

Owner's Manual

NetDirector™ 1U Rackmount KVM Switches with IP Access

Models: B022-U08-IP, B022-U16-IP

PROTECT YOUR INVESTMENT!

Register your product for quicker service and ultimate peace of mind.

You could also win an ISOBAR6ULTRA surge protector—a \$50 value!

www.tripplite.com/warranty



1111 W. 35th Street, Chicago, IL 60609 USA • www.tripplite.com/support

Copyright © 2015 Tripp Lite. All rights reserved. All trademarks are the property of their respective owners.

Table of Contents

1. FCC Information	3	6.5 Logging Into the KVM over IP	16
2. User Notice	3	6.5.1 Logging In via Web Browser	16
3. Package Contents	3	6.5.2 Logging In via the AP Windows Client	17
4. Introduction	3	6.5.3 Logging In via the AP Java Client	18
4.1 Features	3	6.6 Web Browser and Non-Browser Remote Port Access	18
4.2 System Requirements	4	6.6.1 Port Access via Remote OSD	19
4.2.1 External Console	4	6.6.2 Port Access via Remote OSD Toolbar	19
4.2.2 Computers	4	6.6.3 Mouse Synchronization	20
4.2.3 Remote Console	4	6.6.4 Remote Auto Scan	21
4.2.4 Supported Browsers	4	6.6.5 Panel Array Mode	21
4.2.5 Custom KVM Cable Kits	4	6.6.6 Remote Control Panel	22
4.2.6 Operating Systems	4	7. Administration	25
4.3 Components	5	7.1 Local Console OSD	26
4.3.1 Front View	5	7.1.1 Local Console OSD F2 LIST Function	26
4.3.2 Rear View	5	7.1.2 Local Console OSD F3 Settings (SET) Page	26
5. Installation	6	7.1.3 Local Console OSD F4 Administration (ADM) Page	28
5.1 General Safety Instructions	6	7.1.4 Local Console Firmware Upgrade	29
5.2 Rack Mounting Instructions	7	7.2 Remote OSD	30
5.3 Grounding	7	7.2.1 Remote OSD List Drop-Down	30
5.4 Installation	7	7.2.2 Remote OSD Configuration Tab	31
5.5 Network Setup-IP Address Configuration	8	7.2.3 Remote OSD Administration Tab	31
5.5.1 Local Console	8	7.3 Web Management Interface	42
5.5.2 IP Installer	8	7.3.1 General Information	42
5.5.3 Browser	9	7.3.2 Network	43
5.5.4 Non-Browser Clients	10	7.3.3 Security	44
6. KVM Operation	12	7.3.4 ANMS	45
6.1 Sharing USB Peripheral Devices	12	7.3.5 User Management	51
6.2 Powering Off and Restarting	12	7.3.6 Customization	51
6.3 Local Console Login	12	7.3.7 Maintenance	53
6.4 Local Console Port Access	13	7.3.8 Log	53
6.4.1 Local Console OSD Invocation Sequence	13	7.4 Log Server	54
6.4.2 Local Console OSD Navigation	13	8. Specifications	57
6.4.3 Local Console OSD Main Screen Headings	13	8.1 OSD Default Settings	58
6.4.4 Local Console OSD F1 GOTO Function	13	8.2 Keyboard Emulation	58
6.4.5 Local Console OSD F5 Skip Function	13	9. Warranty & Product Registration	59
6.4.6 Local Console OSD F6 Broadcast Mode (BRC)	14		
6.4.7 Local Console OSD F7 Auto Scan Function	14		
6.4.8 Local Console OSD F8 Logout Function	14		
6.4.9 Local Console Pushbuttons	14		
6.4.10 Local Console Hotkey Commands	14		

1. FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

2. User Notice

All information, documentation and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed "as is." Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

3. Package Contents

This package consists of:

- B022-U08-IP or B022-U16-IP KVM Switch
- 6 ft. USB/PS2 Combo KVM Cable Kits (x2)
- USB/PS2 Combo Console Cable Kit
- RJ11 to DB9 Firmware Upgrade Cable
- Rackmount Hardware
- External Power Supply
- Rubber Feet
- CD with Owner's Manual, Quick Start Guide and Device Files
- Quick Start Guide

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices in the installation.

4. Introduction



4.1 Features

- 1U Rackmount KVM Switch with built-in IP access.
- Connect either USB or PS/2 computers using P778-Series USB/PS2 Combo KVM Cable Kits – no need for separate cable kits.
- Control up to 8 (B022-U08-IP) or 16 (B022-U16-IP) computers on a single KVM switch.
- Remotely access computers via LAN, WAN or Internet via the Windows™ or Java browser clients.
- AP Windows and Java clients allow the KVM to be remotely accessed via the network without going through a browser.
- External USB 1.1 port allows USB peripheral devices to be shared amongst connected computers.
- Grayscale feature allows you to view remote sessions in black and white, reducing the amount of data traveling over the network and improving keyboard/mouse response time over IP.
- Web management interface, OSD and toolbars provide convenient, user-friendly operation.
- 3-level security (Admin, User and Select) – up to 64 accounts can be created.
- Panel Array Mode – remotely monitor multiple ports at the same time.
- Message board feature allows users who are logged in at the same time to communicate with each other and manage port access.
- CD includes a Windows-based log server that records events on the installation and writes them to a searchable database.
- Supports RADIUS and LDAP/S authentication.
- Flash firmware upgradable via network and included firmware upgrade cable.
- Supports both IPv4 and IPv6.
- Supports Link Local IPv6 Address and IPv6 Stateless Auto configuration protocol.
- Web Management Interface, Remote OSD and Local OSD can be displayed in English, Spanish, French, German and Japanese.
- Advanced encryption technologies: 128-bit SSL, 128-bit RC4, 1024-bit RSA, 56-bit DES, 256-bit AES, 168-bit 3DES.
- Video resolutions up to 2048 x 1536, DDC2B are supported at the local console. Video resolutions up to 1600 x 1200 @ 60Hz, 24-bit color depth are supported at the remote console.

4. Introduction *(continued)*

4.2 System Requirements

4.2.1 External Console

- A VGA, SVGA or MultiSync monitor capable of displaying the highest resolution provided by any computer in the installation.
- PS/2 or USB keyboard and mouse.

4.2.2 Computers

The following equipment must be installed on each computer:

- A VGA, SVGA or MultiSync video graphics card with an HD15 port.

Either:

- PS/2 mouse and keyboard ports (6-pin Mini-DIN).
- USB port.

4.2.3 Remote Console

- For best results, computers that remotely access the KVM switch should have at least a Pentium III 1 GHz processor.
- Users who want to access the KVM switch with the Windows client must have DirectX 8.0 or higher installed. DirectX is available for free download from Microsoft's Website: <http://www.microsoft.com/downloads>.
- Users who want to access the KVM switch with the Java client must have Sun's Java 6 (update 3 or higher) runtime environment installed. Java is available for free download from the Sun Java Website: <http://java.com>.
- For best results, a network transfer speed of at least 128 Kbps is recommended.
- Browsers must support 128-bit data encryption.
- To run the Log Server, you must have the Microsoft Jet OLEDB 4.0 (or higher) driver installed.

4.2.4 Supported Browsers

Browser	Versions Supported
Internet Explorer	6 and higher
Firefox	1.5 and higher
Mozilla	1.7 and higher
Safari	4.0 and higher
Opera	9.0 and higher
Netscape	8.1 and higher

4.2.5 Custom KVM Cable Kits

The KVM switch uses custom P778-Series USB/PS2 Combo KVM Cable Kits, which can be used to connect to a computer with either USB or PS/2 connectors. One cable kit is required for each connected computer.

4.2.6 Operating Systems

Supported operating systems are shown in the table, below:

Operating System	Versions Supported
Windows	2000 and higher
Linux RedHat	7.1 and higher
Linux Fedora	Core 5 and higher
Linux SuSE	9.0 and higher
Linux Mandriva (Mandrake)	9.0 and higher
UNIX AIX	3.51 and higher

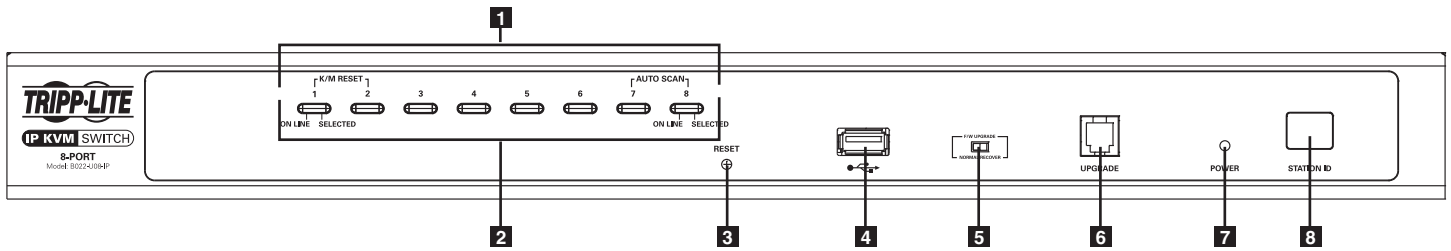
Operating System	Versions Supported
UNIX Free BSD	3.51 and higher
UNIX Sun	Solaris 8 and higher
Novell Netware	5.0 and higher
Mac	OS 9 and higher
DOS	6.2 and higher

4. Introduction *(continued)*

4.3 Components

4.3.1 Front View

Note: The diagram below shows the B022-U08-IP. The B022-U16-IP will be the same, except for the number of KVM ports and KVM pushbuttons. Also, an Auto Scan can be initiated on the B022-U16-IP by pressing pushbuttons 15 and 16 instead of 7 and 8.



1 Port Selection Pushbuttons: These buttons toggle between the computers attached to the corresponding KVM ports.

- Simultaneously pressing and holding buttons 1 and 2 for three seconds will perform a keyboard / mouse reset.
- Simultaneously pressing and holding buttons 7 and 8 (for B022-U08-IP) or 15 and 16 (for B022-U16-IP) for three seconds will initiate an Auto Scan.

2 Port LEDs: The Port LEDs are built into the Port Selection Pushbuttons.

- An Online LED on the left side of the pushbutton will illuminate Orange to indicate that a powered-on computer is connected to the corresponding port.
- A Selected LED on the right side of the pushbutton will illuminate Green to indicate that the corresponding port has the focus of the KVM.

3 Reset Button: Press this recessed button with a thin object to perform a system reset.

4 USB Peripheral Port: A USB 1.1 port is provided for the sharing of USB peripherals among connected computers (e.g. flash drive, CD-ROM drive, etc.).

Note: USB peripherals can only be shared among computers that are connected to the KVM switch via the USB connectors on the P778-Series USB/PS2 Combo KVM Cable Kit.

5 Firmware Upgrade Switch: During a firmware upgrade, as well as normal operation, this switch should be in the NORMAL position. If a firmware upgrade does not perform successfully, this switch is flipped to the RECOVER position during the firmware upgrade recovery process (See the Firmware Upgrade section of this manual for details).

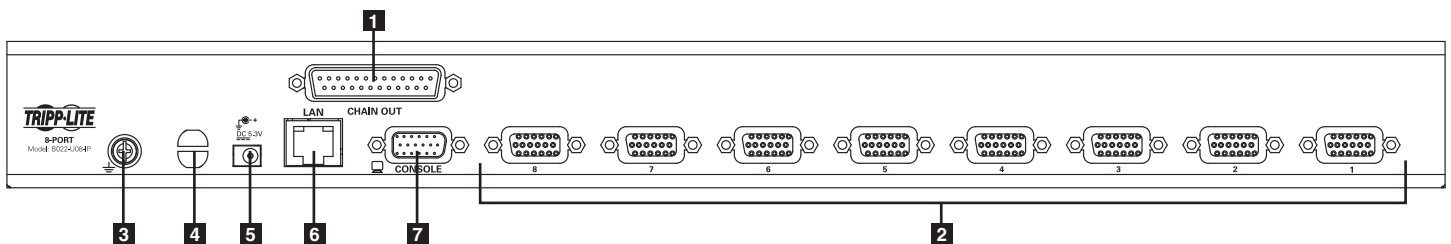
6 Firmware Upgrade Port: The RJ11 connector on the included firmware upgrade cable connects to the KVM switch here.

