also requires assignment of a facility number using the General option, described earlier in this table.	“Syslog Screens” on page 401
<b>PCMCIA</b>	Configure PCMCIA cards.	“PCMCIA Screens” on page 401
<b>Authentication</b>	Configure an authentication method for logins to the KVM/net Plus and authentication servers for KVM/net Plus and KVM port logins.	“Authentication Screens” on page 405
<b>Save/Load Config</b>	Permanently save configuration changes, load a stored configuration or restore the configuration to factory default values.	“System Info Menu” on page 416
<b>Exit</b>	Exit from the menu.	N/A

## Understanding OSD Configuration Screen Series

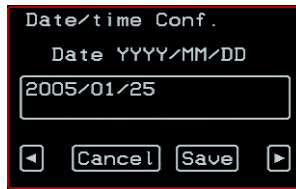
Selecting an option from the “Configure” menu usually brings you through a series of related screens, which you navigate through one at a time until you reach the final screen.

For example, if you select Date/Time, you are presented with a series of “Date/time Config.” screens starting with “NTP” and ending with “Time,” as shown in the following figure.

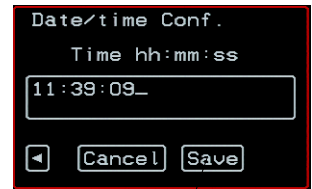
First screen



Next button



Final screen



Final Save button

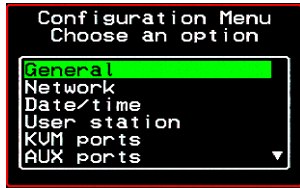
**Figure 7-2:** First, Middle, and Last Screens in Configuration Series

As illustrated, all the configuration screens except the final screen have a right arrow at the bottom right that you can select to go to the next screen. Clicking “Save” on any one of the screens saves the changes made to that point. You can wait until you get to the final screen in a series before saving changes. Clicking “Save” on the final screen saves any change you have made and takes you back to the Configuration menu.

See “Navigating the OSD” on page 346, if needed, for instructions on how to use the Tab key and other keys to move around the screens in the OSD.

# General Configuration Screens [OSD]

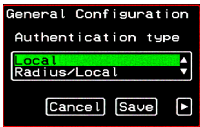
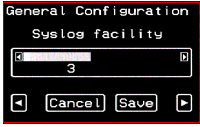
You can select the General option on the OSD Configuration Menu to configure several general features of the KVM/net Plus, which are introduced under “General” on page 352.



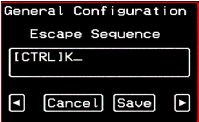
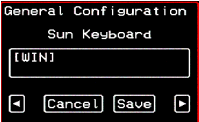
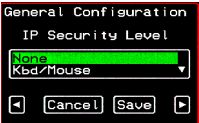
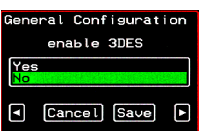
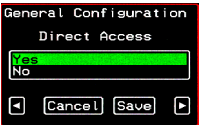
Selecting Configure>General from the OSD Main Menu brings up the Authentication type screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-5 gives a brief description of the sequence of General configuration screens.

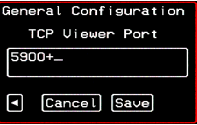
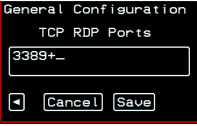
**Table 7-5:** General Configuration Screens [OSD]

Screen	Description
<b>Authentication Type</b> 	The authentication type applies to <i>direct KVM port logins from the KVM/net Plus login screen</i> : None, Local, Radius, TacacsPlus, Kerberos, LDAP, RadiusDownLocal, TacplusDownLocal, KerberosDownLocal, LdapDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal, and Windows NT/2K/2K3. Direct logins to KVM ports must also be enabled. (See “Direct Access” on page 356.) You also must ensure that an authentication server is specified for the type of method you select. See “Authentication Screens” on page 405.
<b>Syslog Facility</b> 	The syslog facility number that is used by the administrator of the syslog server to identify messages generated by devices connected to the KVM ports. Obtain the facility number to use for the KVM/net Plus from the syslog server’s administrator. Values are from 0 through 7. See “Syslog Servers” on page 52 for examples of using facility numbers as needed. In addition, the IP address of the syslog server must be configured, as described under “Syslog Screens” on page 401.

**Table 7-5: General Configuration Screens [OSD] (Continued)**

Screen	Description
<p><b>Escape Sequence</b></p> 	<p>The escape sequence for AlterPath Viewer hot keys [Default: Ctrl+k, shown as [CTRL]K in the screen]. See “Redefining KVM Connection Hot Keys” on page 40 for more details.</p>
<p><b>Sun Keyboard</b></p> 	<p>The escape key for Sun hot keys. Default = the Windows [WIN] key, which is the key with the Windows logo on it. Other options are: [CTRL], [SHIFT], and [ALT]. See “Redefining Sun Keyboard Equivalent Hot Keys” on page 40 for more details.</p>
<p><b>IP Security Level</b></p> 	<p>The level of encryption: “None,” “encrypt keyboard and mouse data,” or “encrypt data from the keyboard, video, and mouse.”</p>
<p><b>3DES</b></p> 	<p>Disables or enables 3DES encryption.</p>
<p><b>Direct Access</b></p> 	<p>Enables or disables direct access to KVM ports from the Web Manager login screen.</p>

**Table 7-5:** General Configuration Screens [OSD] (Continued)

Screen	Description
<p><b>TCP Port Viewer</b></p> 	<p>Allows you to assign an alternate TCP Port number or numbers for the AlterPath Viewer to use [Default, 5900+]. Use the plus sign (+) to increment the port number by 1 for each additional AlterPath Viewer. For example: 5903+ means that the first AlterPath Viewer uses port 5903 and the second uses port 5904. Use the hyphen (-) to indicate a range of addresses, for example, 5903-5907. Use the comma (,) to separate two TCP port addresses, for example, 5901,5903. Combine commas and hyphens, as desired, for example: 1901,5903-5905,5907. <b>Note:</b> Do not use reserved port numbers 1 through 1024.</p>
<p><b>TCP RDP Ports</b></p> 	<p>Specify the TCP ports or a range of TCP ports to be used for RDP (in-band) server connections. You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the KVM/net Plus. For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”. You can request valid TCP ports from your network administrator.</p>

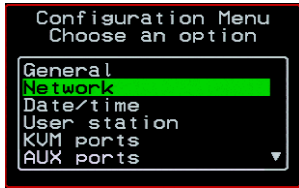
---

**Note:** The Save button on every screen saves configuration changes into the configuration files. To permanently save the configuration changes, you must select Save/Load Conf. from the Configuration Menu.

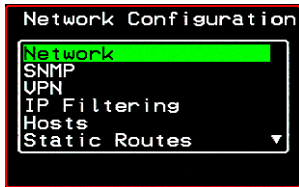
---

## Network Configuration Menu Options [OSD]

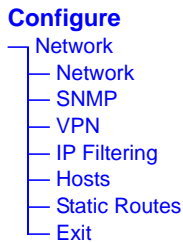
You can select the Network option on the OSD Main Menu to configure network-related services for the KVM/net Plus.



Selecting Network under Configuration brings up the Network Configuration Menu. The Network Configuration Menu provides a number of options, as shown in the following screen.



Not all the options are visible. The following diagram lists the names of all the configuration options accessed from the Configure>Network menu.





The configuration screen series for each of the options under Configure>Network are listed and described in the following sections:

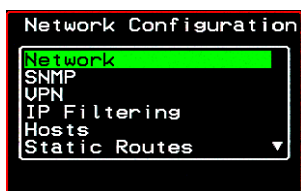
---

Network Configuration Screens [OSD]	Page 359
SNMP Configuration Screens [OSD]	Page 362
VPN Configuration Screens [OSD]	Page 366
IP Filtering Configuration Screens	Page 370
Hosts Configuration Screens [OSD]	Page 377
Static Routes Configuration Screens	Page 378

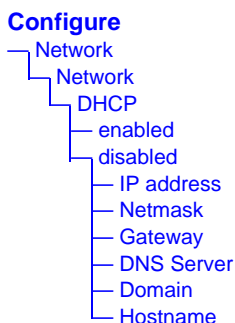
---

## ***Network Configuration Screens [OSD]***

You can select the Network option from the Network Configuration menu to configure DHCP or configure a fixed IP address and other basic network parameters.



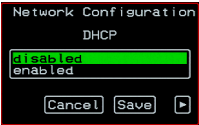
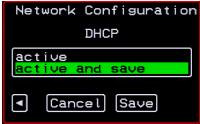
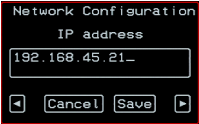
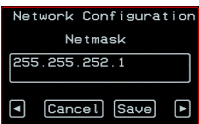
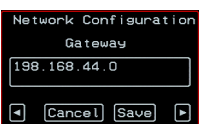
The following diagram lists the names of the configuration screens accessed under Configure>Network>Network.



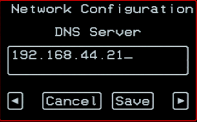

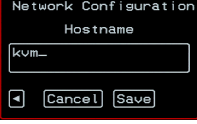
Selecting Configure>Network>Network from the OSD Main Menu brings up the DHCP screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-6 gives a description of all the related configuration screens.

**Table 7-6:** Network Configuration Screens [OSD]

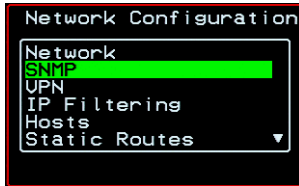
Screen	Description
<p><b>DHCP</b></p> 	<p>Enable or disable DHCP. When you select “enabled,” the screen shown in the following figure appears.</p>  <p>“active” saves the changes to the configuration files. “active and save” overwrites the backup configuration files and makes the changes permanent. Either choice brings you back to the Network Configuration menu.</p> <p>When “disabled” is selected, the IP address, Netmask, Gateway, DNS Server, Domain, and Hostname forms appear in the sequence shown in the following rows.</p>
<p><b>IP Address</b></p> 	<p>The IP address of the KVM/net Plus.</p>
<p><b>Netmask</b></p> 	<p>The netmask for the subnet (if applicable) in the form <i>NNN.NNN.NNN.N</i> (for example: 255 . 255 . 252 . 0).</p>
<p><b>Gateway</b></p> 	<p>The IP address for the gateway (if applicable).</p>

**Table 7-6: Network Configuration Screens [OSD] (Continued)**

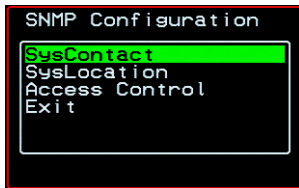
Screen	Description
<b>DNS Server</b> 	The IP address for the DNS server.
<b>Domain</b> 	The domain name.
<b>Hostname</b> 	The hostname for the KVM/net Plus.

## SNMP Configuration Screens [OSD]

You can select the SNMP option from the Network Configuration menu to configure SNMP.



Selecting SNMP under Configuration>Network brings up the SNMP Configuration Menu. The SNMP Configuration Menu provides a number of options, as shown in the following screen.



The following diagram lists the names of all the configuration screen series accessed from the Configure>Network>SNMP Configuration menu.

The following diagram lists the names of the configuration screens accessed under Configure>Network>SNMP.

## Configure

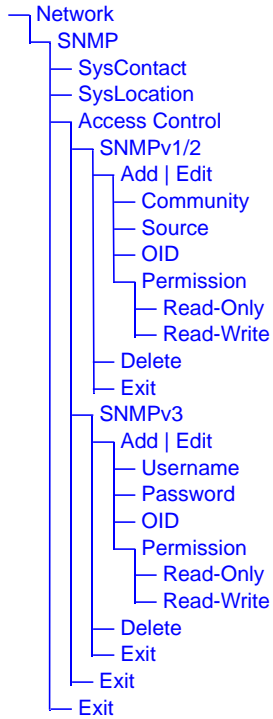
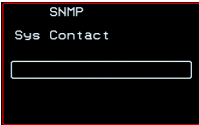
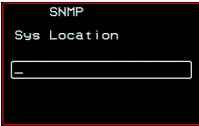
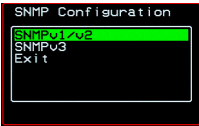
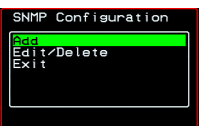

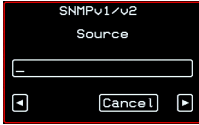
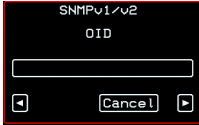
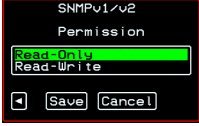




Table 7-7 gives a brief description of all the SNMP configuration screens.

**Table 7-7: SNMP Configuration Screens [OSD]**

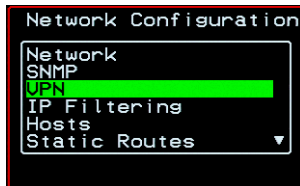
Screen	Description
<p><b>SysContact</b></p> 	<p>The email address for the KVM/net Plus administrator, for example: <code>kvm_admin@cyclades.com</code>.</p>
<p><b>SysLocation</b></p> 	<p>The physical location of the KVM/net Plus.</p>
<p><b>Access Control</b></p> 	<p>Choices are SNMP v1/2 or SNMP v3.</p>
<p><b>SNMP Configuration</b></p> 	<p>Appears when either SNMP v1/2 or SNMP v3 is selected. Choices are “Add,” “Edit/Delete,” or “Exit.”</p>
<p><b>SNMPv1/v2 Community</b></p> 	<p>The community name is sent in every SNMP communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under “Permission”: either read only or read write. The most common community is “public” and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the KVM/net Plus.</p>

**Table 7-7: SNMP Configuration Screens [OSD] (Continued)**

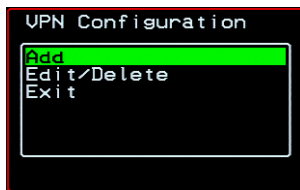
Screen	Description
<p><b>SNMPv1/v2 Source</b></p> 	<p>The source IP address or range of IP addresses.</p>
<p><b>SNMPv1/v2 or v3 OID</b></p> 	<p>Object Identifier. Each managed object has a unique identifier.</p>
<p><b>SNMPv1/v2 or v3 Permission</b></p> 	<p>Choices are “Read-Only” and “Read-Write.”            Read Only - Read-only access to the entire MIB (Management Information Base) except for SNMP configuration objects.            Read/Write - Read-write access to the entire MIB except for SNMP configuration objects.</p>
<p><b>SNMPv3 Username</b></p> 	<p>User name.</p>
<p><b>SNMPv3 Password</b></p> 	<p>Password.</p>

## ***VPN Configuration Screens [OSD]***

You can select the VPN option from the Network Configuration menu to configure VPN.



Selecting VPN under Configuration>Network brings up the VPN Configuration Menu. The VPN Configuration Menu provides the options shown in the following screen.



You can use these options to add a VPN connection or to edit or delete a previously configured VPN connection. See “VPN” on page 238 for details.

The following diagram lists the names of the configuration screens accessed from the Add and Edit/Delete options on the Configure>Network>VPN Configuration menu.



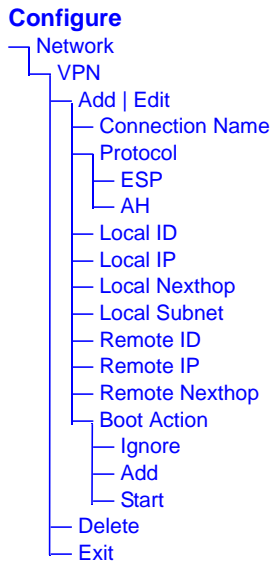
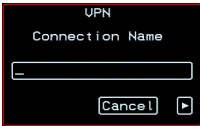
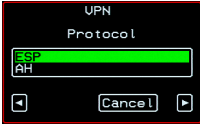
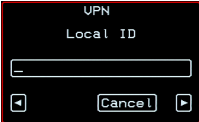
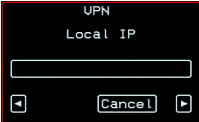
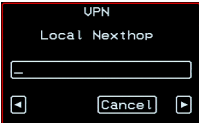
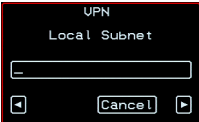
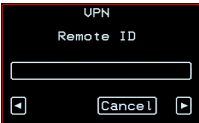
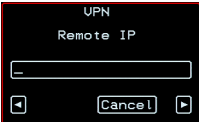


Table 7-8 gives a brief description of the VPN configuration screens series under Add and Edit.