7 Power LED: The Power LED illuminates blue to indicate the unit is receiving power.

8 Station ID LED: The Station ID LED will display the number of the station that currently has the console's focus.

4.3.2 Rear View

Note: The diagram below shows the B022-U08-IP. The B022-U16-IP will be the same, except for the number of KVM ports.



1 Daisy-chain-Out Port

2 KVM Ports: The custom wired KVM cable kits that connect to the computers plug in here.

3 Grounding Terminal: The wire (user provided) used to ground the unit connects to the KVM here.

4 Cable Tie Slot: A cable tie can be routed through this slot in order to tie the connected cables together for organizational purposes.

5 Power Jack: The included power supply connects to the KVM here.

6 LAN Port: The cable that connects the KVM switch to a LAN, WAN or Internet plugs in here.

7 Console Port: The included USB/PS2 Combo Console Cable Kit connects to the KVM switch here, allowing you to attach a VGA monitor and USB or PS/2 keyboard/mouse.

5. Installation

5.1 General Safety Instructions



- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built-in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- This device is designed for IT power distribution systems with up to 230V phase-to-phase voltage.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- Consideration should be given to the connection of equipment to the supply circuit, and what effect overloading the supply circuit might have on overcurrent protection and supply wiring.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a Tripp Lite Surge Suppressor, Line Conditioner or Uninterruptible Power Supply (UPS).
- Position system cables and power cables carefully; be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.

- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair:
 - The power cord or plug has become damaged or frayed.
 - Liquid has been spilled into the device.
 - The device has been exposed to rain or water.
 - The device has been dropped, or the cabinet has been damaged.
 - The device exhibits a distinct change in performance, indicating a need for service.
 - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- Use of this equipment in life support applications where failure of this equipment can reasonably be expected to cause the failure of the life support equipment or to significantly affect its safety or effectiveness is not recommended. Do not use this equipment in the presence of a flammable anesthetic mixture with air, oxygen or nitrous oxide.

Rack Mounting Safety Instructions

- The ambient operating temperature in the rack may be an issue and is dependent upon the rack load and ventilation. When installing in a closed or multi-unit rack assembly, make sure that the temperature will not exceed the maximum rated ambient temperature.
- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Always load the rack so that a hazardous condition is not created due to uneven loading.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80% of the branch circuit rating.
- Ensure that proper airflow is provided to devices in the rack.
- Do not step on or stand on any device when servicing other devices in a rack.
- Do not connect the RJ11 connector marked "Upgrade" to a public telecommunication network.
- **Caution!** Slide/Rail (LCD KVM) mounted equipment is not to be used as a shelf or a work space.



CAUTION!
Slide/rail-mounted
equipment is not to be
used as a shelf
or a workspace.

5. Installation *(continued)*

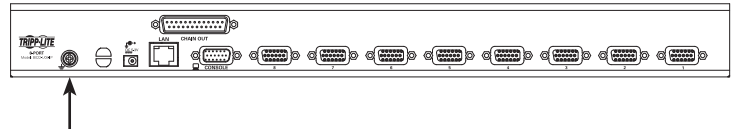
5.2 Rack Mounting Instructions

Standard Rack Mounting

1. Depending on whether you want to mount the KVM switch to the front or back of the rack, attach the included rackmount brackets to the front or rear sides of the KVM switch.
2. Using user-supplied screws, mount the rackmount brackets of the KVM switch to the rack.

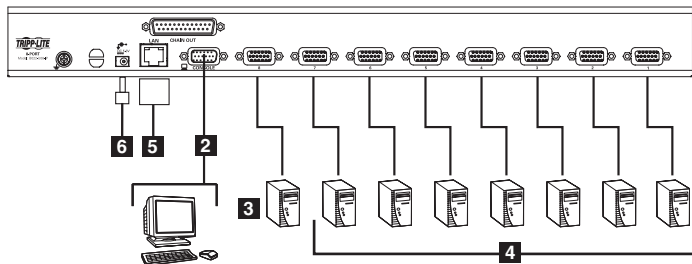
5.3 Grounding

To prevent damage to your installation, it is important that all devices are properly grounded. Using a user-supplied grounding wire, ground the KVM switch by connecting one end of the wire to the grounding terminal on the unit, and the other end of the wire to a suitably grounded object.



5.4 Installation

To install your KVM switch, refer to the following steps and installation diagram.



- 1 Power OFF all computers that are being connected to the KVM switch.
- 2 Add an external console to the KVM by connecting the included USB/PS2 console cable kit to the console port on the back of the unit, and then connecting an external monitor (HD15), keyboard (USB or PS/2) and mouse (USB or PS/2) to the connectors on the cable kit.

- 3 Connect a P778-Series USB/PS2 Combo KVM Cable Kit between an available KVM port on the back of the unit and a computer/server. P778-Series Cable Kits allow you to connect to a computer with either USB or PS/2* keyboard/mouse ports, without the need for separate cables. *Note: The distance between the KVM and the connected computer must not exceed 33 ft. (10 m).*
- 4 Repeat step 3 for each additional computer you wish to connect.
- 5 Connect the LAN port on the back of the unit to the network using Cat5e/6 cabling.
- 6 Connect the included external power supply to the KVM switch, and then plug it into a Tripp Lite Surge Suppressor, PDU or Uninterruptible Power Supply (UPS).
- 7 After the KVM switch powers up, power ON the connected computers.

*When connecting to computers using the PS/2 connectors of a P778-Series Cable Kit, the **Mouse Sync Mode** setting must be set to **Manual** in order to access the computer over IP. If **Mouse Sync Mode** is set to **Automatic**, you will not have mouse functionality when accessing that computer over IP. This setting is set to **Manual** by default.

5. Installation *(continued)*

5.5 Network Setup-IP Address Configuration

In order to configure a fixed IP address, you will need to access the KVM switch in one of four ways; *Local Console*, *IP Installer*, *Browser* or *Non-Browser Clients*.

5.5.1 Local Console

Note: The local console OSD only allows you to configure IPv4 network settings. For IPv6, access the Web Management Interface or Remote Session OSD.

- When accessing the KVM switch for the first time, a prompt will appear asking for a *Username and Password*. The default *Username* is **administrator**, and the default *Password* is **password**. For security purposes, it is strongly recommended that you change the username and password on this account to something unique. When you have entered your username and password, the OSD will appear with the following page displayed.
- Press the **[F4]** key to bring up the OSD Admin page.
- In the OSD Admin page, highlight **SET IP ADDRESS** and press the **[Enter]** key.
- DHCP** – The first field allows you to enable or disable DHCP. When enabled, the KVM is assigned an IP address by the DHCP server. This setting is enabled by default. To disable the **DHCP** setting and set up a fixed IP address, press the **[Spacebar]** key. Once the DHCP is disabled, you will be allowed to edit the remaining fields in the SET IP ADDRESS screen.
- In the remaining fields, enter in the IP address, subnet mask and default gateway you want to assign to the KVM switch.
- Press the **[Esc]** key to exit the **SET IP ADDRESS** screen, and to pull up a prompt asking if you wish to save the settings you just entered. If you do not wish to save the settings, press the **[N]** key. If you do wish to save the settings, press the **[Y]** key. Upon pressing the **[Y]** key, the settings will be saved and the KVM will be reset.

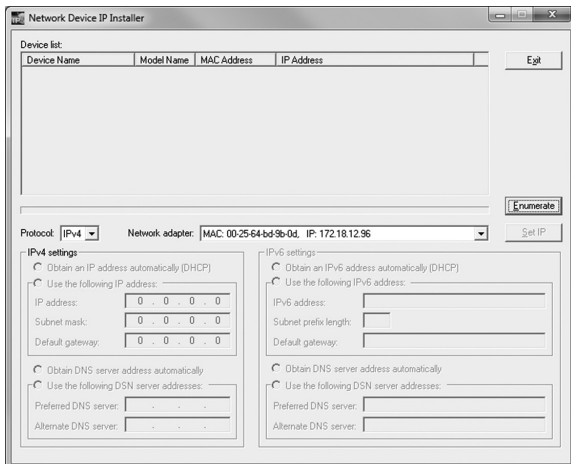
F1:GOTO	F3:SET	F5:SKP	F7:SCAN	X
F2:LIST	F4:ADM	F6:BRC	F8:LOUT	zZ
ADMINISTRATOR				
LIST:ALL				
SN.PN	QV	X	NAME	
02 • 14			ABC COMP1	▲
02 • 15	◀	X	ABC COMP2	▲
02 • 16		X	ABC COMP3	
03 • 01			WEB SERVER 1	
03 • 02			WEB SERVER 2	
03 • 03	◀	X	FAX SERVER 1	
03 • 04		X	FAX SERVER 2	
03 • 05	◀	X	MAIL SERVER 1	▼

5.5.2 IP Installer

The CD that comes with the product includes a Windows-based *IP Installer* utility that can be used to obtain and edit the IP address assigned to the KVM. To use the *IP Installer* utility, the computer you are using must be running a Windows operating system, and must be on the same network as the KVM. Also, the *IP Installer* setting in the *Network* page of the Web Management Interface must be set to *Enabled*, which it is by default (see the *Network* settings section in this manual for details).

Note: The IP Installer settings can only be accessed via the browser-based Web Management Interface. They are not accessible in the Remote OSD.

- Save the *IP Installer.exe* file from the CD to a desired location on a computer that is on the same network as the KVM.
- Locate the *IP Installer.exe* file that you just saved and double-click on it. A screen similar to the one below will appear:



- Select your KVM from the *Device List*. **Note:** If the list is empty, or your device doesn't appear, click the *Enumerate* button to refresh the *Device List*. If there is more than one device in the list, use the *MAC address* on the bottom of your unit to determine the desired device.
- To assign a fixed IP address, check the *Use the following IP address* checkbox and fill in the *IP Address*, *Subnet Mask*, and *Default Gateway* fields with information appropriate for your network (IPv4 or IPv6).
- Click the *Set IP* button to apply the changes to the unit. The new IP address will appear in the *Device List*.
- Click the *Exit* button to exit the *IP Installer* utility.

5. Installation (continued)

5.5.3 Browser

By default, the KVM switch is set to have an IP address assigned automatically via DHCP server. If this is the case, you will need to obtain the IP address from your network administrator. If connected to a network without a DHCP server, it boots with a default IP address. The default IPv4 and IPv6 addresses can be found on the sticker on the bottom of the unit.

1. Enter the unit's IP address into your web browser.
2. You may be prompted by a screen stating that there is a problem with this website's security certificate. Click on the option to continue to the website anyway. (See *Web Browser Login* section for details on installing the security certificate)
3. You will be brought to a login page. Enter the default Username (*administrator*), and the default Password (*password*). The Web Management Interface will open upon entering the Username and Password.
4. Click on the *Network* icon at the top of the page to bring up the *Network* settings page.
5. By default, the *Obtain IP address automatically [DHCP]* checkbox is checked. To set a fixed IP address, check the *Set IP address manually [Fixed IP]* check box in the IPv4 or IPv6 settings section, depending on your network.
6. The *IP Address*, *Subnet Mask* and *Default Gateway* fields will be activated upon checking the *Set IP address manually [Fixed IP]* checkbox. Fill in these fields with information appropriate for your network.
7. As with the IP Address settings, the DNS Server settings can be obtained automatically or assigned manually. To manually enter these settings, check the *Set DNS server address manually* checkbox and fill in the *Preferred DNS server* and *Alternate DNS server* fields with information appropriate for your network. **Note:** The Alternate DNS server field is optional.
8. When you have entered the IP Address and DNS Server settings, click the *Apply* button. Clicking the *Apply* button will automatically check the *Reset on exit* checkbox located in the *Customization* page of the Web Management Interface. When you log out, the unit will be reset and your network changes will be applied.