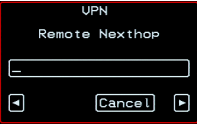
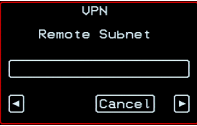
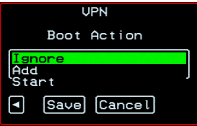
**Table 7-8:** VPN Configuration Screens [OSD]

Screen	Description
<p><b>Connection Name</b></p> 	Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN”
<p><b>Protocol</b></p> 	The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header)

**Table 7-8:** VPN Configuration Screens [OSD] (Continued)

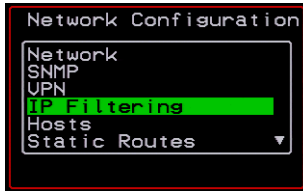
Screen	Description
<p><b>Local ID</b></p> 	<p>The hostname of the KVM/net Plus, referred to as the “local” host.</p>
<p><b>Local IP</b></p> 	<p>The IP address of the KVM/net Plus.</p>
<p><b>Local NextHop</b></p> 	<p>The router through which the KVM/net Plus sends packets to the host on the other side.</p>
<p><b>Local Subnet</b></p> 	<p>The netmask of the subnetwork where the KVM/net Plus resides, if applicable.</p>
<p><b>Remote ID</b></p> 	<p>The hostname of the remote host or security gateway</p>
<p><b>Remote IP</b></p> 	<p>The IP address of the remote host or security gateway.</p>

**Table 7-8: VPN Configuration Screens [OSD] (Continued)**

Screen	Description
<p><b>Remote NextHop</b></p> 	<p>The IP address of the router through which the host on the other side sends packets to the KVM/net Plus.</p>
<p><b>Remote Subnet</b></p> 	<p>The netmask of the subnetwork where the remote host or security gateway resides, if applicable.</p>
<p><b>Boot Action</b></p> 	<p>Choices are “Ignore,” “Add,” and “Start.” “Ignore” means that VPN connection is ignored. “Add” means to wait for connections at startup. “Start” means to make the connection</p>

## ***IP Filtering Configuration Screens***

You can select the IP Filtering option from the Network Configuration menu to configure the KVM/net Plus to filter packets like a firewall.

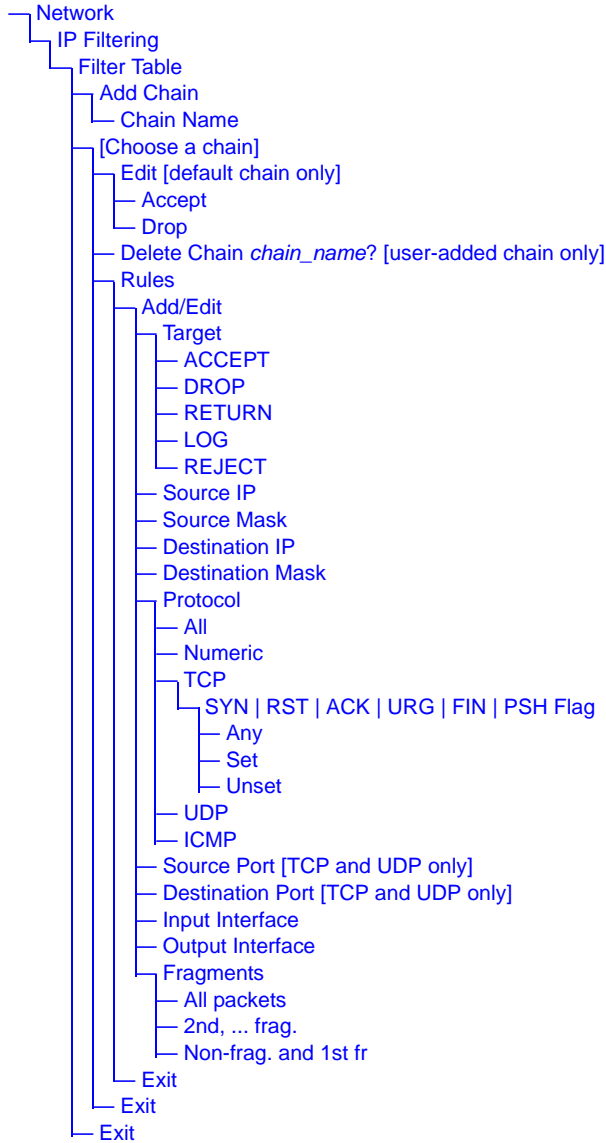


Selecting IP Filtering under Configuration>Network brings up the “Filter Table.” The “Filter Table” lists the default chains along with any administratively configured chains, the “Add Chain,” and the “Exit” options, as shown in the following screen.




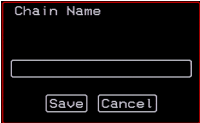
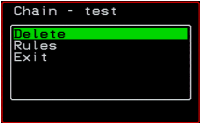

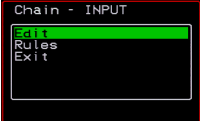
You can use this menu to create chains and set up rules for the new chains or you can edit or delete a previously configured chain. The following diagram lists the names of the configuration screens accessed under Configure>Network>IP Filtering.

## Configure

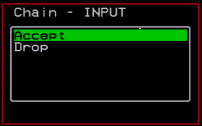

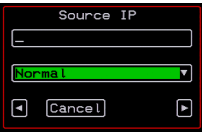
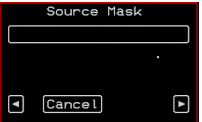


The following table shows the IP filtering screens.

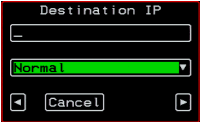
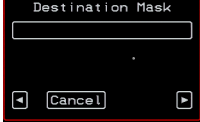
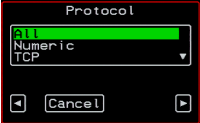
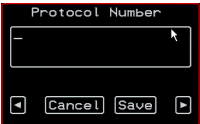

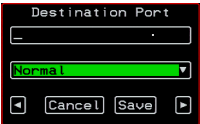
**Table 7-9: IP Filtering Configuration Screens [OSD]**

Screen	Description
<p><b>Filter Table</b></p> 	<p>Lists the default chains along with any administratively configured chains, the “Add Chain,” and the “Exit” options.</p>
<p><b>Chain Name</b></p> 	<p>Only appears when “Add Chain” is selected. Entering the name of the chain adds the new chain’s name to the “Filter Table,” where you need to select the name of the new chain and define rules for the chain.</p>
<p><b>Chain - <i>chain_name</i></b></p> 	<p>Appears when a user-added chain is selected from the “Filter Table.” The choices are “Delete,” “Rules,” “Exit.”</p>
<p><b>Delete Chain <i>chain_name</i>?</b></p> 	<p>Appears when a user-added chain is selected and the Delete option is chosen from the “Chain - <i>chain_name</i>” menu.</p>
<p><b>Chain - <i>CHAIN_NAME</i></b></p> 	<p>Appears when a default chain is selected from the “Filter Table.” The choices are “Edit,” “Rules,” and “Exit.”</p>

**Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)**







Screen	Description
<p data-bbox="113 265 164 291"><b>Edit</b></p> 	<p data-bbox="404 265 1134 361">Appears when a default chain is selected and the Edit option is chosen from the Chain - <i>Chain_name</i> menu. Choices are “Accept” or “Drop.”</p>
<p data-bbox="113 743 190 769"><b>Target</b></p> 	<p data-bbox="404 475 1134 708">The following screens define the rules for packet filtering. The packet is filtered for the characteristics defined in the rule, for example, a specific IP header, input and output interfaces, TCP flags or protocol. The target action is performed on all packets that have the characteristic. If “Inverted” is selected for a characteristic, the target action is performed on all packets that do not have the characteristic.</p> <p data-bbox="404 743 1134 907">Appears when a user-added chain is selected. Choices specify the target action to take when a packet’s characteristics match the rule, or, if “Inverted” is selected, if the packets do not match the rule. Choices are: “ACCEPT,” “DROP,” “RETURN,” “LOG,” and “REJECT.”</p>
<p data-bbox="113 951 233 977"><b>Source IP</b></p> 	<p data-bbox="404 951 958 977">The IP address of the source of an input packet.</p>
<p data-bbox="113 1159 275 1185"><b>Source Mask</b></p> 	<p data-bbox="404 1159 1035 1220">The netmask of the subnetwork where an input packet originates.</p>

**Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)**

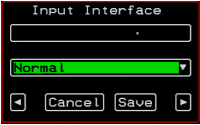
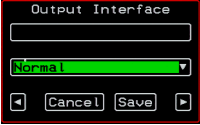
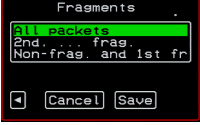
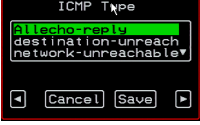
Screen	Description
<p><b>Destination IP</b></p> 	<p>The IP address of an output packet's destination.</p>
<p><b>Destination Mask</b></p> 	<p>The netmask of the subnet to which an output packet is going.</p>
<p><b>Protocol</b></p> 	<p>Choices are "All," "Numeric," "TCP," "UDP," "ICMP."</p>
<p><b>Protocol Number</b></p> 	<p>Appears only if "Numeric" is selected from the "Protocol" menu.</p>
<p><b>Source Port</b></p> 	<p>Appears only if "TCP" or "UDP" are selected from the "Protocol" menu. The source port number.</p>
<p><b>Destination Port</b></p> 	<p>Appears only if "TCP" or "UDP" are selected from the "Protocol" menu. The destination port number.</p>



**Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)**

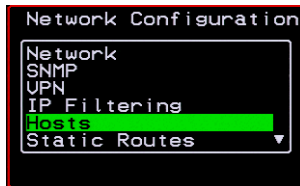
Screen	Description
<b>SYN Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
<b>RST Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
<b>ACK Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
<b>URG Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
<b>FIN Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”
<b>PSH Flag</b> 	Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”

**Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)**

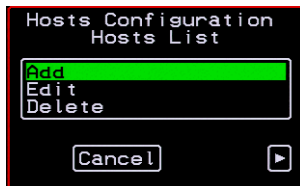
Screen	Description
<b>Input Interface</b> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>
<b>Output Interface</b> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>
<b>Fragments</b> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>
<b>ICMP Type</b> 	<p>Appears only if ICMP is selected from the “Protocol” menu. Choices are:</p> <ul style="list-style-type: none"> <li>• all</li> <li>• echo-reply</li> <li>• destination-unreachable</li> <li>• network-unreachable</li> <li>• host-unreachable</li> <li>• port-unreachable</li> <li>• fragmentation needed</li> <li>• source-route-failed</li> <li>• network-unknown</li> <li>• host-unknown</li> <li>• network-prohibited</li> <li>• host-prohibited</li> </ul>

## Hosts Configuration Screens [OSD]

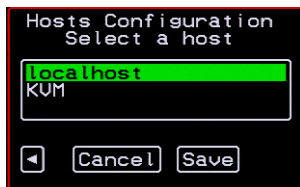
You can select the Hosts option from the Network Configuration menu to configure hosts.



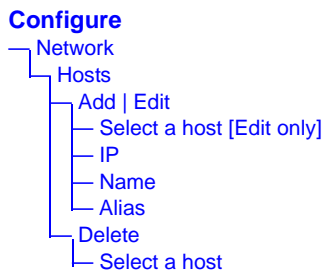
Selecting Hosts under Configuration>Network brings up the “Hosts List” action menu, as shown in the following screen.



You can select the options on this menu to add, edit, or delete host entries. Selecting “Edit” or “Delete Entry” brings up the following “Select a host” screen.

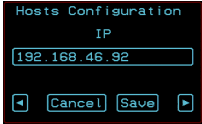
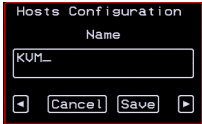
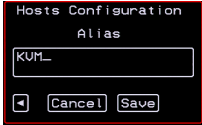


The following diagram lists the names of the configuration screens accessed under Configure>Network>Hosts.



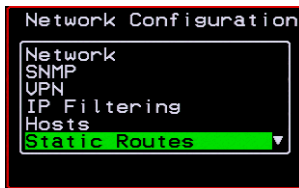
The following table shows the screens for the Add and Edit options.

**Table 7-10: Hosts Configuration Screens [OSD]**

Screen	Description
<p><b>IP</b></p> 	IP address of the host
<p><b>Name</b></p> 	Hostname of the host
<p><b>Alias</b></p> 	Optional alias of the host

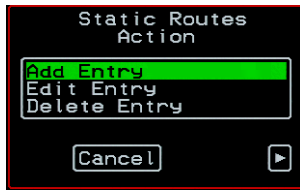
### **Static Routes Configuration Screens**

You can select the Static Routes option from the Network Configuration menu to configure static routes.

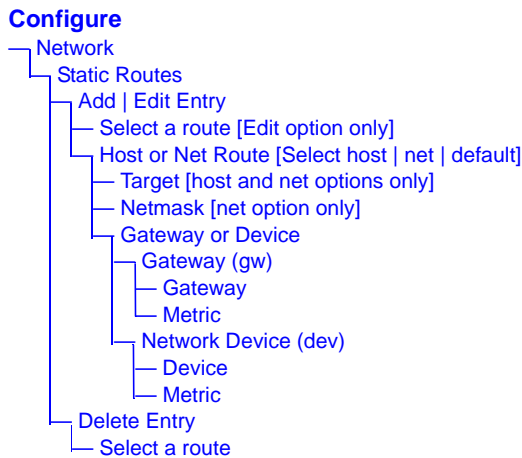


If judiciously used, static routes can sometimes reduce routing problems and routing traffic overhead. If injudiciously used, when a network fails, static routes can block packets that would otherwise be able to find alternate routes around the point of failure if dynamic-routing were in effect.

Selecting Static Routes under Configuration>Network brings up the Static Routes Action Menu, as shown in the following screen.



The following diagram lists the names of the configuration screens accessed under Configure>Network>Static Routes.

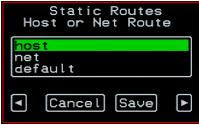
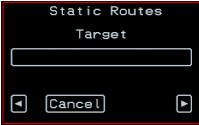
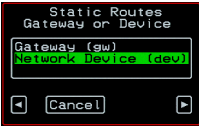




The following table shows the static routes screens that appear when you select one of the actions.


**Table 7-11:Static Routes Screens [OSD]**

Screen	Description
<p><b>Select a route</b></p>	<p>Appears only when the Edit and Delete options are selected. Choices are “default” and any previously configured static routes.</p>

**Table 7-11:Static Routes Screens [OSD] (Continued)**

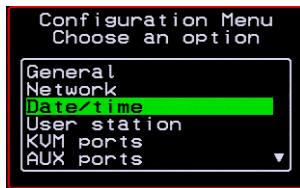
Screen	Description
<p><b>Host or Net Route</b></p> 	<p>Types of routes: “host,” “net,” or “default.” <b>Note:</b> A default route is used to direct packets that are addressed to networks not listed in the routing table.</p>
<p><b>Target</b></p> 	<p>IP address for the target host or network.</p>
<p><b>Netmask</b></p> 	<p>Appears only when “net” is selected from the “Host or Net Route” screen. Netmask for the destination.</p>
<p><b>Gateway or Device</b></p> 	<p>Two options are: “Gateway (gw)” or “Network Device (dev).”</p>
<p><b>Gateway</b></p> 	<p>Appears only when “Gateway (gw)” is selected from the “Gateway or Device” menu. Gateway IP address.</p>
<p><b>Device</b></p> 	<p>Appears only when “Network Device” is selected from the “Gateway or Device” menu. Device address (such as eth0).</p>

**Table 7-11:Static Routes Screens [OSD] (Continued)**

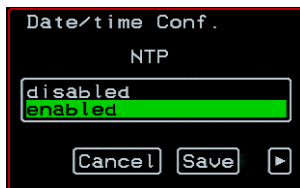
Screen	Description
<b>Metric</b> 	The number of hops to the destination.

## Date/time Configuration Screens

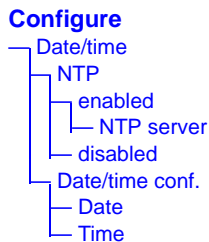
You can select the Date/time option from the OSD Configuration menu to either configure an NTP server or manually set the date and time.