Access Ports

Program: 9000 HTTP: 80 HTTPS: 443

IPv4 Configuration

Obtain an IP address automatically [DHCP]

Set IP address manually [Fixed IP]

IP Address: 192.168.1.180

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Obtain DNS server address automatically

Set DNS server address manually

Preferred DNS server: 192.168.1.2

Alternate DNS server: 192.168.1.3

IPv6 Configuration

Obtain an IP address automatically [DHCP]

Set IP address manually [Fixed IP]

IP Address: fe80::210:74ff:fe67:20c4

Prefix Length: 10

Default Gateway:

Obtain DNS server address automatically

Set DNS server address manually

Preferred DNS server:

Alternate DNS server:

IP Installer Settings

Enabled View Only Disabled

Apply

See the *Network Settings* section in this manual for complete information on the rest of the settings in this page.

5. Installation *(continued)*

5.5.4 Non-Browser Clients

The CD that comes with the product includes Windows and Java client applications that allow you to remotely access the KVM without using a web browser. The applications function the same, but the Windows client is designed for Windows computers, whereas the Java client is designed for either Windows or non-Windows computers. When accessed from a computer that is on the same network as the KVM, the client will search the network for the device and display it in a device list for you to access. If accessed from a computer that is not on the same network as the KVM, you must obtain the IP address from your network administrator and manually enter it into the client. (See the *Browser* section above for information on obtaining the IP address) To use the Windows or Java client to assign a fixed IP address, follow the steps below.

1. Save the Windows or Java client from the CD to a desired location on your computer. Double-click the file to open it.
2. When accessing the Windows client for the first time, it will need to be installed on your computer. Follow the installation prompts that appear. Once installed, a Windows client icon will appear on your desktop.
3. When accessing either the Windows or the Java client for the first time, you will be prompted to enter the product serial number, which can be found on the CD that came with the unit. Once entered, you will not be prompted for it again. The non-browser client connection screen appears.

Server List

Name	IP Address
------	------------

Server:
IP: 12.233.90.229
Port: 9000

Login Logout Remote View Change Password

4. If you are on the same network as the KVM, the client will locate it and display it in the *Device List*. In this case, highlight the unit in the *Device List* and click the *Login* button. If you are not on the same network as the unit, it will not be displayed in the list. You must manually enter the IP address in the IP Address field, and then click the *Login* button.
5. Upon clicking the *Login* button, you will be prompted to enter in a Username and Password. Enter the default Username (*administrator*), and the default Password (*password*). The *Logout* button, and the *Remote View* and *Change Password* buttons on the right of the non-browser client main page will be activated. The *Login* button will be deactivated.

Server List

Name	IP Address
------	------------

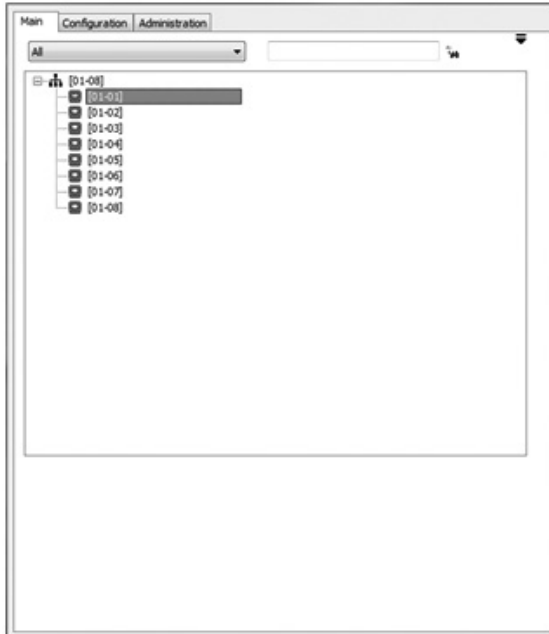
Server:
IP: 12.233.90.229
Port: 9000

Login Logout Remote View Change Password

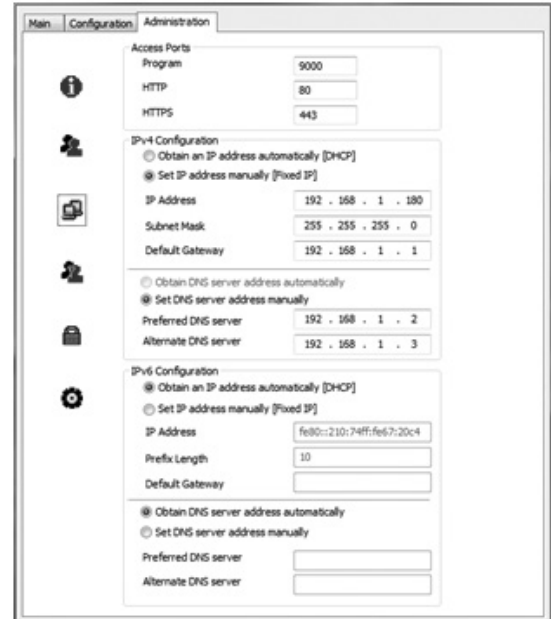
5. Installation *(continued)*

5.5.4 Non-Browser Clients *(continued)*

- Click the *Remote View* button to initiate a remote session, which will open with the remote OSD displayed. The remote OSD contains most of the features that are contained in the Web Management Interface, but it is presented in a different format (See the *Remote OSD* section for details on the difference between it and the Web Management Interface).



- Click on the *Administration* tab at the top of the screen. On this page, click on the *Network Icon* to pull up the *Network* page. From here, a fixed IP address can be assigned in the same way as when using a web browser (See steps 5 through 8 in the *Browser* section).



6. KVM Operation

Computers connected to the KVM can be accessed via the local console or over IP. This chapter discusses the basic operation of the KVM switch, both locally and remotely.

6.1 Sharing USB Peripheral Devices

The USB 1.1 port on the front panel of the KVM switch can be used to share USB peripherals between connected computers. Simply connect a USB device to this port, and any connected computer you switch to will have access to the device. The USB peripheral sharing functionality works the same whether you are accessing the connected computers via the local console or over IP.

Note: The following limitations apply to the USB peripheral port:

1. This port serves as a 1-port USB 1.1 hub; USB 2.0 devices can be connected but will not function at USB 2.0 speeds.
2. USB peripherals can only be shared among computers that are connected to the KVM switch via the USB connectors on the P778-Series USB/PS2 Combo KVM Cable Kit.
3. USB peripherals can only be shared among computers that are connected to the KVM switch that the USB peripheral is plugged into. If a USB peripheral is plugged into the USB 1.1 port of the third KVM switch in a daisy-chain installation, only computers connected to that KVM can access the USB peripheral; computers connected to any other KVM in the installation will not be able to access the USB peripheral.
4. When accessing a USB peripheral on a connected computer, it is recommended that you properly eject the device before switching to another computer. When switching computers, the device is automatically disconnected from the previous computer and connected to the next, as if it was manually unplugged from a USB port on one computer and then plugged into the USB port of another computer.

6.2 Powering Off and Restarting

If it becomes necessary to power off the KVM switch, follow this procedure:

1. Shut down all computers connected to the KVM switch. If you are powering off multiple computers in a daisy-chain installation, shut down all computers connected to each KVM switch you are powering off.

Note: It is necessary to unplug any computers that have the Keyboard Power On function. If left on, the KVM switch will continue to receive power via these computers.

2. Starting with the first KVM in the installation, unplug the KVM switch from its power source. Power OFF and unplug each additional KVM switch in succession.
3. Wait 10 seconds and then plug the KVM switch, starting with the first station, back into its power source.
4. Once the first station KVM switch has ascertained its position in the daisy-chain, power ON and plug in the next KVM switch in the installation. Follow this procedure for each additional KVM switch in the installation.
5. Once all KVM switches in the installation have been powered back ON, turn on the power to all connected computers.

6.3 Local Console Login

When accessing the console KVM switch for the first time, a prompt will appear asking for a *username* and *password*. The default *username* is **administrator**, and the default *password* is **password**. For security purposes, it is strongly recommended that you change the username and password on this account to something unique. Once the KVM has been set up and user accounts have been created, the login prompt will only appear when a user logs out of the KVM. When you have entered your username and password, the OSD will appear with the following page displayed.



SN	PN	QV	X	NAME
02	14			ABC COMP1
02	15	◀	X	ABC COMP2
02	16		X	ABC COMP3
03	01			WEB SERVER 1
03	02			WEB SERVER 2
03	03	◀	X	FAX SERVER 1
03	04		X	FAX SERVER 2
03	05	◀	X	MAILSERVER 1

Note: 1. The screenshot depicts the Administrator's Main Screen. The User Main Screen does not have the F4 and F6 functions, since they can't be accessed by ordinary Users and are reserved for the Administrator.

2. OSD always starts in List view, with the highlight bar at the same position it was when the OSD was last closed.
3. Only the ports that have been set accessible by the Administrator for the currently logged in User are visible.
4. If the port list is collapsed into stations, simply click on the plus sign next to the desired station number, or highlight the desired station number and hit the [Enter] key.

6. KVM Operation *(continued)*

6.4 Local Console Port Access

Once logged into the KVM, you can access connected computers via the local console using the *Local Console OSD*, *Local Console Pushbuttons* or *Hotkey Commands*. The following sections describe all of the ways in which you can access connected computers via the local console.

6.4.1 Local Console OSD Invocation Sequence

Once logged into the KVM switch and accessing a connected computer, you will need to use one of two sequences to re-open the OSD Main Menu; [**Scroll Lock, Scroll Lock**] or [**Ctrl, Ctrl**]. The default OSD invocation sequence is [**Scroll Lock, Scroll Lock**].

6.4.2 Local Console OSD Navigation

When in the *Local Console OSD*, you can use your keyboard and mouse to access its features.

- To close out of the *Local Console OSD*, click the [**X**] at the upper right corner of the OSD or press the [**Esc**] key.
- To logout, press the [**F8**] key, click the **F8** at the top of the OSD, or click the **zZz** symbol in the upper right hand corner of the OSD.
- To move through the OSD list one line at a time, click the up and down triangle symbols (**▲**, **▼**) or use the [**↑**] and [**↓**] keyboard keys. If there are more entries than appear on the screen, the screen will scroll.
- To move up or down one screen at a time, click the Up and Down Arrow symbols (**↑**, **↓**), or use the [**Pg Up**] and [**Pg Dn**] keyboard keys. If there are more entries than appear on the screen, the screen will scroll.
- To activate a port, double-click it, or highlight it and press the [**Enter**] key. Once a port is accessed, the OSD will close and the screen of the computer connected to the port will be displayed.

6.4.3 Local Console OSD Main Screen Headings

SN	The Station Number of each KVM in the installation will be displayed in this column. The Station Number of each KVM switch will be displayed as an expandable folder, which can be expanded to show all of the KVM ports in the corresponding station, or collapsed to hide them.
PN	The port numbers of each KVM in the installation are displayed in this column. If the individual stations are collapsed, their port numbers will not be displayed.
QV	An arrow in this column indicates that the corresponding port is selected for Quick View scanning.
☀	A sun symbol in this column indicates that a computer is both connected to the corresponding port and powered ON.
NAME	If a port has been given a name, its name appears in this column.

6.4.4 Local Console OSD F1 GOTO Function

Click **F1** at the top of the OSD or press the [**F1**] key to activate the **GOTO** function. **GOTO** allows you to search the ports on the installation by keying in a *Name* or *Port ID*. As you type in a *Name* or *Port ID*, the OSD list will automatically display all ports in the installation that match your search terms. To access a port from the list, simply double-click on it or highlight it and press the [**Enter**] key. To exit **GOTO** mode and return to the OSD main page, press the [**Esc**] key.

- To search by *Name*, type [**1**] into the field that appears when the **GOTO** function is activated; a *Name* field will appear. Type in a name to display all accessible ports in the installation that match your entry.
- To search by *Port ID*, type [**2**] into the field that appears when the **GOTO** function is activated; a *Port ID* field will appear. Type in a port ID to display all accessible ports in the installation that match your entry.