Selecting Date/time under Configuration>Network brings up the NTP menu, as shown in the following screen.



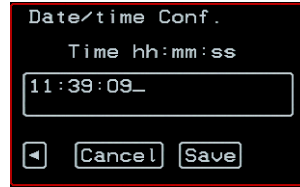
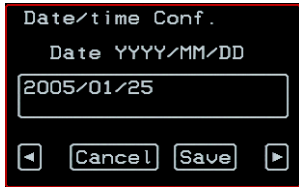
The following diagram lists the names of the configuration options accessed from the Configure>Date/time menu.



If NTP is enabled, the following screen appears for entering the IP address of the NTP server.

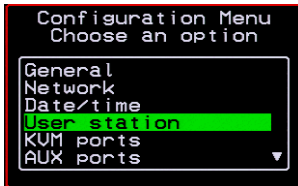


If NTP is disabled, the following series of two screens appears to allow you to enter the date and time manually.



## User Station Screens

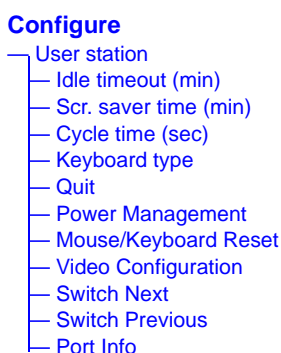
You can select the User Station option from the OSD Configuration menu to redefine the parameters that apply to a local user session (when a user is accessing the OSD through the User 1 or User 2 port).





The changes apply only to the currently accessed local station. For example, if an administrator configures these settings while connected to the User 2 port, these settings will be changed for all users who log in to the User 2 port, but the User 1 port setting will remain unchanged.

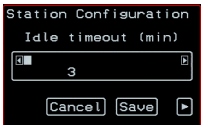
The following diagram lists the configuration screens accessed through the Configure>User station option. All the screens that appear after the “Keyboard type” screen are for optionally redefining the command key portion of the KVM connection hot keys: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Configuration,” “Switch Next,” “Switch Previous,” and “Port Info.” See “Redefining Keyboard Shortcuts (Hot Keys)” on page 40 for details, if needed.



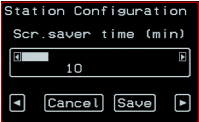
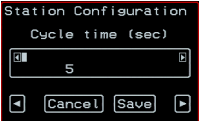
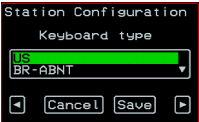
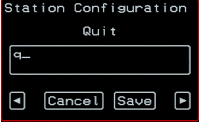
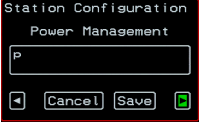
**Figure 7-3:** User Station Configuration Screens

The following table shows the user station configuration screens.

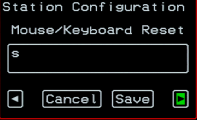
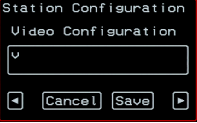
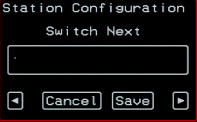
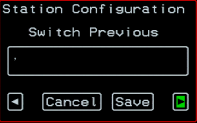
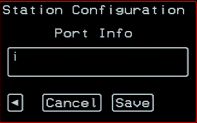
**Table 7-12:**User Station Configuration Screens

Screen	Description
<b>Idle timeout</b> 	The period of inactivity before the user is logged out from the OSD. The default is 3 minutes.

**Table 7-12:**User Station Configuration Screens (Continued)

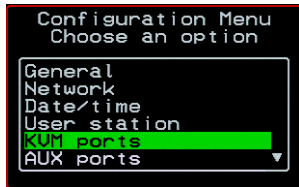
Screen	Description
<p><b>Scr. saver timeout</b></p> 	<p>The period of inactivity before the screen saver starts. The default is 10 minutes.</p>
<p><b>Cycling</b></p> 	<p>The number of seconds each server is viewed while the user is cycling from one port to another. Default = 5 seconds. See “To Initiate Cycle by Server” on page 326 for instructions on how to cycle through the servers.</p>
<p><b>Keyboard Type</b></p> 	<p>The type of keyboard connected to the User 1 or User 2 management port of the KVM/net Plus.</p> <ul style="list-style-type: none"> <li>• US [Default]</li> <li>• BR-ABNT</li> <li>• BR-ABNT2</li> <li>• Japanese</li> <li>• German</li> <li>• Italian</li> <li>• French</li> <li>• Spanish</li> </ul>
<p><b>Quit</b></p> 	<p>Redefine the command key for the KVM connection quit hot key.</p>
<p><b>Power Management</b></p> 	<p>Redefine the command key portion of the KVM connection power management hot key.</p>

**Table 7-12:User Station Configuration Screens (Continued)**

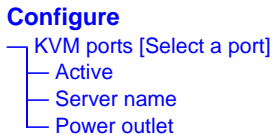
Screen	Description
<p><b>Mouse/Keyboard</b></p>  A screenshot of the 'Station Configuration' dialog box, specifically the 'Mouse/Keyboard Reset' tab. It features a text input field containing the letter 's'. Below the field are three buttons: a left-pointing arrow, 'Cancel', and 'Save', followed by a green checkmark icon.	Redefine the command key portion of the KVM connection mouse/keyboard reset hot key.
<p><b>Video</b></p>  A screenshot of the 'Station Configuration' dialog box, specifically the 'Video Configuration' tab. It features a text input field containing the letter 'v'. Below the field are three buttons: a left-pointing arrow, 'Cancel', and 'Save', followed by a right-pointing arrow.	Redefine the command key portion of the KVM connection video brightness and contrast hot key.
<p><b>Switch Next</b></p>  A screenshot of the 'Station Configuration' dialog box, specifically the 'Switch Next' tab. It features a text input field containing the letter 'n'. Below the field are three buttons: a left-pointing arrow, 'Cancel', and 'Save', followed by a right-pointing arrow.	Redefine the command key portion of the KVM connection switch next hot key.
<p><b>Switch Previous</b></p>  A screenshot of the 'Station Configuration' dialog box, specifically the 'Switch Previous' tab. It features a text input field containing the letter 'p'. Below the field are three buttons: a left-pointing arrow, 'Cancel', and 'Save', followed by a green checkmark icon.	Redefine the command key portion of the KVM connection switch previous hot key.
<p><b>Port Info</b></p>  A screenshot of the 'Station Configuration' dialog box, specifically the 'Port Info' tab. It features a text input field containing the letter 'i'. Below the field are three buttons: a left-pointing arrow, 'Cancel', and 'Save'.	Redefine the command key portion of the KVM connection port info hot key.

## KVM Ports Screens

You can select the KVM Ports option on the OSD Configuration Menu to configure KVM ports.



The following diagram lists the configuration screens accessed through the Configure>KVM ports option.




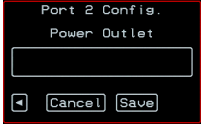
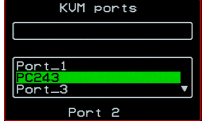
**Figure 7-4:** KVM Ports Configuration Screens

The following table shows the KVM port configuration screens.

**Table 7-13:** KVM Port Configuration Screens

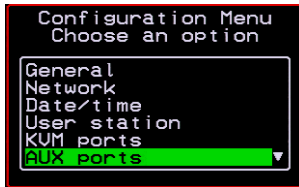
Screen	Description
<p><b>KVM ports</b></p> <p>A screenshot of a terminal window titled "KVM ports". It shows a text input field containing "Port_2". Below it is a scrollable list box containing "Port_1", "Port_2" (highlighted in green), and "Port_3". At the bottom, the text "Port 2" is displayed.</p>	Lists all KVM ports by their default names or administratively defined aliases.
<p><b>Active</b></p> <p>A screenshot of a terminal window titled "Port 2 Config.". It shows the word "Active" above a text input field containing "Yes" (highlighted in green). Below the field are "Cancel" and "Save" buttons, and a right-pointing arrow button.</p>	Choices are “Yes” and “No” to activate or deactivate the selected KVM port.

**Table 7-13:KVM Port Configuration Screens (Continued)**

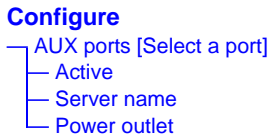
Screen	Description
<p><b>Server name</b></p> 	<p>Allows you to assign a descriptive alias, such as the name of the server to which the selected KVM port is connected. Only alpha-numeric characters, hyphens (-), and underscores (_) are accepted. The new alias replaces the default port name in the list of ports as shown here:</p>
<p><b>Power Outlet</b></p> 	 <p>Allows you to enter one or more numbers that identify power outlet or outlets into which the server that is connected to this KVM port is plugged. The outlet number(s) format must be: <i>A:N</i>, where <i>A</i> is the number of the AUX port to which the IPDU is connected (either 1 or 2) and <i>N</i> is the number of the outlet. When IPDUs are daisy-chained, the outlets on the second and subsequent IPDUs are numbered sequentially. For example, if two eight-outlet AlterPath PMs are daisy-chained, you would use the number 12 to specify the fourth outlet on the second PM in the chain. You can enter up to twenty characters, so you can specify up to four outlets. See “Controlling Power While Connected to KVM Ports” on page 45 for details. Also see “To Power On, Power Off, or Reboot the Connected Server” on page 329, if needed.</p>

## AUX Ports Screens

You can select the AUX Ports option on the OSD Configuration Menu to configure the AUX ports.



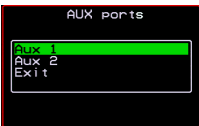
The following diagram lists the configuration screens accessed through the Configure>AUX ports option.



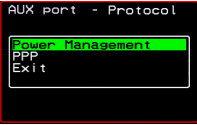


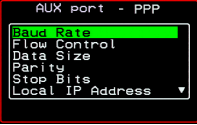
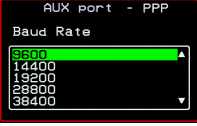
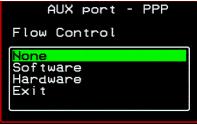
**Figure 7-5:** AUX Ports Configuration Screens

The following table shows the AUX ports configuration screens.

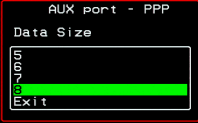
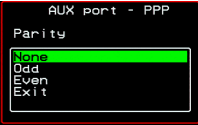
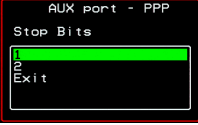
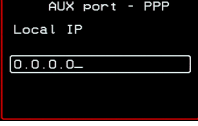
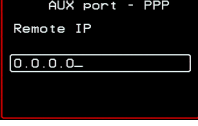
**Table 7-14:** KVM Ports Configuration Screens

Screen	Description
<b>AUX ports</b> 	Lists the AUX 1 and AUX 2 ports.

**Table 7-14:KVM Ports Configuration Screens (Continued)**

Screen	Description
<b>AUX ports - Protocol</b> 	<p>Choices are “Power Management” and “PPP.”                      If you select Power Management, the following confirmation screen displays:</p>
	
	<p>If you select PPP, the following connection configuration menu displays:</p>
	
<b>AUX port - PPP</b> 	<p>Appears when PPP is selected from the AUX ports - Protocol screen. Allows you to configure the connection settings for any PPP connection being made through an external modem connected to the AUX port.</p>
<b>AUX port - PPP Baud Rate</b> 	<p>The port speed.</p>
<b>AUX port - PPP Flow Control</b> 	<p>Gateway or interface address used for the route.</p>

**Table 7-14:KVM Ports Configuration Screens (Continued)**

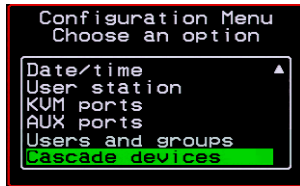
Screen	Description
<p><b>AUX port - PPP Data Size</b></p> 	<p>The number of data bits.</p>
<p><b>AUX port - PPP Parity</b></p> 	<p>None, even, or odd.</p>
<p><b>AUX port - PPP Stop Bits</b></p> 	<p>The number of stop bits.</p>
<p><b>AUX port - PPP Local IP</b></p> 	
<p><b>AUX port - PPP Remote IP</b></p> 	



# Cascade Devices

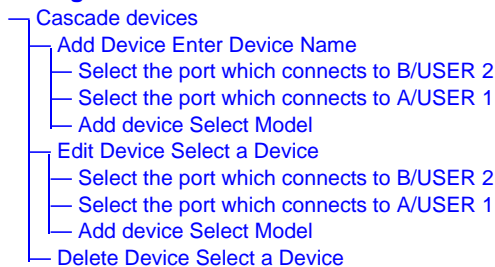
You can select the Cascade Devices option on the OSD Configuration Menu to perform the following tasks:

- Add a secondary KVM unit to be cascaded from the master KVM/net Plus.
- Edit the configuration of a cascaded device.
- Delete the configuration of a cascaded device.



The Cascade Devices option of the Configuration Menu allows you to configure a secondary KVM unit to be cascaded to the KVM/net Plus to increase the number of supportable ports. The secondary device may be a KVM/net Plus, a KVM/net, a KVM, or a KVM Expander. The following diagram lists the configuration screens accessed through the Configure>AUX ports option.

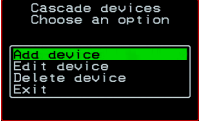
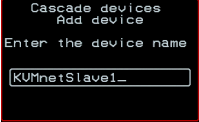
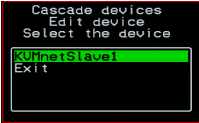
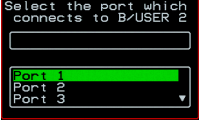
## Configure



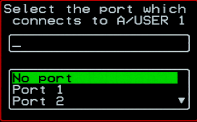
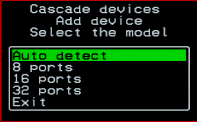
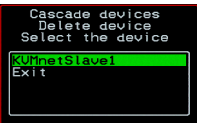
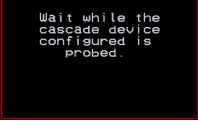

**Figure 7-6:** Cascade Devices Configuration Screens

The following table shows the Cascade Devices configuration screens.

**Table 7-15:**Cascade Devices Configuration Screens

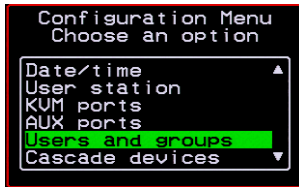
Screen	Description
<p><b>Cascade device Choose an option</b></p> 	<p>Options include Add device, Edit device, and Delete device.</p>
<p><b>Cascade Device Add Device Enter the device name</b></p> 	<p>Appears when Add device is selected from the “Cascade device Choose an option” screen. Enter the name of the new cascaded KVM unit.</p>
<p><b>Cascade Device Edit Device Select the device</b></p> 	<p>Appears when Edit device is selected from the “Cascade device Choose an option” screen. Select the name of a previously added cascaded KVM unit.</p>
<p><b>Select the port which connects to B/USER 2</b></p> 	<p>Enter the port number of the master KVM/net Plus that is connected to the User 2 port of the secondary KVM device or the B port on the Expander. <b>Note:</b> See “Connecting Cascaded KVM Units to the Primary KVM/net Plus” on page 126 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net Plus.</p>

**Table 7-15: Cascade Devices Configuration Screens (Continued)**

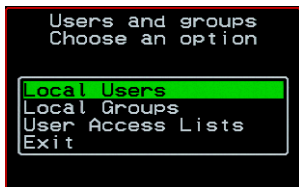
Screen	Description
<p><b>Select the port which connects to A/USER 1</b></p> 	<p>Enter the secondary KVM port that is connected to the User 1 port of the primary KVM/net Plus or the User A port on the Expander.</p>
<p><b>Cascade device Add device Select Model</b></p> 	<p>Select the number of ports on the cascaded KVM unit or select Auto detect and press &lt;Enter&gt;. Selecting Auto detect automatically detects the number of ports on the cascaded KVM unit. The unit must be already connected in order for the auto detect option to work. During auto detection, the following message appears.</p>
<p><b>Cascade Device Delete Device Select the device</b></p> 	<p>Appears when Delete device is selected from the “Cascade device Choose an option” screen. The following confirmation screen appears once a cascaded device is selected.</p>
	

## Users and Groups Screens

You can choose the “Users and groups” option from the OSD Configuration menu to configure users, groups, and KVM port permissions.

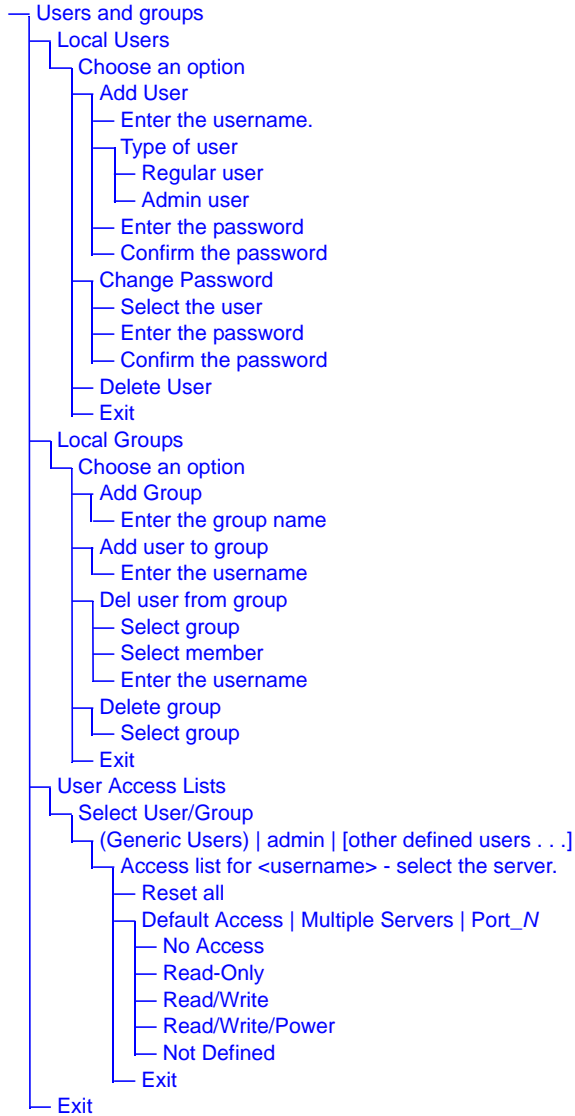


When you select “Users and Groups,” the “Choose an option” screen appears, as shown in the following screen example. The “Local Users” option is for configuring users; the “Local Groups” option is for configuring groups, and the “User Access Lists” option is for configuring users’ and groups’ access to KVM ports.



The following diagram lists the configuration screens accessed through the Configure>Users and Groups options:

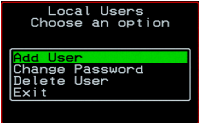
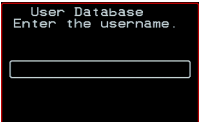
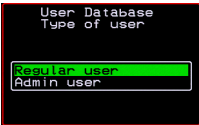
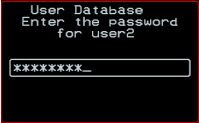
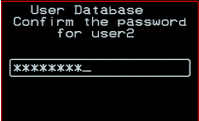
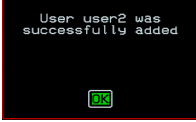
## Configure





**Figure 7-7:** Users and Groups Configuration Screens

The following table shows the configuration screens that appear when the “Local Users” option is selected from the Users and Groups menu under Configure in the OSD.

**Table 7-16:**Local Users Configuration Screens

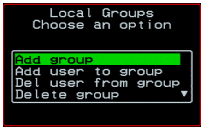
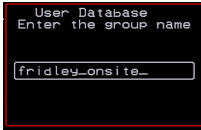
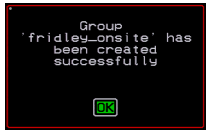
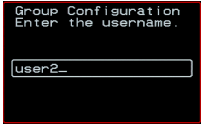
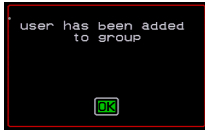
Screen	Description
<p><b>Choose an option</b></p> 	<p>Options are: “Add User,” “Change Password,” “Delete User,” or “Exit.”</p>
<p><b>User Database Enter the username</b></p> 	<p>Appears only when “Add User” is selected.</p>
<p><b>Type of user</b></p> 	<p>Appears only when “Add User” is selected.</p>
<p><b>Enter the password</b></p> 	<p>Appears only when “Add User” or “Change Password” are selected. <b>Note:</b> Passwords are case sensitive. When the password is successfully confirmed, the following dialog box appears.</p>
<p><b>Confirm the password</b></p> 	

**Table 7-16:Local Users Configuration Screens (Continued)**

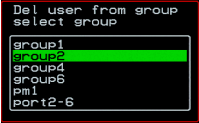

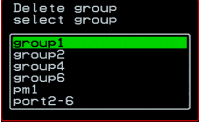

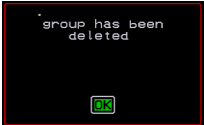
Screen	Description
<p><b>Select the user</b></p> 	<p>Appears only when “Change Password” or “Delete User” are selected. When “Delete User” and then a username are selected, a confirmation screen like the following appears:</p> 

The following table shows the configuration screens that appear when the “Local Groups” option is selected from the Users and Groups menu under Configure in the OSD.

**Table 7-17:Local Groups Configuration Screens**

Screen	Description
<p><b>Choose an option</b></p> 	<p>Options are “Add group,” “Add user to group,” “Del. user from group,” “Delete group,” and Exit</p>
<p><b>Enter the group name</b></p> 	<p>When “Add group” is selected. After the group name is entered, a confirmation screen like the following appears.</p> 
<p><b>Enter the username</b></p> 	<p>When “Add user” or “Add user to group” are selected. To add multiple users, use a comma to separate each username. When the user is successfully added, the following confirmation screen appears.</p> 

**Table 7-17:**Local Groups Configuration Screens (Continued)

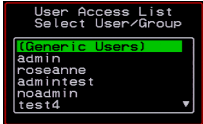
Screen	Description
<p><b>Delete user from group select group</b></p> 	<p>When “Del user from group” is selected.</p>
<p><b>Select member</b></p> 	<p>When “Del user from group” and a username are selected, the user is removed from the group, and the following confirmation screen appears:</p>
<p><b>Delete group select group</b></p> 	<p>When “Delete group” and a group name are selected, the following confirmation screen appears.</p>
	
	



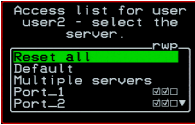

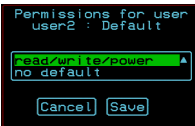
You can use the User Access Lists menu to view and change KVM port access permissions for the Default User and all administratively configured users and groups. See “Prerequisites for Accessing Servers With KVM Connections” on page 297 for details.

The following table shows the configuration screens related to setting KVM port access permissions when the “User Access List” option is selected from the Users and Groups menu under Configure in the OSD.

**Table 7-18: User Access List KVM Port Permissions Configuration Screens**

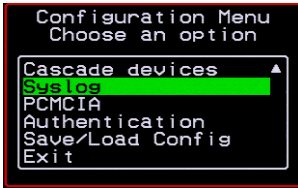
Screen	Description
<p data-bbox="113 552 345 579"><b>Select User/Group</b></p> 	<p data-bbox="430 552 1169 855">“[Generic Users],” “admin,” and any administratively defined users and groups are listed, along with the “Exit” option. The Generic Users’ permissions apply to all users except for “admin” and any users in the “admin” group. By default, the Generic Users’ default permission is “No Access,” and no KVM port permissions are defined. Therefore, by default, any regular users that may be added cannot access any KVM ports. The KVM/net Plus administrator can configure access to KVM ports for added regular users by:</p> <ul data-bbox="430 861 1169 1079" style="list-style-type: none"> <li data-bbox="430 861 1169 927">• By selecting “[Generic Users]” and modifying the permissions</li> <li data-bbox="430 947 1169 975">- OR -</li> <li data-bbox="430 982 1169 1079">• By configuring specific permissions for one or more individual users or groups (by selecting a single port or the “Multiple servers” option)</li> </ul>

**Table 7-18:**User Access List KVM Port Permissions Configuration Screens

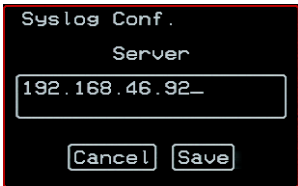
Screen	Description
<p><b>Access list for <i>username</i> - select the server</b></p>	<p>The access list includes the “Reset all,” “Default,” “Multiple servers,” and “Exit” options along with each individual KVM ports.</p> <p>The “Default” option defines access permissions for all KVM ports, which apply unless the user has specific access permissions for any KVM ports.</p> <p>For a new user, because “Default Access,” is not defined, and also because no permissions are specified for that user’s access to any specific port, the Generic Users’ permissions apply.</p> <p>A series of three checkboxes appear to the right of each entry that has specific permissions (as defined in the following row). If a port has “No Access” defined, the checkboxes are empty. The headings for the checkboxes are: <i>rwp</i> for read, write, and power, and the boxes are checked appropriately when any of these permissions are defined. For example, in the screen to the left, the <i>r</i> and <i>w</i> boxes are checked next to “Port_1” and “Port_2,” which indicates that the user has read-write access to these ports.</p> <p>If “Reset all” is selected, the following confirmation screen appears.</p>
	
<p><b>Permissions for <i>username</i> : <i>port_number</i> or for <i>username</i> : followed by another Access list option, such as “Default” or “Multiple Servers”</b></p>	<p>The permissions from this menu can be configured to be “Default” permissions for all ports, applied to Multiple Servers, or applied to a selected port.</p> <p>Permissions menu options are “No Access,” “Read-Only,” “Read Write,” “Read/Write/Power.” When “Default” is selected from the previous menu, the “Not Defined” menu option also appears. When any of the other options</p>
	

## Syslog Screens

You can select the Syslog option on the OSD Configuration Menu to specify the IP address for a syslog server.



Selecting the Configure>Syslog option brings up a Server screen for entering the IP address of a syslog server.

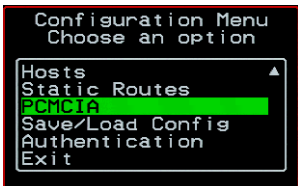


**Figure 7-8:** Syslog Configuration Server Screen

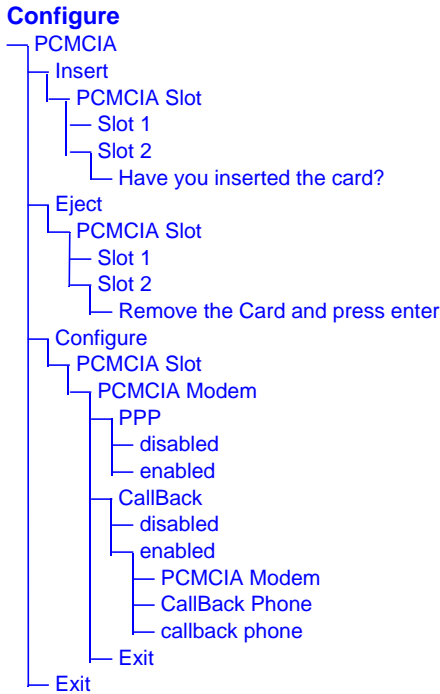
To complete the configuration of system logging, you must specify a facility number as shown in “Syslog Facility” on page 355.

## PCMCIA Screens

You can select the PCMCIA option on the OSD Configuration Menu to configure PCMCIA modem cards. For instructions on installing a PCMCIA card, see “Installing PCMCIA Cards in the Front Card Slots” on page 114.

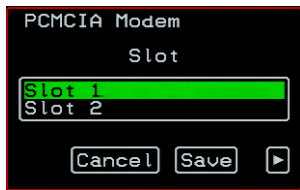


The following diagram lists the screens for configuring PCMCIA modem cards.

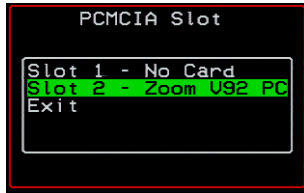


**Figure 7-9:** PCMCIA Configuration Screens

Selecting the Configure>PCMCIA option brings up a PCMCIA screen with the options shown in the following figure.



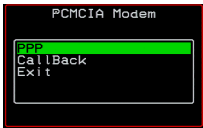

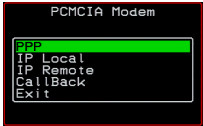
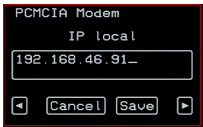
When configuring a new card, you select the “Insert” option, then select the Slot where the new card is inserted. A prompt asks if you have inserted the card. The PCMCIA Slot screen and the card insertion query screen are shown in the following figure.





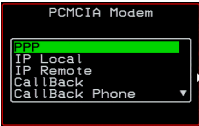
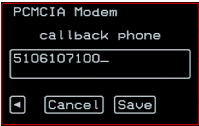
Selecting “Continue,” returns you to the PCMCIA menu, where you select the Configure option. The KVM/net Plus automatically detects the type of card and presents the appropriate series of configuration screens.

The following table shows the screens for a PCMCIA modem card.

**Table 7-19:**OSD Configuration Screens for a PCMCIA Modem Card

Screen	Description
<p><b>PCMCIA Modem</b></p> 	<p>Choices are “PPP,” “CallBack,” or “Exit.”</p>
<p><b>PPP</b></p> 	<p>Appears only when PPP is selected from the PCMCIA Modem menu. Options are “disabled” and “enabled.”</p>
<p><b>PCMCIA Modem</b></p> 	<p>Appears only when PPP is enabled. Choices are: “PPP” for disabling and enabling PPP, “IP Local,” “IP Remote,” “CallBack,” and Exit.</p> <p><b>Note:</b> By default, if no local IP is specified, the IP address of the KVM/net Plus is used. If no remote IP is specified, the IP address 10.0.0.1 is used. Use the default IP address unless you have a specific reason to use another.</p>
<p><b>IP Local</b></p> 	<p>Appears only when PPP is enabled and “IP Local” is selected.</p>

**Table 7-19:**OSD Configuration Screens for a PCMCIA Modem Card (Continued)

Screen	Description
<p><b>IP Remote</b></p> 	Appears only when PPP is enabled and “IP Remote” is selected.
<p><b>callback</b></p> 	Appears only when “Callback” is selected. Choices are: “disabled” and “enabled.”
<p><b>PCMCIA Modem</b></p> 	Appears when callback is enabled with an additional option: “Callback Phone.”
<p><b>callback phone</b></p> 	Appears only when PPP and callback are enabled and “Callback Phone” is selected from the PCMCIA Modem menu.

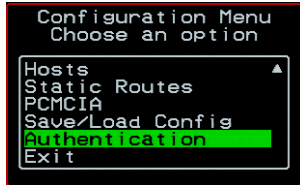
---

**Warning!** Before physically ejecting a card, always select the “Eject” option. Ejecting the card without using the Eject option can cause a system panic.

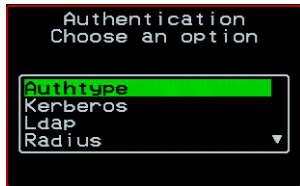
---

## Authentication Screens

You can select the Authentication option on the OSD Configuration Menu to configure an authentication type (AuthType) for logins to the KVM/net Plus and to configure authentication servers for any type of logins: to the KVM/net Plus or to KVM ports. See “Authentication” on page 48 for details about authentication on the KVM/net Plus.

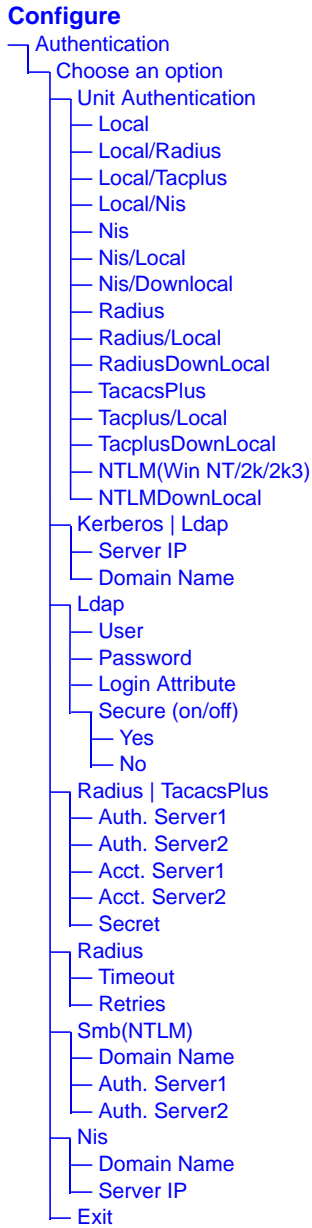


The Authentication menu appears as shown in the following figure.