6.4.5 Local Console OSD F5 Skip Function

Skip Mode allows connected computers to be accessed using the [**←**], [**→**], [**↑**] and [**↓**] keys on the keyboard. To invoke *Skip Mode* via the local console OSD, click **F5** at the top of the OSD or press the [**F5**] key. When invoked, the KVM displays the screen of the last selected port, with a left/right triangle symbol next to the port's port ID to signify it is being accessed in *Skip Mode*. The ports accessed in *Skip Mode* are determined by the *Scan Select* setting in the **F3 Set** page of the local console OSD. During *Skip Mode*, normal keyboard and mouse functionality is suspended. Keyboard functionality is limited to those keys mentioned in the table below. Mouse functionality is suspended altogether.

Key	Description
[←]	Skips from the currently selected port to the next accessible port prior to it.
[→]	Skips from the currently selected port to the next accessible port after it.
[↑]	Skips from the currently selected port to the last accessible port on the previous station.
[↓]	Skips from the currently selected port to the first accessible port on the next station.
[Esc]	Exits <i>Skip Mode</i> at the currently selected port.
[Spacebar]	Exits <i>Skip Mode</i> at the currently selected port.

6. KVM Operation (continued)

6.4.6 Local Console OSD F6 Broadcast Mode (BRC)

Broadcast Mode is an Administrator-ONLY function. Clicking the **F6** at the top of the OSD or pressing the [**F6**] key invokes *Broadcast Mode*. When this function is in effect, commands sent from the console are broadcast to all available computers on the installation. This function is particularly useful for operations that need to be performed on multiple computers, such as performing a system-wide shutdown, installing or upgrading software, etc. *Broadcast Mode* works in conjunction with the *F2 LIST* function. The *F2 LIST* function lets you select which ports will be displayed on the OSD main screen. When a command is broadcast, it is done only to the ports currently displayed on the OSD main screen.

- A speaker symbol appears before the Port ID Display to indicate *Broadcast Mode* is in effect.
- The mouse will not function while *Broadcast Mode* is in effect. You must exit *Broadcast Mode* in order to regain control of the mouse.
- To exit *Broadcast Mode*, invoke the OSD (with the OSD hotkey), and then click **F6** at the top of the OSD or press the [**F6**] key.

6.4.7 Local Console OSD F7 Auto Scan Function

Auto Scan Mode allows connected computers to be accessed automatically at set time intervals. To invoke *Auto Scan Mode* via the local console OSD, click **F7** at the top of the OSD or press the [**F7**] key. When invoked, the KVM begins scanning according to the *Scan Select* and *Scan Duration* settings in the **F3 Set** page of the local console OSD. During an auto scan, normal keyboard and mouse functionality is suspended. Keyboard functionality is limited to the [**Spacebar**] key (exits auto scan at the currently selected port), [**Esc**] key (exits auto scan at the currently selected port) and the [**P**] key (pauses auto scan at the currently selected port). Mouse functionality is suspended altogether.

6.4.8 Local Console OSD F8 Logout Function

To logout of the KVM switch, click on the **F8** at the top of the page or press the [**F8**] key. You will be prompted to confirm that you wish to logout. Press the [**Y**] key if yes, or the [**N**] key if no. When logged out, the *username* and *password* screen will appear, requiring a username and password to be entered to access the KVM.

6.4.9 Local Console Pushbuttons

In addition to using the local console OSD to access connected computers, you can access them using the KVM's pushbuttons. The KVM switch front panel includes pushbuttons for its ports only. Press a pushbutton to bring the KVM's focus to the corresponding port.

6.4.10 Local Console Hotkey Commands

When accessing a connected computer via the local console, you can use hotkey commands to operate the KVM switch instead of going back into the OSD. This chapter discusses the available hotkeys and their functions. Below is a list of the various hotkeys, broken up into those for port control and those that perform other functions.

Port Control Hotkeys

- Selecting the active port
- Auto Scan Mode port switching
- Skip Mode port switching

Other Hotkeys

- Computer keyboard and mouse reset
- Setting the Beeper
- Setting the Mode Invocation Sequence Hotkey
- Setting the OSD Hotkey
- Setting the Port Operating System
- Restoring the OSD default values

Invoking the Hotkey Mode

All hotkey operations begin by invoking *Hotkey Mode*. In order for *Hotkey Mode* to work, it must be activated in the KVM's OSD. By default, *Hotkey Mode* is enabled. There are two sequences that can be used to invoke *Hotkey Mode*, both of which are explained below. You can toggle between these two sequences using the OSD. The [**Num Lock**] and [-] Minus keys are the default invocation keys.

Num Lock and Minus (-) keys

1. Press and hold down the [**Num Lock**] key.
2. While the [**Num Lock**] key is held down, press and release the [-] Minus key.
3. After releasing the [-] Minus key, release the [**Num Lock**] key.

Control and F12 keys

1. Press and hold down the [**Ctrl**] key.
2. While the [**Ctrl**] key is held down, press and release the [**F12**] key.
3. After releasing the [**F12**] key, release the [**Ctrl**] key.

When Hotkey Mode has been invoked:

- The monitor goes blank and the hotkey command line is displayed. This is where you will enter in the hotkey commands described in this chapter.
- The [**Caps Lock**] and [**Scroll Lock**] keyboard LEDs will blink in succession.
- Ordinary keystrokes will be suspended until *Hotkey Mode* is exited. *Hotkey Mode* is exited once a hotkey command is performed, or by pressing the [**Esc**] or [**Spacebar**] keys.

Port ID Numbering

- Each CPU port in an installation is assigned a unique Port ID. The Port ID is made up of two parts, a *Station Number* and a *Port Number*.
- The *Station Number* is a two-digit number that identifies the switch's position in the daisy chain installation. This corresponds to the number displayed on the Station ID LED.

6. KVM Operation *(continued)*

6.4.10 Local Console Hotkey Commands *(continued)*

- The *Port Number* is a two-digit number which identifies the port number of the KVM switch that the computer is connected to.
- The *Station Number* precedes the *Port Number*.
- Station and Port numbers are always 2 digits, so 1 - 9 becomes 01 - 09. For example, a computer attached to Port 7 of Station 15 has a Port ID of 15-07.

Selecting the Active Port

You can directly access a port by doing the following:

1. Invoke *Hotkey Mode*.
2. Enter the Port ID. The Port ID numbers appear on the command line as they are entered. To correct a mistake, use **[Backspace]** to erase the wrong number.
3. Press the **[Enter]** key; the KVM switches to the designated computer and you automatically exit *Hotkey Mode*.

Auto Scan Mode

When invoked, *Auto Scan Mode* monitors the connected computers automatically at regular intervals so that you don't have to manually switch between them. When in *Auto Scan Mode*, the KVM switch monitors the connected computers per the *Scan Select* and *Scan Duration* settings in the **F3 Set** page of the local console OSD. To invoke *Auto Scan Mode*, follow these steps:

1. Invoke *Hotkey Mode*.
2. Key in **[A]** and hit the **[Enter]** key. You automatically exit *Hotkey Mode* and enter *Auto Scan Mode*.
3. *Auto Scan Mode* can be paused at any time by pressing the **[P]** key or left-clicking the mouse. To resume scanning, press any key or left-click the mouse.
4. To exit *Auto Scan Mode*, press the **[Esc]** key or **[Spacebar]** key.

Note: While Auto Scan Mode is in effect, ordinary keyboard and mouse functions are suspended; only Auto Scan Mode compliant keystrokes and mouse clicks can be input. You must exit Auto Scan Mode in order to regain normal control of the console.

Skip Mode

Skip Mode allows connected computers to be accessed using the **[←]**, **[→]**, **[↑]** and **[↓]** keys on the keyboard. This manual version of *Auto Scan Mode* lets you dwell on a particular port for as long as you like. To invoke *Skip Mode*, follow these steps:

1. Invoke *Hotkey Mode*.
2. Press the **[←]**, **[→]**, **[↑]** or **[↓]** key.
3. After pressing one of the arrow keys, you automatically exit *Hotkey Mode* and enter *Skip Mode*. When in *Skip Mode*, you can switch ports as follows:
 - The **[←]** key skips from the current port to the first accessible port prior to it.
 - The **[→]** key skips from the current port to the first accessible port after it.
 - The **[↑]** key skips from the current port to the last accessible port of the previous station.
 - The **[↓]** key skips from the current port to the first accessible port of the next station.
4. To exit *Skip Mode*, press the **[Esc]** key.

Note:

1. *While Skip Mode is in effect, you can keep on skipping through ports until you exit.*
2. *During Skip Mode, ordinary keyboard and mouse functions are suspended—only Skip Mode compliant keystrokes can be input. You must exit Skip Mode in order to regain normal control of the console.*

Hotkey Beeper Control

To toggle the Beeper on and off, key in the following hotkey combination:

1. Invoke *Hotkey Mode*.
2. Key in **[B]**. After you press **[B]**, the Beeper toggles On or Off. The command line displays *Beeper On* or *Beeper Off* for one second; then the message disappears and you automatically exit *Hotkey Mode*.

Computer Keyboard/Mouse Reset

If the keyboard or mouse ceases to function for a particular port, you can perform a keyboard/mouse reset via the hotkey command below. This performs the same function as unplugging/re-plugging the keyboard and mouse on the connected computer. To perform a keyboard/mouse reset, do the following:

1. Invoke *Hotkey Mode*.
2. Press the **[F5]** key. After pressing the **[F5]** key, you exit *Hotkey Mode* and the KVM switch performs a keyboard/mouse reset for the currently selected computer. (This may take a few seconds to take affect.)

Hotkey Mode Invocation Sequence

The hotkey sequence to invoke *Hotkey Mode* can be toggled via hotkey command as well as the local console OSD. To toggle the invocation sequence between **[Num Lock, (-) Minus]** and **[Ctrl, F12]**, do the following:

1. Invoke *Hotkey Mode*.
2. Press the **[H]** key. After pressing the **[H]** key, the hotkey mode invocation sequence is changed and the text HOTKEY HAS BEEN CHANGED briefly appears on the monitor. *Hotkey Mode* is then exited and you regain normal operation of the KVM switch.

OSD Invocation Sequence

The hotkey sequence to invoke the OSD can be toggled via hotkey command as well as the local console OSD. This hotkey sets the invocation sequence for both the *Local Console OSD* and the *Remote OSD*. To toggle the invocation sequence between **[Scroll Lock, Scroll Lock]** and **[Ctrl, Ctrl]**, do the following:

1. Invoke *Hotkey Mode*.
2. Press the **[T]** key. After pressing the **[T]** key, the local console OSD invocation sequence is changed and the text HOTKEY HAS BEEN CHANGED briefly appears on the monitor. *Hotkey Mode* is then exited and you regain normal operation of the KVM switch.

Port OS Control

In addition to choosing the operating system for a connected port via the local console OSD, administrators can set the port operating system via hotkey command. To change a port's operating system via hotkey, do the following:

1. Invoke *Hotkey Mode*.
2. Key in **[Function]**, where **[Function]** represents one of the following:
 - a) **[F1]** – Sets the Operating System to Windows.
 - b) **[F2]** – Sets the Operating System to Mac.
 - c) **[F3]** – Sets the Operating System to Sun.

After pressing one of these keys, the operating system will be changed for the selected port and you will exit *Hotkey Mode*.

Restore Default Values

This Administrator-ONLY hotkey restores the KVM switch to its default values. To restore the default values via hotkey, do the following:

1. Invoke *Hotkey Mode*.
2. Press the **[R]** key.
3. Hit the **[Enter]** key. After hitting the **[Enter]** key, the text RESET TO DEFAULT SETTING is briefly displayed, and then *Hotkey Mode* is exited.

6. KVM Operation *(continued)*

6.4.10 Local Console Hotkey Commands *(continued)*

Hotkey Summary Table

Note: All of the hotkey commands in this table require Hotkey Mode to be invoked prior to implementing the hotkey command.