Not all options are visible.

The following diagram lists the Authentication screens.

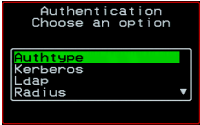
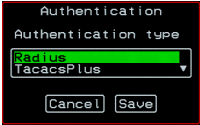


**Figure 7-10:**Authentication Options and Screens



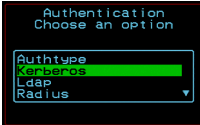
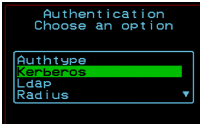
The following tables show the screens that appear when the “Authentication” option is selected from the Configure menu in the OSD. The first table shows the screen for choosing a KVM/net Plus login authentication method.

**Table 7-20:**Authentication Configuration Screens for KVM/net Plus Logins



Screen	Description
<p><b>Choose an option</b></p> 	<p>Choose either “Unit authentication” to select an Authentication method for KVM/net Plus logins, or choose one of the Authentication methods listed on this screen to configure an authentication server: Kerberos, Ldap, Radius, TacacsPlus, Smb(NTLM), or Nis.</p>
<p><b>Authentication type</b></p> 	<p>Authentication method options for KVM/net Plus logins. Default = “Local.” Other authorization type options are: Local/Radius, Local/Tacplus, Local/Nis, Nis, Nis/Local, Nis/Downlocal, Radius, Radium/Local, RadiusDownLocal, TacacsPlus, Tacplus/Local, TacplusDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal</p>

The following table shows the common screens that appear when Kerberos or Ldap are selected to configure an authentication server.

**Table 7-21:**Common Configuration Screens for Kerberos and LDAP Authentication Servers

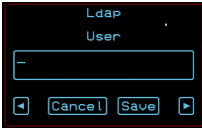
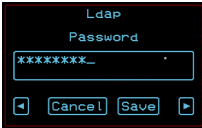
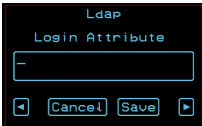

Screen	Description
<p><b>Ldap</b></p> 	<p>Choose Ldap to configure an LDAP authentication server.</p>
<p><b>Kerberos</b></p> 	<p>Choose Kerberos to configure a Kerberos authentication server.</p>

**Table 7-21:** Common Configuration Screens for Kerberos and LDAP Authentication Servers (Continued)

Screen	Description
<b>Server IP</b> 	IP address of the Kerberos or LDAP server.
<b>Domain Name</b> 	Domain name.


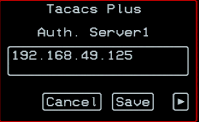

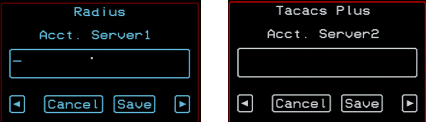
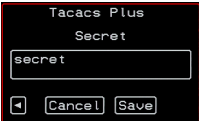

The following table shows the unique screens for configuring an LDAP server that appear in addition to the screens shown in Table 7-21, “Common Configuration Screens for Kerberos and LDAP Authentication Servers,” on page 7-407. The following table shows the configuration screens for the

**Table 7-22:** Unique LDAP Authentication Server Configuration Screens

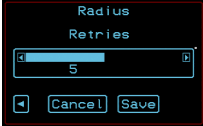
Screen	Description
<p><b>User</b></p> 	The LDAP user name.
<p><b>Password</b></p> 	The LDAP password.
<p><b>Login Attribute</b></p> 	The login attribute.
<p><b>Secure (on/off)</b></p> 	Choices are “Yes” or “No.”

Radius and TACACS+ authentication servers. The following table shows the

**Table 7-23:** Configuration Screens for the Radius or TACACS+ Authentication Servers

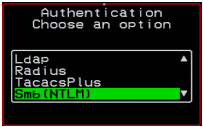
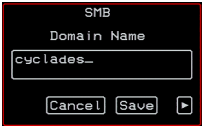

Screen	Description
<p><b>Radius</b></p> <p><b>TacacsPlus</b></p> 	<p>Choose Radius or TacacsPlus to configure a Radius or TACACS+ authentication server.</p>
<p><b>Auth. Server1</b></p>  <p><b>Auth. Server2</b></p> 	<p>IP addresses of one or two authentication servers. The second server is optional.</p>
<p><b>Acct. Server1 and Acct. Server2</b></p> 	<p>IP addresses of one or two optional accounting servers.</p>
<p><b>Secret</b></p> 	<p>Shared secret.</p>
<p><b>Timeout</b></p> 	<p>Appears only when Radius is selected. Timeout in seconds. The default is 3.</p>

**Table 7-23:** Configuration Screens for the Radius or TACACS+ Authentication Servers  
(Continued)

Screen	Description
<p><b>Retries</b></p> 	<p>Appears only when Radius is selected. Number of retries. The default is 5.</p>

Screens for configuring a Smb (NTLM) authentication server.

**Table 7-24:** Smb (NTLM) Configuration Screens

Screen	Description
<p><b>Smb(NTLM)</b></p> 	<p>Choose Smb(NTLM) to configure an SMB (NTLM) authentication server.</p>
<p><b>Domain Name</b></p> 	<p>The domain name.</p>
<p><b>Auth. Server1 and Auth. Server2</b></p> 	<p>IP addresses for one or two SMB (NTLM) authentication servers. The second server IP is optional.</p>

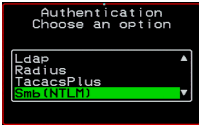
The following table shows the screens for configuring a NIS authentication server.

**Table 7-25:**NIS Configuration Screens

---

**NIS**

Choose the NIS authentication server



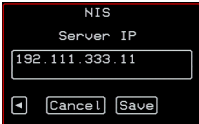
**Domain Name**

Enter the Domain Name



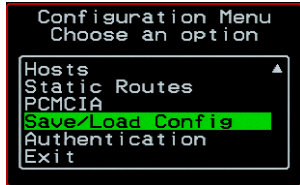
**Server IP**

IP address of the NIS server.

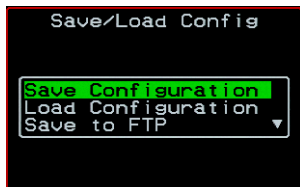


## Save/Load Configuration Screens

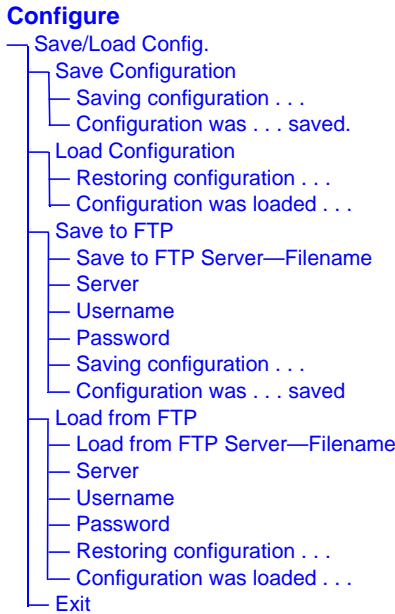
You can use the Save/Load Config option on the OSD Configuration Menu to save any configuration changes you have made since the last save into a backup directory or onto an FTP server. You can also restore configuration file changes from a backup directory or FTP server to overwrite any configuration changes that were made since the last save.



The Save/Load Config screen appears as shown in the following figure. Not all options are visible.



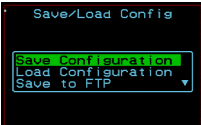
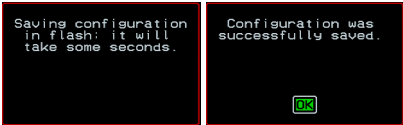
The following diagram lists the Save/Load Configuration screens.



**Figure 7-11:** Save/Load Config Configuration Screens

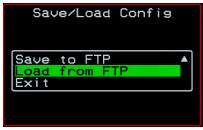
The following table shows the screens that appear when the “Save/Load Configuration” option is selected from the Configure menu in the OSD.

**Table 7-26:** Save/Load Configuration Screens

Screen	Description
<p><b>Save Configuration</b></p> 	<p>When “Save Configuration” is selected, the following two screens appear.</p> 



**Table 7-26: Save/Load Configuration Screens (Continued)**

Screen	Description
<p><b>Load Configuration</b></p> 	<p>When “Load Configuration” is selected, the following two screens appear.</p>  
<p><b>Save to FTP</b></p> 	<p>When “Save to FTP” is selected, the following five screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.” The last screens confirm the save to FTP succeeded.</p>      
<p><b>Load from FTP</b></p> 	<p>When “Load from FTP” is selected, the following four screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.”</p>     

## System Info Menu

System Information window provides administrators detailed system information. The following table offers an example of the type of information you may see on the System Info window.

**Table 7-27: System Information Example**

<b>Information Type</b>	<b>Example</b>
<b>Board</b>	KVM/net Plus Server ports: 32 User stations: 2 ID: B7DA3C0A000011
<b>Version</b>	Firmware: 2.0 Orig. Boot: 2.0.7 Alt. Boot: no code SYS FPGA: 0x43 MUX FPGA: 0x5b
<b>Memory</b>	RAM: 128 Mbytes Flash: 16 Mbytes RAM usage: 17% RAMDISK usage: 100%
<b>CPU</b>	Clock: 48 MHz
<b>Time</b>	Mon Jul 19 2005 12:35:12 PDT up 10 min
<b>User1 connection</b>	Int. uC, V1.0.4
<b>User2 connection</b>	RP main, V1.0.4 RP local, V1.0.4

## ▼ *To Access System Information*

1. On the Main Menu, select System Info.

The System Info window appears.



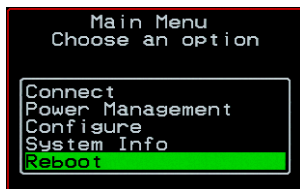
2. Use the up and down arrow keys to view the information.
3. To exit, press the escape key.

## Reboot

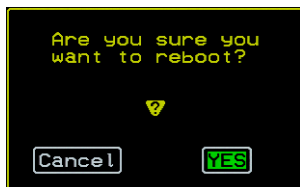
You can reboot the KVM/net Plus from the Main Menu of the OSD. This is particularly useful when operating through the RP.

## ▼ *To reboot the KVM/net Plus*

1. Select Reboot from the Main Menu.



The following message appears.



2. Select Yes to reboot the KVM/net Plus.

## Controlling the OSD Through the AlterPath KVM RP

While using the AlterPath KVM RP, an administrator has full access to the OSD menus, so all local administration tasks can be performed in an office or at any other location up to 500 feet away from the KVM/net Plus. In addition, you do not need a dedicated monitor, keyboard, and mouse to use the RP; the RP box allows you to use the monitor, keyboard, and mouse of your regular work station and use keyboard shortcuts to toggle between the view at your local work station and the view of the KVM/net Plus.

See “Installing the AlterPath KVM RP” on page 129 for details on how to install an RP. No configuration is required to begin using the RP.

### ▼ **To Use to the AlterPath KVM RP to Access the KVM/net Plus**

1. Connect the RP to the KVM/net Plus using a CAT5 cable up to 500 feet long.

See “Installing the AlterPath KVM RP” on page 129 for detailed instructions and diagrams on how to connect the RP to the KVM/net Plus and to your local work station.

2. Power on the RP.
3. Press the Select Local-Remote button on the front of the AlterPath KVM RP unit to switch the local video display from your local work station to the KVM/net Plus OSD.

The OSD login screen appears.



4. Type your username followed by your password and press Enter.

The main menu of the KVM/net Plus OSD appears. See “OSD Main Menu” on page 348 for a description of the OSD Main Menu items.

5. Depending on your access privilege, perform one or more of the following actions:
  - If logged in as administrator, perform configuration tasks as described in “Configure Menu Overview” on page 351, “System Info Menu” on page 416, and “Reboot” on page 417.
  - If desired, connect to devices that are physically connected to the KVM/net Plus.
    - See “Connection Menu” on page 349 for instructions.
  - If desired, power manage devices that are plugged into a configured AlterPath Power Management unit. (PM).
    - See “Power Management Menu” on page 350 for instructions.

### ▼ ***To Switch the RP Video Display from the OSD to the Local Computer***

Do one of the following:

- Press the following keyboard shortcut:  
Scroll Lock Scroll Lock L
- Press the Select Local-Remote button on the RP front.  
The green LED labelled Remote turns off, and the green LED labelled Local lights on.  
By default the RP is set to beep when the monitor display switches from local to remote. See “To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations” on page 420 for instructions on turning the beep on or off.

### ▼ ***To Switch the RP Video Display from the Local Computer to the OSD***

Do one of the following:

- Press the following keyboard shortcut:  
Scroll Lock Scroll Lock R
- Press the Select Local-Remote button on the RP front.  
The green LED labelled Local turns off, and the green LED labelled Remote lights on.

By default the RP is set to beep when the monitor display switches from local to remote. See “To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations” on page 420 for instructions on turning the beep on or off.

▼ ***To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations***

- Press the following keyboard shortcut:  
Scroll Lock Scroll Lock B

# Appendix A

## Troubleshooting

This chapter provides information and tasks related to troubleshooting the KVM/net Plus in the following sections.

---

Replacing a Boot Image	Page 420
Downloading a New Software Version	Page 422
Changing the Boot Image	Page 423
To Boot in U-Boot Monitor Mode	Page 425
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 425
To Boot in Single User Mode from U-Boot Monitor Mode	Page 426
To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode	Page 426
To Restore the KVM/net Plus Configuration to the Factory Default	Page 427

---

## Replacing a Boot Image

How the KVM/net Plus boots is introduced at a high level in “Boot Configuration” on page 256. The additional information in this section is to give an administrator with root access to the KVM/net Plus enough understanding to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

The KVM/net Plus uses a U-Boot boot loader that resides in soldered flash memory and automatically runs at boot time. U-Boot boots the KVM/net Plus from an image whose location is configurable. The image can reside either in removable flash memory on the KVM/net Plus or on a boot server on the network. For more about U-Boot, go to: <http://sourceforge.net/projects/u-boot>.

By default, the KVM/net Plus boots from the first partition.

- The KVM/net Plus initially boots from a software image referred to as “image 1.”
- The first time you download and install a new software version from Cyclades, the new image is stored as “image 2” in the removable flash memory and the configuration is changed to boot the KVM/net Plus from “image 2.”
- The second time you download a new software version, the latest image is stored as “image 1,” and the KVM/net Plus configuration is changed to boot from “image 1.”
- Subsequent downloads are stored following the same pattern, alternating “image 1” with “image 2.”

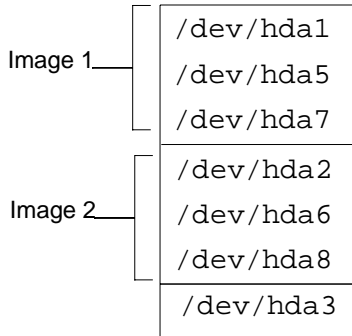


Each image on the KVM/net Plus's removable flash has three separate file systems mounted on three Linux partitions. As shown in the following table, the first partition for each image is in VFAT (file allocation table) format, and it contains the Linux kernel. The second partition, in ext2 format, contains the root-mounted filesystem, and is read only. The third partition, in ext2 format, contains the configuration files and is read/write.

**Table A-1: Boot Partitions, Formats, and Contents**

<b>Filesystem</b>	<b>Format</b>	<b>Contents</b>
hda1	VFAT	Linux kernel for Image 1
hda2	VFAT	Linux kernel for Image 2
hda3	ex2	configuration backup
hda4	extended partition	
hda4	ext2	root filesystem for Image 1
hda6	ext2	root filesystem for Image 2
hda7	ext2	configuration for Image 1
hda8	ext2	configuration for Image 2

The following figure illustrates the partitions where Image 1 and Image 2 are stored.



## Downloading a New Software Version

You can download a new software version in the following ways:

- Use the Web Manager Firmware Upgrade form to download the image from an FTP server

When the image is downloaded by FTP, a script (`saveimage`) automatically extracts the filesystem from the image, mounts it, and copies the files to the removable flash. If a current version of the image is being run from one of the three-partitions sets, the downloaded image is stored in the other set of partitions. The environment variable `currentimage` is changed so that the system boots from the new image.

- Do a network boot from the new image and then save it onto the removable flash

The monitor command `net_boot` boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if there is no removable flash card is inserted.

From the command line, you can run the `create_cf` script with the `--doformat` option to automatically save the image in removable flash. The script erases everything in the flash, partitions the flash, if necessary, formats the partitions, and copies the files currently in the RAMDISK into the corresponding image partitions. If the flash is already partitioned, you

can choose where the image is saved using the option `--imageN`.

## Changing the Boot Image

If, for any reason, you want to change to another image from the current one, if you have access to the Web Manager, you can use the Configuration > System > Boot Configuration form in Expert mode to select the other image, and then use the reboot button on the Management > Reboot form in Expert mode to reboot the KVM/net Plus.

If you do not have access to the Web Manager, you can change the boot image in one of the following ways:

- With the `bootconf` command.  
See “Changing the Boot Image with `bootconf`” on page 423.
- With U-Boot monitor mode and the available boot commands.  
See “Changing the Boot Image in U-Boot Monitor Mode” on page 424.

### ***Changing the Boot Image with `bootconf`***

If you do not have access to the Web Manager, you can use the options available with the Linux `bootconf` command to change your boot image.

#### **▼ *To Boot from an Alternate Image With `bootconf`***

1. Connect to the KVM/net Plus from a terminal connected to the console port or create a `telnet` or `ssh` connection, and log in as root.
2. Enter the `bootconf` command.

```
# bootconf
```

The `bootconf` application prompts you for values to accept or change.

3. Press “Enter” to accept the current values as prompted until the “Image names” and the prompt shown in the following screen example appear.

```
Image names:
image1:zvmppcons.v100
image2:zvmppcons.v102

Current image (image(1) or image(2)) [1] :
```

4. Enter the number of the alternate image to boot from.

The following screen example shows the number 2 entered to configure booting from image 2.

```
Current image (image(1) or image(2)) [1] :2
```

5. Enter **Y** when prompted: “Do you confirm these changes in flash.”

```
Do you confirm these changes in flash ( (Y)es, (N)o (Q)uit )[N]:Y
```

6. Restart the KVM/net Plus.

```
[root@ons /]# reboot
```

## ***Changing the Boot Image in U-Boot Monitor Mode***

You can access U-Boot monitor mode in one of the following two ways:

- During boot, when the “Hit any key to stop autoboot” prompt appears, pressing any key before the timer expires brings the KVM/net Plus to monitor mode.
- If boot fails, the KVM/net Plus automatically enters monitor mode.

The U-Boot `hw_boot` command boots from either the first or second image according to the value of the “currentimage” environment variable, which can be either 1 or 2. You can use the following procedures to specify another image.

"To Boot in U-Boot Monitor Mode"	Page 425
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 425

To Boot from an Alternate Image With bootconf	Page 423
To Boot in Single User Mode from U-Boot Monitor Mode	Page 426

## ▼ **To Boot in U-Boot Monitor Mode**

1. Open a terminal connection to the console port, and log in as root.
2. Enter the `reboot` command.

```
# reboot
```

3. During boot, when the “Hit any key to stop autoboot” prompt appears, press any key before the time elapses to stop the boot.
4. The U-Boot monitor prompt appears:

```
=>
```

5. Enter `help` to see a list of supported commands.

```
=> help
```

## ▼ **To Boot from an Alternate Image in U-Boot Monitor Mode**

1. Go to U-Boot monitor mode.  
See "To Boot in U-Boot Monitor Mode" if needed.
2. Set the current image environment variable to the number of the image you want to boot.

```
=> setenv currentimage N
```

For example, to boot from image 2 enter the number 2, as shown in the following screen example.

```
=> setenv currentimage 2
```

3. Enter the boot command.

```
=> hw_boot
```

### ▼ **To Boot in Single User Mode from U-Boot Monitor Mode**

1. See “To Boot in U-Boot Monitor Mode” on page 425 if needed.
2. Boot by entering `hw_boot` followed by `single`, as shown in the following screen example.

```
=> hw_boot single
```

### ▼ **To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode**

After performing a network boot, you can use the `create_cf` command at any time to save the files in the removable flash. The only changes you should make before running `create_cf` are configuration file changes.

1. Log in as root.
2. Set the “bootfile,” “serverip,” and “ipaddr” environment variables using the boot filename, the boot server’s IP address, and the IP address of the KVM/net Plus to use for network booting.

The format of the boot filename is: `zmpcons.vversion_number`, for example: `zmpcons.v120`.

```
=> setenv ipaddr KVM/net Plus'_IP_address  
=> setenv serverip boot_server's_IP_address  
=> setenv bootfile boot_file's_name
```

3. Check that the environment variables are set properly with the `showenv` command.

```
=> printenv
```

4. Enter the `net_boot` command.

```
=> net_boot
```

5. Log in as root after boot completes.
6. Run the `create_cf` command with the `--doformat` argument.

```
[root@ons root]# create_cf --doformat
```

7. Configure the KVM/net Plus to boot from flash.
8. Reboot.

## ▼ **To Restore the KVM/net Plus Configuration to the Factory Default**

This procedure assumes that the `saveconf` command has been previously run to save the configuration.

- While logged in as root through the console, via `telnet`, or via any `ssh` session, enter the `restoreconf` command with the `factory_default` option.

```
[root@ KVM/net Plus root]# restoreconf
factory_default
```

```
restoreconf:
Usage:
Restore from flash:          restoreconf
Restore from factory default: restoreconf factory_default
Restore from storage device: restoreconf sd
Restore from local file:    restoreconf local <FILE>
Restore from FTP server:    restoreconf ftp <FILE>
<FTP_SERVER> <USER> <PASSWORD>
Restore from TFTP server:   restoreconf tftp <FILE>
<TFTP_SERVER>
Restore from SSH server:    restoreconf ssh <FILE>
<SSH_SERVER> <USER>
```





# Appendix B

## Technical Specifications

The following table provides the technical specifications for the KVM/net Plus.

**Table B-1: Technical Specifications**

---

<b>Interfaces</b>	<ul style="list-style-type: none"><li>• 1 Ethernet 10/100BT on RJ-45</li><li>• 1 RS-232 console port on RJ-45</li><li>• 2 RS-232 auxiliary port on RJ-45</li><li>• 16 or 32 KVM ports on RJ-45 (CAT5 based)</li><li>• 1 VGA port on HD15, 1 Keyboard port on Mini-DIN6 and 1 Mouse port on Mini-DIN6 (User Interface)</li><li>• 1 KVM User Interface on RJ-45 (CAT5 based)</li><li>• 2 PCMCIA slots, 16-bit PC Card</li></ul>
<b>CPU</b>	MPC859T (PowerPC), 130 MHz clock speed
<b>Memory</b>	128 MBytes SDRAM DIMM / 128 MBytes Compact Flash
<b>Power</b>	Internal 100/240 VAC, 50/60 Hz, .78A at 120 VAC / 0.46A at 240 VAC
<b>Form Factor</b>	1U rack mountable
<b>Operating Temperature</b>	32°F to 122°F (0°C to 50°C)
<b>Storage Temperature</b>	-40°F to 185°F (-40°C to 85°C)
<b>Humidity</b>	5% to 90% non-condensing

---

**Table B-1: Technical Specifications (Continued)**

---

<b>Dimensions (WxDxH)</b>	<ul style="list-style-type: none"><li>• KVM/net Plus – 17.0" x 15.0" x 1.7" (432mm x 381mm x 43.2mm)</li><li>• KVM Expander – 12 x 2.5 x 1.53 in (30.48 x 6.35 x 3.87 cm)</li><li>• KVM Terminator 1.24 x 2.60 x 0.85 in (3.15 x 6.60 x 2.16 cm)</li><li>• KVM RP 9 x 9 x 1.75 in (22.86 x 22.86 x 4.45 cm)</li></ul>
<b>Certifications</b>	<ul style="list-style-type: none"><li>• FCC</li><li>• CE</li><li>• VCCI</li><li>• C-Tick</li><li>• CSA (US and Canada)</li><li>• EN60950</li></ul>

---

# Glossary

## **3DES**

Tripple Data Encryption Standard, an encrypting algorithm (cipher) that processes each data block three times, using a unique key each time. 3DES is much more difficult to break than straight DES. Because it is the most secure of the DES combinations, 3DES is also slower in performance.

## **authentication**

The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.

## **basic in/out system (BIOS)**

Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.

## **baud rate**

The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.

## **BogoMips**

A measurement of processor speed made by the Linux kernel when it boots, to calibrate an internal busy-loop.

## **boot**

To start a computer so that it is ready to run programs for the user. A PC can be booted either by turning its power on, (Cold Boot) or by pressing Ctrl+Alt+Del (Warm Boot).

<b>bootp</b>	Bootstrap Protocol. A TCP/IP protocol allowing a BOOTP server node to allocate IP addresses to diskless work stations at startup.
<b>CAT5</b>	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.
<b>console</b>	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.
<b>checksum</b>	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.
<b>DHCP</b>	<p>Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.</p> <p>DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.</p>
<b>escape sequence</b>	<p>A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.</p> <p>An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one</p>

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.

<b>IPsec</b>	Short for <i>IP Security Protocol</i> , IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as 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.
<b>Kerberos</b>	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.
<b>KVM</b>	Keyboard, video and mouse interface to a server.
<b>LDAP</b>	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.
<b>MAC</b>	Medium Access Control. Internationally unique hardware identification address that is assigned to the NIC (Network Interface Card) which interfaces the node to the LAN.
<b>network mask</b>	<p>A number used by software to separate the local subnet address from the rest of a given Internet protocol address</p> <p>Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (for example, 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.</p>

<b>NTP</b>	<i>Network Time Protocol.</i> A standard for synchronizing your system clock with the "true time", defined as the average of many high-accuracy clocks around the world.
<b>OSD</b>	On-Screen Display.
<b>packet</b>	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.
<b>parity</b>	<p>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.</p> <p>The following lists the available parity parameters and their meanings:</p> <p><b>Odd</b> – Parity bit set so that there is an odd number of 1 bits</p> <p><b>Even</b> – Parity bit set so that there is an even number of 1 bits</p> <p><b>None</b> – Parity bit is ignored, value is indeterminate</p>
<b>PCMCIA</b>	<b>Personal Computer Memory Card International Association</b> – An organization that supports standards for a compact hardware interface that accepts a variety of devices such as modems, storage, and other devices.
<b>port</b>	A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a

port number may be seen as an address of an application within the computer.

**PPP**

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

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

**RADIUS**

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

**RC4**

Rivest Cipher four, an encryption method using variable length secret key streams. RC4 is an alternate to DES and is approximately ten times as fast as DES; however, it is less secure.

**SMTP**

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

**SNMP**

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

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

(Source: Webopedia)



**SNMP Traps**

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

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

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

**SSH**

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

**Stop Bit**

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

**Subnet Mask**

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

**TACACS**

Terminal Access Controller Access Control System.

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

**TACACS+**

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

**Telnet**

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

executed as if you were entering them directly on the server console.

- TFTP** Trivial File Transfer Protocol. A simple network application based on User Datagram Protocol (UDP). It is used to transfer files from one computer to another.
- TTY** 1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.
- UDP** *User Datagram Protocol* uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.
- VPN** *Virtual Private Networking* allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.
- Watchdog timer** Mechanism to detect hardware and operating system failures.

# Index

## Numerics

3DES 190, 356  
56K 335

## A

access 153

- assigning KVM port 186
- in-band server 4
- user 67
- user and group 185

Access Control 364

Access list for username - select the server  
399

access to

- KVM ports, enabling direct 165
- Web Manager 102
- Web Manager, default IP address 102
- Web Manager, dynamic IP address 103

Access window 6, 308, 314

Access window tab 310

accessing

- cascaded ports 29
- connected devices 292
- connected devices, tasks related to 38
- in-band servers 296
- KVM RP 131
- KVM servers 297
- ports 38
- RDP servers 204
- system information 415

Acct. Server1 and Acct. Server2 409

ACK 224

ACK Flag 375

Active 386

active sessions 280

- killing 281

- viewing information on 280

activity LEDs 16

activity LEDs, front panel 18

adding

- a group 184

- chain 229

- chain for IP filtering 231

- KVM Expander 66

- packet filtering rule 231

- RDP server 205

- rule for IP filtering 233

- secondary KVM 178

- syslog server 150

- user 145, 182

admin's default password, changing 100

administering users of connected servers 38

administration

- control buttons 136

- KVM/net Plus information 136

- logout button 136

- modes of 141

- options 23

- Web Manager 138

- windows, common features of 136

alarms

- logging 53

- syslog 52

alarms and syslog, configuring 159, 160

## Index

- Alias 378
    - alias for a KVM port, specifying 176
  - AlterPath KVM Expander, installing 119
  - AlterPath KVM Terminators 74, 121
  - AlterPath KVM/net Plus
    - ordering options 19
    - shipping box contents 73
  - AlterPath PM
    - connecting 117
    - upgrading 161
  - AlterPath RP 68, 416
    - installing 129
    - using 416
  - AlterPath Viewer 312
    - options, setting 334
    - overview 310
    - settings 332
  - Any 224
  - Auth. Server1 and Auth. Server2 410
  - authentication for KVM port logins 167
  - authentication method 192, 241
    - configuring an 191
    - KVM ports 167
    - KVM ports 193
  - authentication methods 51
    - choosing among 48
    - tools for specifying 51
  - authentication overview 48
  - Authentication Protocol 241
  - Authentication Required, PPP configuration 253
  - authentication screens 404
  - authentication server
    - Kerberos 195
    - LDAP 197
    - NIS 200
    - Radius 201
    - SMB(NTLM) 199
    - TACACS+ 202
  - authentication servers 194
  - Authentication Type 165, 355
  - Authentication type 406
  - Auto 335
  - Auto Sync Mouse 333
  - AUX 1 port for use with a PM, configuring the 251
  - AUX 1 port, connecting a PM to the 117
  - AUX 2 port, configuring the 251
  - AUX port - PPP 388
    - Baud Rate 388
    - Data Size 389
    - Flow Control 389
    - Local IP 389
    - Parity 389
    - Remote IP 389
    - Stop Bits 389
  - AUX port, connecting an external modem 116
  - AUX ports
    - configuring with OSD 388
    - configuring with Web Manager 250
    - description 15
  - AUX ports - Protocol 388
  - AUX ports screens, OSD 387
- ## B
- back panel
    - KVM RP 68
    - KVM/net Plus 11
  - back up configuration data 270
  - Backspace 346
  - backup configuration 268
  - Baud Rate, PPP configuration 252
  - beeper on AlterPath KVM RP 418
  - Board 414
  - boot
    - configuration 256
    - configuring with Web Manager 259

- image 425
- image, changing the 423
- Boot Action 369
- Boot Action, Local 241
- Boot File Name 258
- bootconf command 423
- box contents, shipping
  - KVM Expander 120
  - KVM RP 130
  - KVM/net Plus 73
- brackets, mounting 74, 121
- brightness, adjusting screen 312, 313, 327
- buffering, data 52

## C

- cabling
  - white paper and ordering 74, 121
- callback 403
- callback phone 403
- card slots, PCMCIA 6
- card, PCMCIA 16
  - configuring a modem 216
  - eject PCMCIA 219
  - installing 114
  - removing 115
- Cascade Device Add Device 391
- Cascade Device Delete Device 392
- Cascade deviceAdd device Select Model 392
- Cascade deviceChoose an option 391
- cascade devices 390
- cascaded devices 27
  - accessing ports on 29
  - adding 178
  - configuring 177
  - connecting 126
  - deleting configuration of 181
  - editing configuration of 179
  - KVM Expander 64

- reading the port numbers of 301
- CE 430
- certifications 430
- chain
  - adding 229, 231
  - editing 229, 233
- Chain - CHAIN\_NAME 372
- Chain - chain\_name 372
- Chain Name 372
- changing default passwords 101
- check boxes, inverted 222
- Choose an option 395, 396, 406
- closing a KVM connection 330
- closing a local KVM connection 330
- code, upgrading the KVM Expander
  - microcontroller 66
- Comments field 183
- Common Escape Sequence 165
- Community 243, 244
- computers to KVM ports, connecting 80, 82
- configuration 159, 162
  - back up or retrieve 270
  - backup 268
  - basic network 86
  - boot 256
  - cascaded KVM unit 179, 181
  - changes, saving 140
  - direct connection for network 84
  - factory default 427
  - firewall 228
  - network 358
  - tasks 106
  - Web Manager 99
- configuration screen series, understanding
  - OSD 354
- configuration screens
  - Date/time 381
  - General 355
  - Hosts 377
  - IP Filtering 370