Hotkey Operation	Hotkey Command	Description
Selecting the active port	[Station ID], [Port ID], [Enter]	Switches the KVM focus to the Station and Port entered in this command. (See page 14 for details on Port ID numbering.)
Auto Scan Mode	[A], [Enter]	Invokes <i>Auto Scan Mode</i> . Press the [P] key at any time during an auto scan to pause on the currently selected computer. Press the [Esc] key or [Spacebar] key to exit <i>Auto Scan Mode</i> at the currently selected computer.
Hotkey beeper control	[B]	Toggles the beeper sound ON/OFF.
Port OS (Windows)	[F1]	<i>(Administrator-only hotkey)</i> Sets the OS of the currently selected port as Windows.
Port OS (Mac)	[F2]	<i>(Administrator-only hotkey)</i> Sets the OS of the currently selected port as Mac.
Port OS (Sun)	[F3]	<i>(Administrator-only hotkey)</i> Sets the OS of the currently selected port as Sun.
Computer keyboard/mouse reset	[F5]	Performs a keyboard/mouse reset for the currently selected computer.
Hotkey mode invocation sequence	[H]	Toggles the sequence to invoke <i>Hotkey Mode</i> between [Num Lock, (-) Minus] and [Ctrl, F12].
OSD invocation sequence	[T]	Toggles the sequence to invoke the OSD between [Scroll Lock, Scroll Lock] and [Ctrl, Ctrl]. Sets the invocation sequence for both the <i>Local Console OSD</i> and the <i>Remote OSD</i> .
Restore default values	[R], [Enter]	<i>(Administrator-only hotkey)</i> Restores the OSD to its default values. Restores both the <i>Local Console OSD</i> and the <i>Remote OSD</i> .
Skip Mode/Previous port	[←]	When typed into the hotkey command line, this key invokes <i>Skip Mode</i> . When in <i>Skip Mode</i> , this key switches KVM focus to the port prior to the currently selected port.
Skip Mode/Next port	[→]	When typed into the hotkey command line, this key invokes <i>Skip Mode</i> . When in <i>Skip Mode</i> , this key switches KVM focus to the port after the currently selected port.
Skip Mode/Previous station	[↑]	When typed into the hotkey command line, this key invokes <i>Skip Mode</i> . When in <i>Skip Mode</i> , this key switches KVM focus to the last port on the station prior to the currently selected port.
Skip Mode/ Next station	[↓]	When typed into the hotkey command line, this key invokes <i>Skip Mode</i> . When in <i>Skip Mode</i> , this key switches KVM focus to the first port on the station after the currently selected port.

6.5 Logging Into the KVM over IP

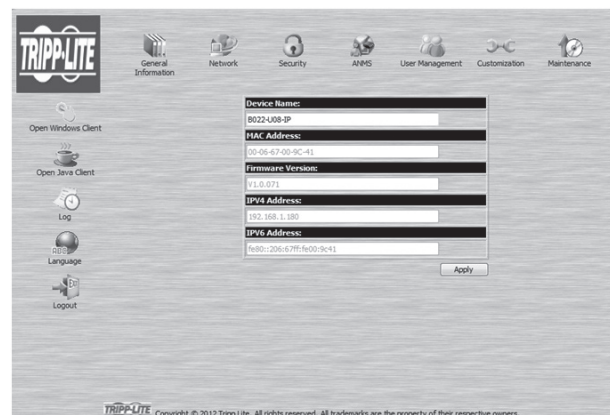
There are three methods that can be used to connect to the KVM switch over IP; *Web Browser*, *AP Windows Client* and *AP Java Client*.

6.5.1 Logging In via Web Browser

1. Open your web browser and type in the IP address of the KVM.
(See *Network Setup – IP Address Configuration* on page 8 for details on determining the KVMs IP address.)
2. A screen will appear asking you to provide a username and password.

Note: If you are first prompted by a screen that says the website's security certificate cannot be trusted, click on the link to proceed anyway; the certificate can be trusted.

3. If accessing the KVM for the first time, enter in the *username administrator* and the *password password*. For security purposes, it is strongly recommended that you change the username and password on this account to something unique. When you have entered your username and password, the KVM web interface will appear with the following page displayed:



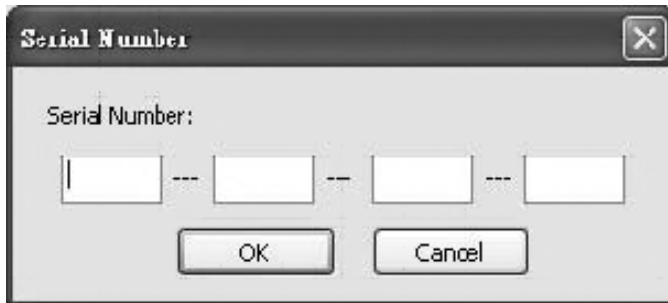
6. KVM Operation (continued)

6.5.2 Logging In via the AP Windows Client

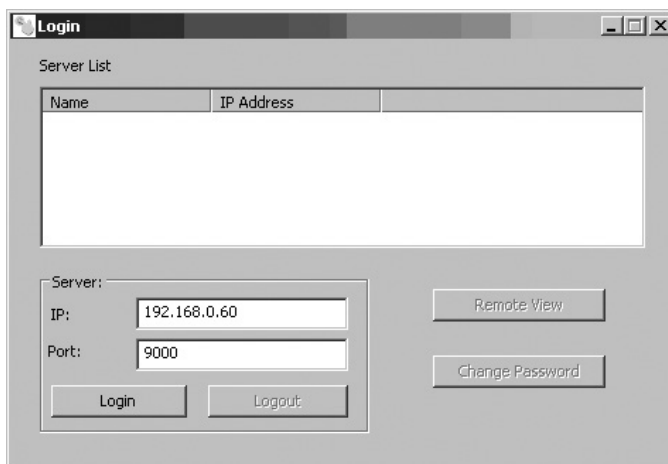
In the event you do not want to connect to the KVM switch via web browser, you can use the AP Windows Client located on the CD to provide non-browser access to the KVM switch via a Windows computer.

Note: The AP Windows Client requires that DirectX 8.0 or higher be installed on your computer.

1. Save the AP Windows Client from the CD to a desired location on your Windows computer.
2. Double-click on the file, and follow the installation instructions that follow.
3. When the installation is complete, an icon will be added to your desktop, and a program entry will be made in the Windows start menu. (*Start > All Programs > B022-U08-IP*) Double-click on the icon or select the program entry in the start menu to open the AP Windows Client.
4. If this is the first time that you are running the utility, a dialog box appears requesting you to input your serial number. The serial number can be found on the CD that comes with the KVM. Key in the serial number (5 characters per box), then click **OK**.

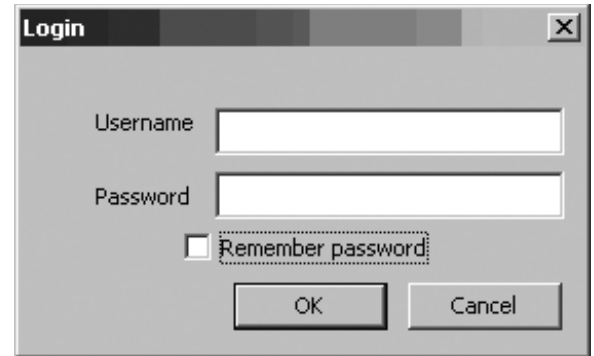


5. Upon entering the serial number, the AP Windows Client main screen appears.

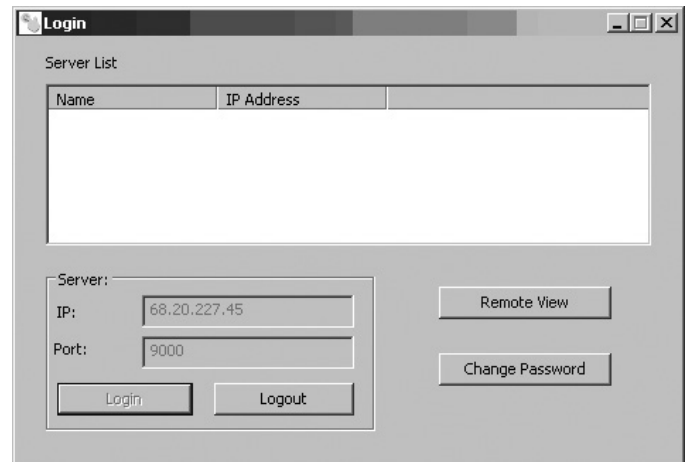


6. The AP Windows Client will search the network for any KVM switches and display their Model Name and IP Address in the main screen's *Server List*. If the KVM you wish to connect to is displayed in the list, highlight it and click the *Login* button. If not, type in the IP address and port number assigned to the desired KVM switch and click the *Login* button. *Note: The default port number assigned to the KVM is 9000.*

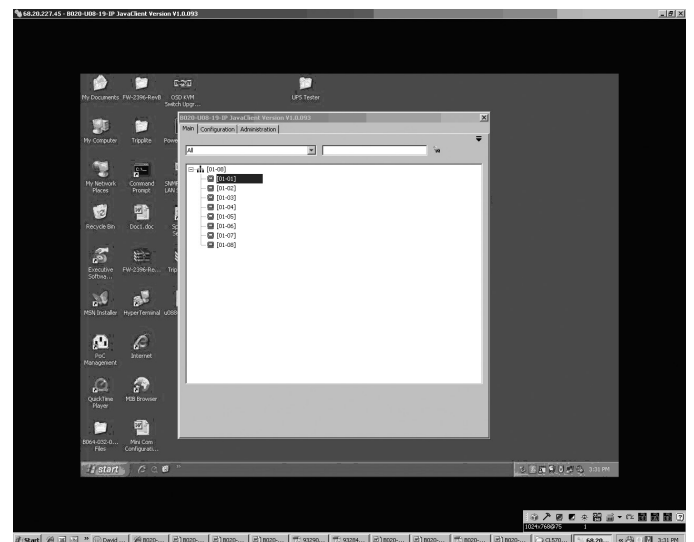
7. A prompt appears asking you to enter your username and password. If accessing the KVM for the first time, enter in the *username administrator* and the *password password*. For security purposes, it is strongly recommended that you change the username and password on this account to something unique.



8. When you have entered your username and password, the *Remote View* and *Change Password* buttons on the main screen become active. Click on the *Remote View* button to remotely connect to the KVM switch.



9. Upon clicking on the *Remote View* button, the screen of the first connected computer on the installation that you have access to is displayed, as well as the *Remote OSD*.



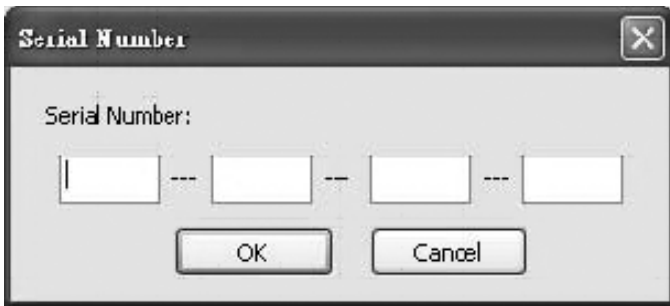
6. KVM Operation (continued)

6.5.3 Logging In via the AP Java Client

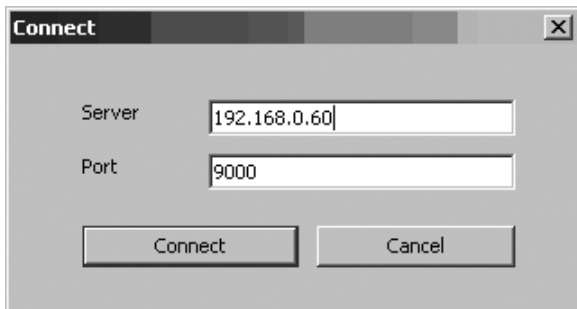
Computers not running Windows can use the AP Java Client located on the CD to provide non-browser access to the KVM switch.

Note: The AP Java Client requires that the Java Runtime Environment (JRE) be installed on your computer. The JRE is available for free download from the Java web site (<http://java.com>).