## Index

- Network 359
- Save/load 411
- SNMP 362
- Static Routes 378
- VPN 366
- Configure 349
- configure menu overview 351
- configuring
  - authentication method 191
  - authentication method for logins through KVM ports 193
  - authentication method, KVM/net Plus logins 192
  - authentication servers 194
  - AUX 1 port 251
  - AUX 2 port 251
  - basic networking
    - OSD 90
    - wiz command 87
  - boot 259
  - cascaded KVM units 177
  - creation of alarms and syslog files for IPDUs 159, 160
  - encryption on port connections 190
  - external modem 251
  - host settings 212
  - hosts 246
  - in-band (RDP) servers 203
  - IP user (KVM over IP) sessions 172
  - KVM port for power management 174
  - local User 1 and User 2 sessions 171
  - logging and alarms 53
  - modem (PCMCIA) card 216
  - modem card 216
  - network parameters, OSD 94
  - network parameters, wiz command 88
  - NIS authentication server 200
  - power management 46
  - PPP connection on a remote computer 340
  - preconfigured KVM/net Plus 106
  - SMB(NTLM) authentication server 199
  - SNMP 243
  - syslogging 215
  - terminal emulator dial up connection 342
  - User 1 sessions 171
  - User 2 sessions 171
  - users to manage power outlets 158
  - VPN 239
- conflicting mouse settings, avoiding 107
- conflicts, avoiding Internet Explorer 110
- conflicts, preventing mouse 107, 108, 109
- Connect 348
- Connect read only 330
- Connect read write 331
- Connect to Server form 304
- connected devices
  - accessing 38
  - authentication 194
  - power on 85
  - powering on 85, 125
  - who can access 292
- connected port information, viewing 310, 325
- connected servers, administering users of 38
- connecting
  - AlterPath PMs 117
  - another port 310
  - cascaded KVM units 126
  - computers to KVM ports 82
  - computers to the KVM ports 80
  - Connect to Server drop-down list 300
  - external modem 116
  - external modem to an AUX port 116
  - KVM Expander 128
  - KVM port through the login screen 306
  - KVM RP to the local work station 132
  - multiple PMs 118
  - PM to the AUX 1 port 117

- servers with the OSD 320
  - servers with the Web Manager 304
  - servers, preparing for 81
- connecting to
  - servers 153
- connection
  - closing a local KVM 330
  - closing KVM 330
  - direct 84
  - Ethernet 79
  - PPP 342
  - quitting the port 315
  - resuming port 315
  - shareing server 317
  - sharing server 315
  - terminal emulator dial up 342
- connection menu 335, 349
- connection menu, OSD 321
- Connection Name 367
- connection type 36
- connection types 36
- connections
  - Access window 6
  - daemons used for incoming 221
  - encryption on port 190
  - modem 339
  - prerequisites for in-band 296
  - prerequisites for KVM 297
  - sharing KVM port 330
  - simultaneous server 22
  - through the OSD, controlling local KVM
    - port 322
  - viewing in-band 296
  - viewing KVM 294
- Connector Name 240
- console
  - port, connection 84
  - port, logging in through the 87
  - port, changing the password through the
    - 87

- contrast, adjusting screen 312
- CPU 414, 429
- CSA (US and Canada) 430
- C-Tick 430
- Cyclades Web Manager 24
- cycle 311, 326
- Cycle Time 170
- Cycling 384
- cycling 311, 326

## D

- daemons 221
- daisy chaing power 125
- data buffering 52
- Data Size, PPP configuration 252
- data, backing up configuration 270
- date and time
  - manual setting 254
  - NTP 255
  - OSD 97
- date/time configuration screens 381
- default
  - IP address 102
  - password, changing admin's 100
  - passwords, changing 100, 101
  - restore factory 427
- deleting
  - cascaded KVM unit 181
  - in-band (RDP) server 208
  - syslog server 150
  - user 147
  - user or group 184
- description 2
- Destination IP 373
- Destination IP field 223
- Destination Mask 373
- Destination Port 224, 374
- Device 380

## Index

### devices

- accessing connected 38
- accessing ports on cascaded KVM 29
- cascade 390
- cascaded 27
- daisy chained on KVM Expander 125
- power on connected 85
- power on KVM-connected 125
- powering on connected 85, 125
- preparing to connect 81
- reading port numbers of cascaded 301
- who can access connected 292

DHCP, configuring 360

DHCP, description 55

dial in 343

dial up connection 342

dimensions 430

Direct Access 164, 356

direct access to KVM ports, enabling 165

direct connection 84, 102

disabling KVM ports 176

DNS Server 361

### document

- audience xxix
- CD xxxi
- downloads xxxi
- organization xxx
- related documentation xxxi

Domain 361

Domain Name 407, 410

download microcode 278

downloading

- documents xxxi

downloading new software 422

DSL 335

dynamic IP address 103

## E

echo-reply 238

### editing

chain 229

chain for IP filtering 233

configuration of a cascaded KVM unit  
179

rule for IP filtering 230

rule options 222

ejecting PCMCIA cards 219

EN60950 430

### enabling

access to Web Manager 102

direct access to KVM ports 165

KVM ports 176

Encrypt Everything 335

Encrypt Keyboard and Mouse 335

encryption 47

encryption on port connections, configuring  
190

Encryption Type 335

End 346

Enter 346

Enter the group name 396

Enter the password 395

Enter the username 396

Esc 346

Escape Sequence 356

escape sequence

conventions for xxxii

Ethernet connection, making an 79

Exit 349

### Expander

cascading 64

connecting 128

features 60

installing 119

KVM 59

LEDs 63

list of cascaded devices 66



- microcontroller code, upgrading 66
- models and components 61
- mounting 122
- ports 62
- power outlets 63, 125
- powering on 125
- setting up 122
- shipping box contents 120
- enabling direct access to KVM ports 165
- Expert mode 151
- Expert mode, overview 152
- external modem
  - configuring 251
  - connecting 116
- external modem, configuring an 251

## **F**

- facility numbers
  - example 53
  - syslog messages 53
- factory default, restoring configuration to 427
- Fast Ethernet 258
- Fast Ethernet Max Interrupt Events 258
- FCC Part 15 430
- features of administrators' Windows,
  - common 136
- features, KVM Expander 60
- Field Adjacent to Go to 249
- fields
  - ICMP protocol 225
  - numeric protocol 224
  - TCP protocol 224
  - UDP protocol 225
- Filter Table 372
- filtering
  - chain for IP 231, 233
  - configuration screens, IP 370

- IP 221
  - KVM port message 215
  - packet 42
  - packet rule adding 231
  - rule for IP 230, 233
- FIN 224
- FIN Flag 375
- firewall configuration procedures 228
- firmware upgrade 272, 275
  - AlterPath PM 161
  - Cyclades pathname for 274
- Flow Control, PPP configuration 252
- Force Screen Auto Alignment 333
- Force Screen Refresh 333
- forms
  - navigation conventions xxxii
- FORWARD packet 222
- Fragments 227, 376
- FTP server, download microcode 278

## **G**

- Gateway 360, 380
- Gateway or Device 380
- general 164, 260
- general configuration screens 355
- general information 260
- GMT 255
- Go to 249
- Graph BG Color 266
- Graph Type 266
- Grey Scale 336
- Grid Line Color 266
- Group field 183
- groups
  - adding 184
  - assign KVM port access to 185, 186
  - deleting 184
  - modifying 185

## Index

- screens 393
- guidelines for using the KVM/net Plus 8

## H

- hierarchy, KVM port permissions 31
- High Color 336
- Home 346
- Host IP 249
- Host or Net Route 379
- host settings 211
- host settings, configuring 212
- host tables 246
- Hostname 361
- hosts configuration screens 377
- hosts, configuring 246
- hot keys
  - conventions for xxxii
  - for emulating sun keyboard keys 324
  - for local station 323
  - redefining KVM connection 40
  - redefining sun keyboard equivalent 40
  - summary of tasks for redefining 41
- humidity 429

## I

- ICMP protocol fields 225
- ICMP Type 376
- icmp-host-prohibited 238
- icmp-host-unreachable 238
- icmp-net-prohibited 238
- icmp-net-unreachable 238
- icmp-port-unreachable 238
- icmp-proto-unreachable 238
- ID, Local 241
- ID, Remote 241
- idle timeout

- configuring 169, 383
  - resuming port connection after 315
- IE security settings, modifying 110
- in-band connections, viewing 296
- in-band server
  - access, description 4
  - adding 205
  - configuring 203
  - deleting 208
  - modifying 205
- in-band servers
  - prerequisites for accessing 204, 296
- info menu, system 414
- info, view IPDUs 156
- information
  - access system 415
  - Access window, refreshing 314
  - obtaining more 137
  - view active sessions 280
  - view and reset IPDU 157
  - view connected port 310, 325
  - viewing system 260
- Input Interface 227, 375
- input interface, output interface, and fragments 226
- INPUT packet 222
- installation, preconfiguring for remote 105
- installing
  - AlterPath KVM Expander 119
  - AlterPath KVM RP 129
  - PCMCIA card 114
  - PCMCIA cards in the front card slots 114
- interfaces 429
- Internet Explorer conflicts, avoiding 110
- Inverted check boxes 222
- IP 378
- IP Address 360
- IP address
  - default 102

- dynamic 103
- IP Address, Local 241
- IP Address, Remote 241
- IP filtering 221
  - add a chain for 231
  - add a rule for 233
  - configuration screens 370
  - edit a chain for 233
  - edit a rule for 230
- IP Local 402
- IP Options 237
- IP Remote 403
- IP Security Level 356
- IP user (KVM over IP) sessions, configuring 172
- IP user sessions, configuring 172
- IP users, local user and 168
- IPDU information, viewing and resetting 157
- IPDU power management 154
- IPDU power management forms, controlling power through 45
- IPDUs info, view 156
- IPDUs, alarms and syslog 159, 160

## K

- Kerberos 194, 406
- Kerberos authentication server, configuring 195
- keyboard
  - and mouse, resetting the 328
  - equivalent hot keys, redefining sun 40
  - keys, hot keys for emulating sun 324
  - shortcuts (hot keys), redefining 40
  - shortcuts (hot keys), redefining KVM connection 166
  - shortcuts, redefining KVM connection 166

- Keyboard Type 170, 384
- keys
  - basic navigation 346
  - conventions for hot keys, escape keys, and keyboard shortcuts xxxii
  - hot keys for emulating sun keyboard 324
  - redefining KVM connection hot 40
  - redefining sun keyboard equivalent hot 40
  - summary of tasks for redefining hot 41
- keys for
  - local, hot 323
- Kill other session 331
- killing active session 281
- KVM 163
- KVM connections
  - closing 330
  - closing local 330
  - hot keys, redefining 40
  - keyboard shortcuts, redefining 166
  - prerequisites 297
  - viewing 294
- KVM devices
  - accessing ports on cascaded 29
  - port numbers of cascaded 301
- KVM Expander 59
  - cascading a 64
  - connect to master 128
  - features 60
  - installing 119
  - LEDs 63
  - master device list 66
  - microcontroller code, upgrading 66
  - models and components 61
  - mounting 122
  - ports 62
  - power on 125
  - power outlets 63, 125
  - powering on 125
  - setting up 122

## Index

- shipping box content 120
  - KVM port
    - access, assigning 185, 186
    - alias 176
    - connecting 306
    - connections, sharing 330
    - connections, OSD 322
    - disabling 176
    - enabling 176
    - logins, specifying authentication method 167
    - logins, specifying authentication 167
    - permissions hierarchy 31
    - permissions, understanding 30
    - power management, configuring 174
  - KVM ports 12, 386
    - connecting computers to 80, 82
    - controlling power while connected to 45
    - enable direct access to 165
    - enabling direct access to 165
    - modifying individual 172
    - syslogging for 215
  - KVM ports screens 385
  - KVM RP
    - beep 418
    - connectors 68
    - powering on 132
    - shipping box contents 130
  - KVM session keyboard shortcuts, redefining 166
  - KVM terminator usage and types 58
  - KVM terminators 74, 121
  - KVM unit
    - adding cascaded 178
    - configuring cascaded 177
    - connecting cascaded 126
    - deleting cascaded 181
    - editing cascaded 179
  - KVM ports, authentication method 193
  - KVM-connected devices, powering on 125
  - KVM-connected server, controlling power 329
- ## L
- LAN 335
  - LDAP 194
  - Ldap 406
  - LDAP authentication server, configuring an 197
  - LED status 6
  - LEDs 16
  - LEDs on ports 16
  - LEDs on the KVM Expander 63
  - LEDs, front panel activity 18
  - Left / Right 346
  - Level 0 190
  - Level 1 190
  - Level 2 190
  - Load Configuration 413
  - Load from FTP 413
  - Local (“Left”) 241
  - local GMT 255
  - Local ID 368
  - Local IP 368
  - Local IP Address, PPP configuration 252
  - local KVM connection, closing a 330
  - local KVM port connections (OSD),
    - controlling 322
  - Local NextHop 368
  - Local Subnet 368
  - local User 1, configure 171
  - local User 2, configure 171
  - local user and IP users 168
  - local work station, connecting RP to 132
  - local, hot keys for 323
  - LOG 223
  - Log Level 237
  - Log Prefix 237

- log target 227
- logging into
  - console 87
  - OSD 91, 347, 348
  - Web Manager 138
  - Web Manager as a regular user 286
  - Web Manager as admin 138
  - Web Manager, prerequisites for 286
- logging to syslog servers, prerequisites for 52
- logging, configuring 53
- Login Attribute 408
- login screen
  - direct logins enabled
    - IP address and port entered 302
    - IP address entered 301
    - Direct Logins Not Enabled 299
- login screen, connecting to a KVM port through the 306
- login screen, Web Manager 297
- logins through KVM ports, configuring an authentication method for 193
- logins, authentication method 167, 192
- logins, authentication servers 194
- logins, simultaneous 21
- logins, specifying authentication for KVM port 167
- Low BW LAN 335
- Low Color 336
- Low Grey Scale 336

## M

- main menu, OSD 348
- managing power, options for 44
- manually, setting the date and time 254
- Mask field 223
- Mean Temp 266
- Memory 414
- memory 429

- menu
  - after connecting to a port, returning to the connection 325
  - Configure, OSD 351
  - connecting to servers through the OSD connection 321
  - Connection 335, 349
  - Network Configuration/ 358
  - options 333
  - OSD main 348
  - Power Management 350
  - System Info 414
- menus and forms in Expert mode, overview of 152
- messages, facility numbers for syslog 53
- Metric 250, 380
- microcode
  - FTP download 278
  - reset 279
  - reset after upgrade 279
  - upgrade 276
  - upgrade, finding pathname for 274
- microcontroller code, upgrading the KVM Expander 66
- mode
  - Expert 151
  - Expert overview 152
  - procedures in Wizard 142
  - steps in Wizard 142
  - Wizard 141
- models and components, KVM Expander 61
- modem
  - configuring the AUX 2 port for use with an external 251
  - connecting an AUX port to an external 116
  - connecting an external 116
  - connections 339
- modem (PCMCIA) card, configuring a 216
- modem card, configuring a 216

## Index

- Modem Initialization, PPP configuration 252
- modes, administrative 141
- modify
  - group 185
  - IE security settings 110
  - in-band (RDP) server 205
- modifying individual KVM ports 172
- monitor mode
  - boot alternate image 425
  - boot in u-boot 425
  - boot single user mode 426
  - changing the boot image in u-boot 424
  - replace boot image, network boot 426
- monitor, temperature 8
- monitoring temperature 263
- monitoring temperatures 56
- more information, obtaining 137
- mounting
  - brackets 74, 121
  - KVM Expander 122
  - KVM Expander, the 122
  - KVM/net Plus 75, 76
- mouse conflicts
  - Windows 2000 / Me 108
  - Windows 95/98/NT 108
  - Windows XP/Windows 2003 107
- mouse conflicts, preventing 107, 108, 109
- mouse, resetting 328
- Mouse/Keyboard 384
- MTU/MRU, PPP configuration 253

## N

- Name 378
- navigating
  - conventions xxxii
  - the OSD 346
- navigation
  - actions, common 347

- keys, basic 346
- Netmask 360, 380
- network 209
- Network bits/sec 333
- network boot in u-boot monitor mode,
  - replacing a boot image 426
- network configuration menu options 358
- network configuration screens 359
- network configuration, making a direct
  - connection for 84
- network configuration, performing basic 86
- Network IP 249
- Network Mask 249
- network parameters
  - OSD 94
  - Web Manager 143
  - wiz command 88
- network time protocol 96
- new software version, downloading 422
- next port 312
- NextHop, Local 241
- NextHop, Remote 241
- NIS 194, 410
- NIS authentication server, configuring a 200
- No Encryption 336
- notifications 52
- NTLM 194
- NTP, setting the time and date with 255
- numbers for syslog messages, facility 53
- numbers of cascaded KVM devices, reading
  - the port 301
- numbers, example of using facility 53
- numeric protocol fields 224

## O

- OID 245
- operating temperature 429
- ordering

- parts 121
- ordering options 19
- ordering parts 74
- organization,
  - document xxx
- OSD
  - change a password in 92
  - configuration screen series,
    - understanding 354
  - configuring basic networking 90
  - configuring networking 94
  - connecting to servers through 320, 322
  - connection menu, connecting to servers
    - through the 321
  - conventions for showing how to navigate
    - to screens xxxii
  - log into 91, 348
  - logging in to 347
  - main menu 348
  - navigating the 346
  - RP 417
  - switching the KVM RP video display to
    - the 417
  - through the AlterPath KVM RP,
    - controlling the 416
  - time and date, setting 97
- OSD Reboot screen 349
- Outlets at Device field 175
- Outlets Manager 155
- outlets, configuring users for managing 158
- outlets, KVM Expander 63
- Output Interface 227, 375
- OUTPUT packet 222
- overview, Configure menu, OSD 351
- overview, Expert mode 152

## P

- packet filtering 42

- packet filtering rule, adding a 231
- Page Up / Page Down 346
- panel activity LEDs, front 18
- parameters defined using the wiz command,
  - applying and confirming the network 89
- parameters using the OSD, configuring
  - network 94
- Parity, PPP configuration 252
- Password 408
- password
  - changing a 147
  - changing a user's 184
  - changing admin's default 100
  - changing default 100, 101
  - changing the root 100
  - changing through console 87
  - changing through OSD 92
  - changing your 289
- Password field 183
- pathname for firmware upgrades 274
- pathname for microcode upgrades 274
- PCMCIA card
  - ejecting 219
  - installing 114
  - removing 115
  - slots 6
- PCMCIA Modem 402, 403
- PCMCIA screens 400
- performing basic network configuration 86
- Permission, SNMP 245
- Permissions for username
  - 399
- permissions hierarchy, KVM port 31
- permissions, port 29
- permissions, understanding KVM port 30
- PM
  - connecting AlterPath 117
  - connecting multiple 118
  - power control of devices 288
  - upgrade 161

## Index

### port

- access 185, 186
- alias 176
- AUX 116
- AUX 1 117
- AUX 1, configuration 251
- AUX 2, configuration 251
- cascaded KVM devices 301
- connecting to KVM 306
- connection, quitting 315
- connections
  - encryption on 190
  - OSD 322
  - sharing KVM 330
- console 84
- disabling KVM 176
- enabling KVM 176
- information, viewing connected 310, 325
- logins, authentication method 167
- permissions 29
- permissions hierarchy, KVM 31
- permissions, understanding KVM 30
- power management, configuration 174
- resuming connection 315
- status 261
- User 1 85

### Port Info 385

### ports

- access types 38
- activity LEDs on 16
- AUX 15, 250
- connecting computers to the KVM 80
- controlling power while connected to KVM 45
- cycle between 311
- enabling direct access to KVM 165
- KVM 12
- modifying individual KVM 172
- stop cycling between 311

### TCP 26

- types of 9

- ports and specify message filtering,
  - configuring syslogging for KVM 215
- ports on cascaded KVM devices, accessing 29
- ports on the KVM Expander 62
- ports screens, AUX 387
- ports screens, KVM 385
- power connector 12
- power control 288
- Power Management 349, 384
- power management 44, 336
  - configuring a KVM port for 174
  - forms 45
  - IPDU 154
  - KVM-connected servers 45, 329
  - menu 350
  - options 44
  - regular users 288
  - setting up and configuring 46
  - Web Manager 45
- Power Outlet 387
- power outlets
  - configuring users to manage 158
  - on the KVM Expander 63
- power outlets, KVM Expander 125
- power specification 429
- power switch 12
- power, supplying to the KVM RP 132
- powering KVM RP 132
- powering on
  - connected devices 85
  - KVM-connected devices 125
  - the KVM 85
  - the KVM Expander 125
  - the KVM RP 132
  - the KVM/net 85
  - the KVM/net Plus 85
- PPP 402



- PPP connection from a remote computer, making a 342
- PPP connection on a remote computer, configuring a 340
- PPP Options, PPP configuration 253
- preconfigured KVM/net Plus, setting up 106
- preconfiguring the KVM/net Plus 105
- prerequisites for
  - accessing in-band servers 296
  - accessing KVM servers 297
  - in-band access 204
  - logging to syslog servers 52
  - using the Web Manager 25
  - Web Manager loggins 286
- Pre-Shared Secret, Local 242
- previous server, switching to 327
- procedures
  - firewall configuration 228
  - in Wizard mode 142
- Profile, PPP configuration 252
- Protocol 367, 374
- protocol 223
- Protocol drop-down list 223
- protocol fields
  - ICMP 225
  - numeric 224
  - TCP 224
  - udp 225
- Protocol Number 374
- PSH 224
- PSH Flag 375

## Q

- Quit 384
- Quit this session 330
- quitting the port connection 315

## R

- RADIUS 194
- Radius 409
- Radius authentication server 201
- RC4 190
- RDP servers, prerequisites for access 204
- reboot 282, 415
- reboot, remote location 282
- recommended settings 332
- redefining
  - hot keys, summary of tasks for 41
  - keyboard shortcuts (hot keys) 40
  - KVM connection hot keys 40
  - KVM connection keyboard shortcuts (hot keys) 166
  - KVM session keyboard shortcuts 166
  - sun keyboard equivalent hot keys 40
- refreshing Access window 314
- regular users
  - log into Web Manager as 286
  - power management for 288
  - Web Manager for 284
- REJECT 223
- reject target 228
- remote
  - computer, configure a PPP connection 340
  - computer, make a PPP connection 342
  - installation 105
  - location, rebooting from a 282
- Remote (“Right”) 241
- Remote ID 368
- Remote IP 368
- Remote IP Address, PPP configuration 253
- Remote Nexthop 369
- Remote Subnet 369
- remove a PCMCIA card 115
- replace boot image 426
- resetting
  - IPDU information 157

## Index

- keyboard and mouse 314
  - microcode 279
  - the keyboard and mouse 328
  - the microcode after upgrade 279
- restore factory default configuration 427
- resume connection after idle timeout 315
- Retries 409
- retrieve configuration data 270
- returning to the connection menu after
  - connecting to a port 325
- Rivest Cipher four 190
- root password, changing the 100
- Route 249
- routes, static 248, 378
- RP
  - access the KVM/net Plus 416
  - beep 418
  - connecting to KVM/net Plus 131
  - connecting to local work station 132
  - connectors on back 68
  - installing 131
  - powering on 132
  - shipping box contents 130
  - supplying power 132
  - video display, switching 417
- RSA Key, Local 241
- RSA Key, Remote 241
- RST 224
- RST Flag 374
- rule and edit rule options, add 222
- rule for IP filtering, adding a 233
- rule for IP filtering, editing a 230
- rule options, add rule and edit 222
- rule, adding a packet filtering 231
- rules
  - add 222

## S

- Save changes 347
- Save Configuration 412
- Save to FTP 413
- save/load configuration screens 411
- saving changes, logging into the Web Manager and 138
- saving configuration changes 140
- Scr. saver timeout screen 384
- screen brightness and contrast, adjusting 312, 313, 327
- Screen Save Timeout field 169
- screen series, understanding OSD configuration 354
- screens
  - authentication 404
  - AUX ports 387
  - date/time configuration 381
  - general configuration 355
  - hosts configuration 377
  - IP filtering configuration 370
  - KVM ports 385
  - network configuration 359
  - OSD
    - conventions for showing how to navigate to screens xxxii
  - PCMCIA 400
  - save/load configuration 411
  - SNMP configuration 362
  - static routes configuration 378
  - syslog 400
  - user station 382
  - users and groups 393
  - VPN configuration 366
- Secret 409
- Secure (on/off) 408
- security 47, 189
- security settings, IE 110
- sensor, temperature 263

- server
  - add or modify an in-band (RDP) 205
  - connect to 153
  - connect to next 327
  - connect to previous 327
  - controlling power of a KVM-connected 329
  - cycle by 326
  - download microcode from an FTP 278
  - in-band (RDP), delete an 208
  - Kerberos authentication, configuring 195
  - LDAP authentication, configuring 197
  - next 327
  - NIS authentication, configuring 200
  - previous 327
  - Radius authentication, configuring 201
  - RDP, delete an 208
  - SMB(NTLM) authentication, configuring 199
  - syslog, add a 150
  - syslog, delete a 150
  - TACACS+ authentication, configuring 202
- server access, in-band 4
- server connections
  - Access window, managing with 308
  - AlterPath Viewer options 334
  - in-band and out of band 34
  - sharing 315, 317
  - simultaneous 22
  - what you see 293
- server drop-down list 300
- Server IP 407, 410
- Server name 386
- servers
  - administering users of connected 38
  - configuring in-band (RDP) 203
  - connecting, OSD 320
  - connecting, Web Manager 304
  - cycling between 326
  - prerequisites for in-band access to RDP 204
  - prerequisites for logging to syslog 52
  - syslog 52
  - servers with in-band connections, prerequisites for accessing 296
  - servers with KVM connections, prerequisites for accessing 297
  - servers, authentication 194
  - services 220
  - session keyboard shortcuts, redefining KVM 166
  - sessions
    - active 280
    - information, viewing active 280
    - killing active 281
  - Set 224
  - set the time and date with NTP 255
  - Set, TCP flag 224
  - settings
    - AlterPath Viewer 332
    - avoiding conflicting mouse 107
    - changing network 143
    - configuring host 212
    - host 211
    - modifying IE security 110
    - recommended Alter Path Viewer 332
  - sharing
    - KVM port connections 330
    - server connections 315, 317
  - Shell field 183
  - shipping box contents
    - AlterPath KVM/net Plus 73
    - KVM Expander 120
    - KVM RP 130
  - shortcuts
    - redefining keyboard 40
    - redefining KVM connection keyboard 166

## Index

- redefining KVM session keyboard 166
  - Show Frames/sec 333
  - Show Startup Dialog 333
  - single user mode 426
  - Smb(NTLM) 409
  - SMB(NTLM) authentication server,
    - configuring an 199
  - SNMP 242
  - SNMP Configuration 364
  - SNMP configuration screens 362
  - SNMP, configuring 243
  - SNMPv1/v2 Community 364
  - SNMPv1/v2 or v3 OID 365
  - SNMPv1/v2 or v3 Permission 365
  - SNMPv1/v2 Source 365
  - SNMPv3 Password 365
  - SNMPv3 Username 365
  - software upgrade 160
  - software version, downloading a new 422
  - Source IP 373
  - Source IP field 223
  - Source Mask 373
  - Source Port 224, 374
  - Source, SNMP 245
  - static routes 248
  - Static Routes screens, OSD 378
  - status
    - LED 6
    - port 261
    - viewing port 261
  - Step 1 Network Settings 142
  - Step 2 Access 144
  - Step 3 System Log 149
  - steps in Wizard mode 142
  - Stop Bits, PPP configuration 252
  - stop cycling 311
  - storage temperature 429
  - Subnet Mask, Local 241
  - Subnet Mask, Remote 241
  - Sun Keyboard 356
  - sun keyboard equivalent hot keys 40
  - sun keyboard keys 324
  - Switch Next 385
  - Switch Previous 385
  - switch, power 12
  - SYN 224
  - SYN Flag 374
  - SysContact 244, 364
  - SysLocation 244, 364
  - syslog 214
  - Syslog Facility 355
  - syslog files for IPDUs, configuring creation
    - of alarms and 159, 160
  - syslog messages, facility numbers for 53
  - syslog screens 400
  - syslog servers 52
    - adding 150
    - deleting 150
    - prerequisites for logging to 52
  - syslogging for KVM ports and
    - specify message filtering, configuring 215
  - syslogging, enhanced 8
  - system 253
  - System Info 349
  - system info menu 414
  - system information, accessing 415
  - system information, viewing 260
- ## T
- T1 335
  - Tab 346
  - tab, Access window 310
  - tables, host 246
  - TACACS+ 194
  - TACACS+ authentication server,
    - configuring a 202
  - TacacsPlus 409

- Target 373, 379
- target drop-down list options 222
- target, log 227
- target, reject 228
- tasks
  - common 134
  - configuration 106
  - for redefining hot keys, summary of 41
  - related to accessing connected devices
    - 38
- TCP Flags 224
- TCP flags
  - ACK 224
  - Any 224
  - FIN 224
  - PSH 224
  - RST 224
  - Set 224
  - SYN 224
  - Unset 224
  - URG 224
- TCP Options 237
- TCP Port Viewer 357
- TCP ports 26
- TCP protocol fields 224
- TCP RDP Ports 357
- TCP Sequence 237
- TCP Viewer Ports 170
- tcp-reset 238
- temperature monitor 8, 263
- temperature sensor 263
- temperatures, monitoring 56
- terminal emulator
  - dialing in 343
  - setting up 342
- terminators, KVM 58
- time and date, NTP 255
- time and date, OSD 97
- Time screen 414
- time, GMT 255
- time, setting manually 254
- time/date 254
- Timeout 409
- timeout, resuming port connections 315
- Toggle Full Screen 333
- Triple Data Encryption Standard 190
- Type of user 395
- type, connection 300
- types of access to ports 38
- types of KVM terminators 58
- types of ports 9
- types of users 20
- typographical conventions xxxi

## U

- u-boot monitor mode 424, 425, 426
- udp protocol fields 225
- Unit boot from 258
- Unset 224
- Up / Down 346
- upgrading
  - Cyclades pathname 274
  - firmware 272, 275
  - firmware AlterPath PM 161
  - KVM Expander microcontroller code 66
  - microcode 276
  - resetting microcode after 279
  - software 160
- URG 224
- URG Flag 375
- User 408
- user
  - add 145, 182
  - delete 147
  - log in as regular 286
- user (KVM over IP) sessions, configuring IP
  - 172
- User 1

## Index

- connection 414
- sessions, configuring 171
- User 1 port, connecting 85
- User 2
  - connection 414
  - sessions, configuring 171
- user access 67
  - remote and local 168
- User Database Enter the username 395
- User Name field 183
- user or group
  - assigning KVM port access 186
  - deleting a 184
- user password, changing a 184
- user station screens, OSD 382
- users
  - local user and IP 168
  - managing power outlets 158
  - of connected servers 38
  - power management for regular 288
  - simultaneous 4
  - types of 20
  - Web Manager for regular 284
- Users & Groups form 181
- Users and Groups screens, OSD 393
- Users Manager form 157

## V

- VCCI 430
- Version 414
- Video 385
- Viewer Options 333
- Viewer options, setting AlterPath 334
- Viewer settings, AlterPath 332
- viewing
  - active sessions information 280
  - and reset IPDU information 157
  - connected port information 310, 325

- general information 260
- in-band connections 296
- IPDUs info 156
- KVM connections 294
- port status 261
- system information 260
- VPN 54, 238
- VPN configuration screens 366
- VPN, configuring 239

## W

- Watchdog Timer 258
- changing admin's default password 100
- Web Manager 24
  - access without direct connection 102
  - completing configuration using the 99
  - Connect to Server form 304
  - connecting to servers through the 304
  - for regular users 284
  - IPDU Power Management forms 45
  - logging as as a regular user 286
  - logging as as admin 138
  - login screen 297
  - navigation conventions xxxii
  - prerequisites for logging into 286
  - prerequisites for using 25
  - Users & Groups form 181
  - Users Manager form 157
  - using a dynamic IP address 103
  - using the default IP address 102
- Web Manager, logging into the 138
- what's new in KVM/net Plus 4
- wiz command
  - apply network parameters 89
  - configure network parameters 87, 88
- wiz command, configuring basic networking 87
- Wizard mode 141

Access (Step 1) 144  
Network Settings(Step 2) 142  
procedures in 142  
steps in 142  
System Log (Step 3) 149

**Y**  
yMax Value 266  
yMin Value 266