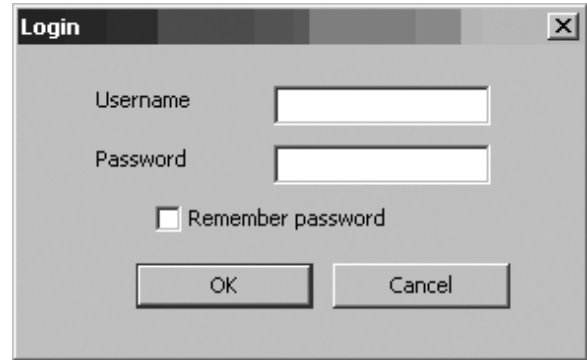
1. Save the AP Java Client from the CD to a desired location on your computer.
2. Double-click on the file you just saved. If this is the first time that you are running the utility, a dialog box appears requesting you to input your serial number. The serial number can be found on the CD that comes with the KVM. Key in the serial number (5 characters per box), then click **OK**.



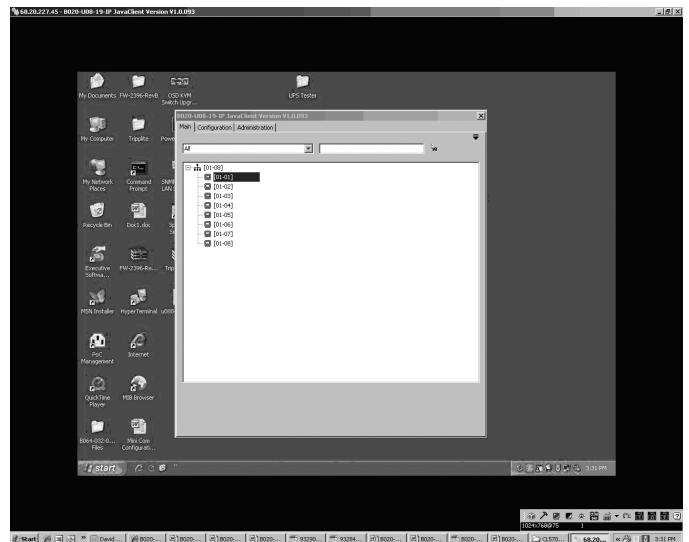
3. Upon entering the serial number, the AP Java Client connect prompt appears, asking you to enter in the *IP address* and *Port* of the KVM you wish to connect to. Enter in this information and click the **Connect** button. *Note: The default port number assigned to the KVM is 9000.*



4. A prompt appears asking you to enter your username and password. If accessing the KVM for the first time, enter in the *username administrator* and the *password password*. For security purposes, it is strongly recommended that you change the username and password on this account to something unique.



5. When you have entered your username and password, the screen of the first connected computer on the installation that you have access to is displayed, as well as the *Remote OSD*.



6.6 Web Browser and Non-Browser Remote Port Access

When accessing the KVM switch over IP, the connected computers can be accessed using either Windows or Java applications. Regardless of which application you use, or whether you log in via browser or AP client, operation of the KVM switch is the same. The only difference is in how you log in and connect to the KVM. When logging in via the AP Windows and Java clients, you are brought directly to the connected computers and the *Remote OSD* is displayed. When logging in via web browser, you are brought to the Web Management Interface, which includes *Windows Client* and *Java Applet* applications for accessing the connected computers. Those who log in using Internet Explorer will be able to access both the *Windows Client* and *Java Applet*, whereas users who log in using another browser only have access to the *Java Applet*. Once logged into the web interface via browser, click on the *Windows Client* or *Java Applet* icon to open the applications and access the connected computers. The same as with the AP clients, once the *Windows Client* and *Java Applet* are opened, the screen of the first connected computer on the installation that you have access to is displayed, as well as the *Remote OSD*.

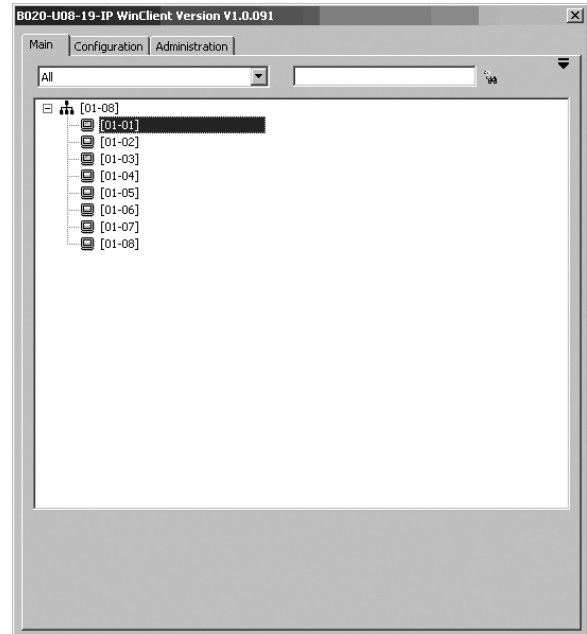
Note: The Java applet requires that the Java Runtime Environment (JRE) be installed on your computer. The JRE is available for free download from the Java web site (<http://java.com>).



6. KVM Operation *(continued)*

6.6.1 Port Access via Remote OSD

The remote OSD displays the ports and KVM stations in the installation in a tree format. KVM stations are displayed with a +/- sign next to them, which when clicked will display or hide the ports on that KVM. To access a port in the installation, you can double-click on the desired port or use the [↑] and [↓] keys to highlight it and hit the [Enter] key.



6.6.2 Port Access via Remote OSD Toolbar

In addition to the remote OSD, a remote OSD toolbar is provided for greater control of the connected ports. The remote OSD toolbar contains icons that when clicked allow you to quickly switch between ports, start an auto scan or invoke panel array mode.



- To open the remote OSD toolbar, hit the [Scroll Lock] key twice. The OSD hotkey can be changed from [Scroll Lock] to [Ctrl] in the Configuration page of the remote OSD (see page 31 for details).
- When the remote OSD toolbar is opened, ordinary keyboard and mouse functionality is suspended. The mouse functionality will be limited to the remote OSD toolbar only. The keyboard functionality will be limited to the hotkey commands mentioned below and the [Ctrl], [Alt], [Delete] command for the local computer. Pressing the [Esc] key will close the remote OSD toolbar.
- When the remote OSD toolbar is opened, you can hit the [Scroll Lock] key once more to open the remote OSD. When the OSD toolbar is not opened, hitting the [Scroll Lock] key three times will open the remote OSD.
- When the remote OSD toolbar is opened, pressing the [←] key will skip to the first accessible port prior to the currently selected port.
- When the remote OSD toolbar is opened, pressing the [→] key will skip to the first accessible port after the currently selected port.
- When the remote OSD toolbar is opened, pressing the [↑] key will skip to the first accessible port in the entire installation.
- When the remote OSD toolbar is opened, pressing the [↓] key will skip to the last accessible port in the entire installation.

This table describes the icons in the remote OSD toolbar:

Icon	Description
	Skips to the last accessible port in the KVM station prior to the currently selected station.
	Skips to the first accessible port in the KVM station after the currently selected station.
	Skips to the first accessible port in the entire installation.
	Skips to the first accessible port prior to the currently selected port.
	Initiates an auto scan.
	Skips to the first accessible port after the currently selected port.
	Skips to the last accessible port in the entire installation.
	Opens the remote OSD.
	Invokes Panel Array Mode (see page 21 for details).
	Closes the remote OSD toolbar.
	Closes out of the remote session.

6. KVM Operation (continued)

6.6.3 Mouse Synchronization

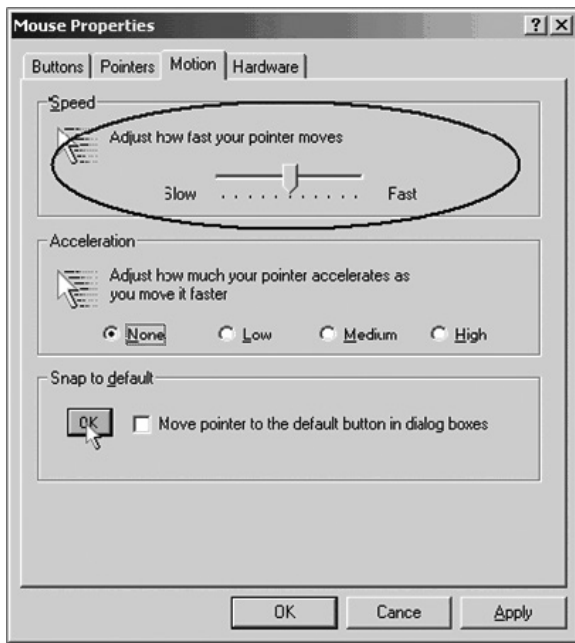
When accessing connected computers over IP, there are two mouse pointers—one for the local computer accessing the KVM and one for the remote computer connected to the KVM. When remotely accessing computers connected to the KVM switch, a *Video Auto Sync* is performed, at which time the local and remote mouse pointers are automatically aligned. If these two mouse pointers do not align properly, or if the response time is slow and choppy, there are a number of methods to get them synced and working properly. Before trying any mouse synchronization procedures, it is always a good idea to ensure that you go to your Mouse Properties Settings and set them according to the instructions below. The *Mouse Properties Settings* should be set on the computers attached to the KVM Switch, not the computer you are using to access it.

Windows

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with your Windows operating system. If you have a third party driver installed—such as one supplied by the mouse manufacturer—you must remove it.

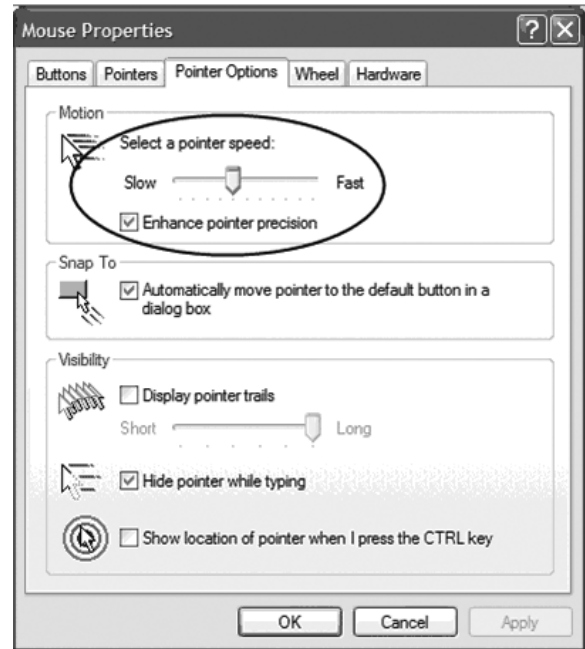
Windows 2000:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse → Mouse Properties**).
2. Click the *Motion* tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Set the mouse acceleration to *None*.



Windows XP / Server 2003 / Vista / 7:

1. Open the *Mouse Properties* dialog box (**Control Panel → Mouse**).
2. Click the *Pointer Options* tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Disable *Enhance Pointer Precision*.



Windows ME:

- Set the mouse speed to the middle position and disable mouse acceleration. (Click the **Advanced** button to get the dialog box for this).

Windows NT / Windows 98 / Windows 95:

- Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

```
Sun: xset m 1Linux: xset m 0
```

Mouse Synchronization Procedures

If you are having syncing problems after adjusting the mouse properties of the connected computer, try the following methods to help synchronize the local and remote mouse pointers:

Note: Mouse synchronization may require several seconds to take effect. Wait 15 to 30 seconds to ensure that the mouse has had enough time to sync.

- Perform a *Video Auto Sync* by clicking on the *Video Auto Sync* icon in the control panel; or, by opening up the *Video Settings* screen and clicking on the *Auto Sync* button. In most cases, the local and remote mouse pointers will automatically align following the *Video Auto Sync*.
- Move the mouse pointer into all four corners of the screen (in any order).
- Invoke the *Adjust Mouse* hotkey command (see page 22 for details). This hotkey command defaults at [Alt], [M], and will bring the local and remote mouse pointers together.
- If mouse and keyboard response time is slow and choppy, adjusting the video settings can help. The less data that is being sent over the network, the faster the mouse and keyboard response time. In particular, adjustment of the *Quality* and *Color Depth Control* settings in the *Video Settings* screen can help decrease the amount of data being transferred.
- Go to the *Display Settings* in the computer connected to the KVM and decrease the *Screen Resolution* and *Color Quality* settings.

6. KVM Operation *(continued)*

6.6.4 Remote Auto Scan

When *Auto Scan Mode* is invoked via the remote OSD toolbar, the KVM begins scanning according to the *Scan Select* and *Scan Duration* settings in the *Configuration* tab of the remote OSD. During an auto scan, normal keyboard and mouse functionality is suspended. Keyboard functionality is limited to the [**Spacebar**] key (exits auto scan at currently selected port), [**Esc**] key (exits auto scan at the currently selected port), [**P**] key (pauses auto scan at the currently selected port) and the [**Ctrl**], [**Alt**], [**Delete**] command for the local computer. Mouse functionality is limited to the auto scan toolbar, which replaces the remote OSD toolbar. The icons in the auto scan toolbar are described in the table:



Icon	Description
	Indicates that the currently selected port is being accessed in <i>Auto Scan Mode</i> .
	Pauses the auto scan at the currently selected port.
	Exits auto scan at the currently selected port
	Displays the port ID according to the <i>Display Mode</i> setting in the <i>Configuration</i> tab of the remote OSD or the F3 Set page of the local OSD.

6.6.5 Panel Array Mode

Panel Array Mode allows connected computers to be simultaneously monitored by dividing the screen into a grid of panels, with each panel representing a KVM port. When *Panel Array Mode* is invoked via the remote OSD toolbar, it scans the connected computers per the *Scan Select* setting in the *Configuration* tab of the remote OSD.



A panel array toolbar is located in the lower right corner of the panel array mode screen. As with the other toolbars, the panel array mode toolbar can be dragged to anywhere on the screen. The table describes the icons located in the panel array toolbar:

Icon	Description
	Moves the focus of the panel array scan back four panels.
	Moves the focus of the panel array scan back one panel.
	Pauses the panel array mode scan, leaving the focus on the currently highlighted panel.
	Moves the focus of the panel array scan forward one panel.
	Moves the focus of the panel array scan forward four panels.
	Increases the number of panels displayed in panel array mode.
	Decreases the number of panels displayed in panel array mode.
	Toggles the 4/3 aspect ratio.
	Exits panel array mode at the currently highlighted port.

6. KVM Operation (continued)

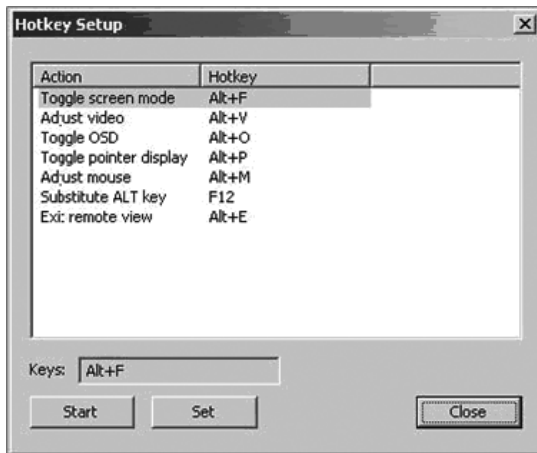
6.6.6 Remote Control Panel

When accessing connected computers over IP, a control panel appears in the lower-right corner of your screen. The remote control panel allows you to perform tasks and edit settings related to the remote session. The icons provided in the remote control panel are described in the following section.



Hotkey Setup

When the *Hotkey Setup* icon is clicked, a screen appears that lists various actions related to the keyboard, video and mouse that can be performed via hotkey commands. The actions that can be performed are listed on the left side of the screen, and the hotkey commands that invoke them are shown to the right.



The table describes the actions that are found in the Hotkey Setup screen:

Action	Hotkey	Description
Toggle screen mode	[Alt] + [F]	Displays the remote screen either as a full-screen or as a window on the local computer.
Adjust video	[Alt] + [V]	Displays the Video Settings screen.
Toggle OSD	[Alt] + [O]	Toggles the remote control panel on and off.
Toggle pointer display	[Alt] + [P]	Toggles the mouse pointer of the local computer on and off, so that only the mouse pointer of the remote computer is displayed.
Adjust mouse	[Alt] + [M]	Aligns the local and remote mouse pointers.
Substitute Alt key	[F12]	Although all other keyboard input is captured and sent to the remote computer, the [Alt] + [Tab] and [Ctrl] + [Alt] + [Del] commands are still sent to your local computer. In order to use these commands on the remote system, another key must be substituted for the [Alt] key. If you substitute the [F12] key, for example, you would use [F12] + [Tab] and [Ctrl] + [F12] + [Del]. Note: By default, the substitute [Alt] key is [F12].
Exit: remote view	[Alt] + [E]	Disconnects and exits the remote session.

Configuring the Hotkeys

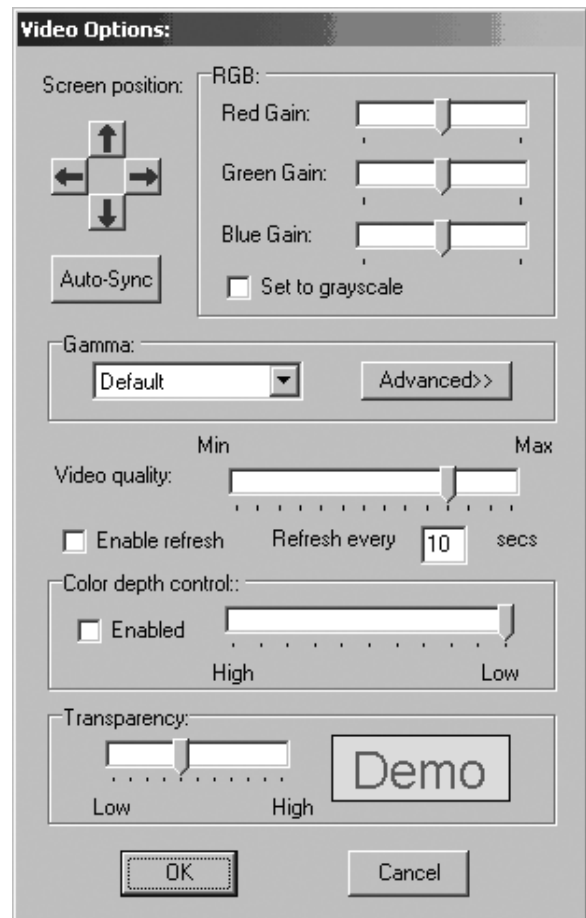
If you find the default hotkey commands inconvenient, you can configure them by following these steps:

1. In the *Hotkey Setup* screen, highlight the action that you wish to edit.
2. Click the **Start** button.
3. Enter in the new hotkey combination. The name of each key appears in the *Keys* field upon being entered.
4. When you have finished entering the new hotkey command, click the **Set** button.
5. Click the **Close** button to exit the *Hotkey Setup* screen.



Video Settings

Clicking the *Video Settings* icon in the control panel brings up the *Video Settings* dialog box. This dialog box allows you to adjust the placement and picture quality of the remote screen on your monitor:



6. KVM Operation (continued)

6.6.6 Remote Control Panel (continued)

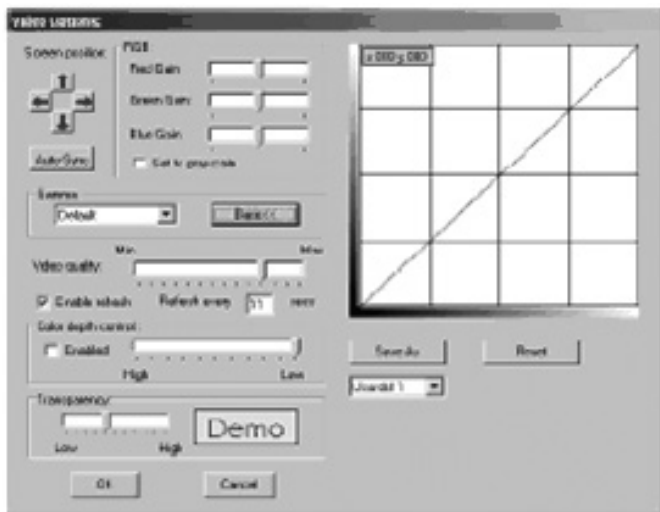
The table describes each of the settings in the Video Settings screen:

Setting	Description
Screen Position	Adjust the horizontal and vertical position of the remote computer window by clicking the arrow buttons.
Auto-Sync	Click the <i>Auto-Sync</i> button to automatically synchronize the remote screen with the local screen. <i>Note: Upon performing an Auto-Sync, the local and remote mouse pointers are automatically synced as well.</i>
RGB	Drag the slider bars to adjust the RGB (Red, Green, Blue) values. If the <i>Set to grayscale</i> checkbox is checked, the remote video is displayed in black and white. Setting the video to grayscale will decrease the amount of information traveling over the network and can help improve keyboard and mouse response time.
Gamma	This setting allows you to adjust the video display's gamma level. (See the <i>Gamma Adjustment</i> Section for details.)
Video Quality	Drag the slider bar to adjust the overall video quality of the remote screen. A higher video quality setting may slow down the keyboard and mouse response time.
Enable Refresh	The KVM switch can be set to redraw the screen every 1 to 99 seconds, eliminating unwanted artifacts from the screen. Check the <i>Enable refresh</i> checkbox and enter in a number from 1 to 99 to have the KVM refresh at the desired time intervals. By default, this feature is disabled, and the <i>Enable refresh</i> checkbox is unchecked.
Transparency	This setting adjusts the transparency of the remote OSD toolbar.
Color Depth Control	This setting adjusts the amount of color information that is being sent over the network. To enable this setting, check the <i>Enabled</i> check box. A higher setting will provide more color, which may slow down keyboard and mouse response time. A lower setting will reduce the amount of information being sent over the network, and may improve keyboard and mouse response time.

Gamma Adjustment

If it is necessary to correct the gamma level for the remote video display, use the Gamma function in the *Video Settings* screen.

- Under Basic configuration, there are ten preset and four user-defined levels to choose from. Go through the options in the drop-down list box to find a setting that works for you.
- For greater control, clicking the *Advanced* button brings up the following dialog box:



- Click and drag the diagonal line at as many points as you wish to achieve the display output you desire.
- Click **Save As** to save up to four user-defined configurations derived from this method. Saved configurations can be recalled from the list box at a future time.
- Click **Reset** to abandon any changes and return the gamma line to its original diagonal position.
- Click **OK** to save your changes and close the dialog box.
- Click **Cancel** to abandon your changes and close the dialog box.

Note: For best results, change the gamma while viewing a remote computer.



Video Auto Sync

Clicking the *Video Auto Sync* icon on the control panel will perform a *Video Auto Sync*. This is the same action that is performed when connecting to a remote computer, or when clicking the *Auto-Sync* button in the *Video Settings* screen.



Gray Scale

Clicking the *Gray Scale* icon on the control panel will display the remote screen in black and white. This is the same action that is performed by checking the *Set to grayscale* checkbox in the *Video Settings* screen.



Message Board





This KVM Switch supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature has been provided, allowing users to communicate with each other:



6. KVM Operation (continued)

6.6.6 Remote Control Panel (continued)

The buttons on the button bar are toggles. Their actions are explained in the table:

Button	Description
	Enable/Disable Chat: When disabled, this icon displays next to the disabled user's name in the <i>User List</i> panel of all users' message boards. Messages directed to the disabled user are not displayed on the message board. The button is shadowed when disabled.
	Occupy/Release Keyboard/Video/Mouse: When you occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. A prompt will come up on the locked out users' monitor stating which user has occupied the KVM. The button in the message board is shadowed and this icon displays next to the occupying user's name in the <i>User List</i> of all other users' message boards.
	Occupy/Release Keyboard/Mouse: When you occupy the KVM, other users can see the remote video, but they cannot input keyboard or mouse data. When enabled, the button is shadowed and this icon displays next to the occupying user's name in the <i>User List</i> of all users' message boards.
	Show/Hide User List: This button will hide or display the user list panel on the right of the message board. This icon is only located in the Windows message board. The Java message board has arrows next to the user list panel that can be clicked on to show/hide the panel.

User List Panel

- The names of all the logged in users appear in the *User List* panel. Select the names of the users that you want to send a message to, or simply select the *All users* option to send a message to all users.
- If a user has chosen to *Disable Chat*, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, the corresponding icon displays before the user's name.

Compose Panel

Type your message into this panel. Click **Send**, or press **[Enter]** to post the message to the board.

Note: You must select the user from the user list that you want to send the message to. To send a message to all users, simply click All Users in the user list.

Message Display Panel

Messages that users post to the board, as well as system messages, display in this panel. If you *Disable Chat*, messages that get posted to the board will not appear.



Ctrl-Alt-Del

As the **[Ctrl] + [Alt] + [Delete]** command is sent to the local computer and not the remote computer, this icon provides an easy way to send this command to the remote computer. The **[Ctrl] + [Alt] + [Delete]** command can also be sent using the substitute **[Alt]** key. (See *Hotkey Setup* section)



Soft Keyboard

The KVM Switch supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language. Click this icon to display the on-screen keyboard:

To change languages, click the drop-down arrow next to the *Soft Keyboard* icon and select the new language.



Exit Remote View

Click this icon to disconnect and exit the remote session.



Num Lock, Caps Lock, Scroll Lock

Click on one of these three icons to toggle the corresponding lock function ON/OFF.



About

Clicking this icon will display the model name and IP firmware version number of the KVM switch.

7. Administration

Administration of the KVM switch can be done through three different interfaces; Local Console OSD, Web Interface and Remote OSD. The Web Interface and Remote OSD give you the most administrative access to the KVM, whereas the settings in the Local OSD are more limited. The table details which settings are available in each interface, and whether those settings are accessible to Administrators, ordinary Users or both. The rest of this chapter goes into these interfaces and their settings in more detail.

	Local OSD		Remote OSD		Web Management Interface	
	User	Admin	User	Admin	User	Admin
Set Language of OSD/GUI	X	X	X	X	X	X
Set Ports to Be Displayed in OSDs	X	X	X	X		
OSD Hotkey	X	X	X	X		
Port ID Display Mode	X	X	X	X		
Port ID Display Duration	X	X	X	X		
Scan Select	X	X	X	X		
Scan Duration	X	X	X	X		
Screen Blanker	X	X	X	X		
Logout Timeout		X	X	X		
Beeper		X	X	X		
Edit Port Names		X	X	X		
Set Port Operating Systems		X		X		
Hotkey Command Mode (On/Off)	X	X				
Hotkey	X	X				
Port ID Display Position	X	X				
Reset Station IDs		X				
Set Local Keyboard Language		X				
Setup IP Address		X		X		X
View Firmware Version		X		X		X
Firmware Upgrade		X		X		X
Reset Default Values		X		X		X
Clear Port Names		X		X		X
View Device Name				X		X
View MAC Address				X		X
Add, Edit and Remove Administrators/Users				X		X
Port Access - Full/View Only/No Access				X		X
Setup DNS Server Address				X		X
IP Installer Settings - Enabled/View Only/Disabled						X
Enable and Setup RADIUS and LDAP Servers				X		X
Log Server Settings - MAC Address and Port Settings				X		X
Enable and Setup IP Address Filters				X		X
Enable and Setup MAC Address Filters				X		X
Set a Default Web Page Name				X		X
Login Failure Settings				X		X
Enable/Disable ICMP, Browser, Device List, Multiuser and Force All to Grayscale				X		X
Mouse Sync Mode - Automatic/Manual				X		X
Backup and Restore System Configuration and User Accounts						X

7. Administration *(continued)*

7.1 Local Console OSD

Upon logging into the *Local Console OSD*, the main page appears (see figure). *Administrators* have access to all features in the OSD, whereas *Users* have access to everything except the *F4 Admin* page and the *F6 Broadcast (BRC)* function. The *Local Console OSD* administrative settings are described in the following section.

F1:GOTO	F2:SET	F5:SKP	F7:SCAN	X
F2:LIST	F4:ADM	F6:BRC	F8:LOUT	ZC
ADMINISTRATOR				
LIST:ALL				
SN.PN	QV	X	NAME	
02 • 14			ABC COMP1	▲
02 • 15	◀	X	ABC COMP2	↑
02 • 16		X	ABC COMP3	
03 • 01			WEB SERVER 1	
03 • 02			WEB SERVER 2	
03 • 03	◀	X	FAX SERVER 1	
03 • 04		X	FAX SERVER 2	
03 • 05	◀	X	MAIL SERVER 1	▼

7.1.1 Local Console OSD F2 LIST Function

This function lets you tailor the list of ports the OSD will display on the Main Screen. The submenu choices and their meanings are given in the table:

Note: The ports that are displayed in the OSD main screen are the only ports that will be affected under Broadcast Mode.

Setting	Description
ALL	Lists all of the ports on the installation that are accessible to the logged-on user, whether they are powered-ON or not.
POWERED ON	Lists all of the ports on the installation that are both accessible to the logged-on user and powered-ON.
QVIEW	Lists all of the ports on the installation that are set as <i>Quick View</i> ports by an administrator.
QVIEW + POWERED ON	Lists all of the ports on the installation that are both set as <i>Quick View</i> ports by an administrator and are powered ON.

7.1.2 Local Console OSD F3 Settings (SET) Page

This function allows each *User* and *Administrator* to set up their working environment. A separate profile for each is stored by the OSD and is activated according to the username and password provided during login. To change a setting:

- 1) Double-click on it, or highlight it and press the **[Enter]** key.
- 2) After you select an item, a submenu with more choices will appear. To make a selection, double-click on a choice or highlight it and press the **[Enter]** key.

7. Administration *(continued)*

7.1.2 Local Console OSD F3 Settings (SET) Page *(continued)*

The settings in the **F3 SET** page are explained in the following table:

Setting	Description
OSD HOTKEY	Select the hotkey sequence that invokes the OSD (both <i>Local Console OSD</i> and <i>Remote OSD</i>); [Scroll Lock, Scroll Lock] or [Ctrl, Ctrl]. This is set to [Scroll Lock, Scroll Lock] by default.
PORT ID DISPLAY POSITION	This setting allows you to position the <i>Port ID</i> anywhere on the screen. The default is the upper left corner. When selected, the screen switches to the last selected port, and displays its <i>Port ID</i> . To position the <i>Port ID</i> , use the touchpad or the keyboard arrow keys, as well as the [Pg Up], [Pg Dn], [Home], [End], and [5] keys (on the numeric keypad with [Num Lock] off). When the <i>Port ID</i> is in the desired location, double-click or press the [Enter] key to lock it in position and return to the OSD. <i>Note: The Port ID is set independently for each port on the installation. The position specified here only applies to the port that is currently active.</i>
PORT ID DISPLAY DURATION	This selection gives you the option of displaying the <i>Port ID</i> for 3 seconds, or having the <i>Port ID</i> always off. The default is to display for 3 seconds.
PORT ID DISPLAY MODE	Select how the <i>Port ID</i> is displayed: <i>Port Number</i> only, <i>Port Name</i> only or both <i>Port Number</i> and <i>Port Name</i> . The default is to display both <i>Port Number</i> and <i>Port Name</i> .
SCAN DURATION	This setting determines the amount of time spent on each port when in <i>Auto Scan Mode</i> . Key in a value from 1 - 255 seconds, and then press the [Enter] key. The default is 5 seconds; a setting of 0 (zero) disables the <i>Auto Scan</i> function altogether.
SCAN/SKIP MODE	Select which ports will be accessed during <i>Auto Scan Mode</i> and <i>Skip Mode</i> . <ul style="list-style-type: none"> • ALL : All ports that are accessible to the currently logged-on user • POWERED ON: All ports that are both accessible to the currently logged in user and powered-on • QUICK VIEW: Ports that are set as <i>Quick View</i> ports by an administrator • QUICK VIEW + POWERED ON: Ports that are both set as <i>Quick View</i> ports by an administrator and are powered on The default setting is ALL.
SCREEN BLANKER	If the console is left idle for the amount of time set with this function, the screen is blanked. Key in a value from 1 - 30 minutes, and then press the [Enter] key. A setting of 0 disables this function. The default is 0 (disabled).
HOTKEY COMMAND MODE	Enables / Disables the hotkey command function. <i>Hotkey Command Mode</i> is enabled by default.
HOTKEY	Toggle between the two <i>Hotkey Mode</i> invocation sequences. Options are [Num Lock, Minus] and [Ctrl, F12].
OSD LANGUAGE	Determines which language the OSD menus are displayed in. Choices are English, Spanish, French, German and Japanese.

7. Administration *(continued)*

7.1.3 Local Console OSD F4 Administration (ADM) Page

This *Administrator-only* page allows administrators to configure the settings of the KVM switch. To change a setting:

- 1) Double-click on it, or highlight it and press the [Enter] key.
- 2) After you select an item, a submenu with more choices will appear. To make a selection, double-click on a choice or highlight it and press the [Enter] key.

The settings in the **F4 ADM** page are explained in the following table:

Setting	Description
SET IP ADDRESS	This page allows administrators to set the network settings for the KVM. DHCP: The first field allows you to enable or disable DHCP. When enabled, the KVM is assigned an IP address by the DHCP server. This setting is enabled by default. To disable the <i>DHCP</i> setting and set up a fixed IP address, press the [Spacebar] key. Once the <i>DHCP</i> is disabled, you will be allowed to edit the remaining fields in the <i>SET IP ADDRESS</i> page. In the remaining fields, enter in the <i>IP Address</i> , <i>Subnet Mask</i> and <i>Default Gateway</i> you want to assign to the KVM switch. When these fields have been populated, press the [Esc] key to exit and pull up a prompt asking if you wish to save the settings you just entered. If you do not wish to save the settings, press the [N] key. If you do wish to save the settings, press the [Y] key. Upon pressing the [Y] key, the settings will be saved and the KVM will be reset. <i>Note: Only an IPv4 address can be assigned using the Local Console OSD. To assign an IPv6 address, use the Web Management Interface or Remote OSD. This page only allows you to set a fixed IP address or enable IP address assignment via DHCP server. It does not allow you to set the HTTP, HTTPS and Program access ports, assign a DNS server address, or edit the IP Installer settings. To set ports and assign a DNS server address, you can use the Web Management Interface or Remote OSD. To edit the IP Installer settings, you must use the Web Management Interface.</i>
SET LOGOUT TIMEOUT	If there is no input from the console for the amount of time set here, the user will be logged out, requiring them to enter their username and password to regain access to the KVM. This can be set from 0 to 180 minutes, with 0 disabling the function. Simply type in the desired time frame and hit the [Enter] key to save your change. This is disabled (0) by default. <i>Note: The Timeout function can only be set in the Web Management Interface and the Local Console OSD.</i>
EDIT PORT NAMES	This function allows administrators to give each port a unique name, making it easier to find the computer you want to access. To add/edit a port name, do the following: 1. Select the port by double-clicking on it, or by highlighting it and hitting the [Enter] key. 2. A name field will appear at the bottom of the screen. Add or edit the port name and hit the [Enter] key to save the change. To exit without saving the change, hit the [Esc] key. Port names can have a maximum of 12 characters, including any combination of letters and numbers (A-Z, 0-9), and the following characters: Asterisk [*], Parentheses ([)], Plus [+], Minus [-], Colon [:], Comma [,], Question Mark [?], Period [.] , Forward Slash [/] and Space. Port names are NOT case sensitive. They will always display as uppercase in the OSD.
RESTORE DEFAULT VALUES	This allows the Administrator to restore all OSD settings to their factory default values except for the network settings, port names and username/passwords. When this function is accessed, a prompt will appear asking if you wish to restore the default settings. If yes, type in a Y and hit the [Enter] key. If no, press the [Esc] key to go back to the previous menu.
CLEAR THE NAME LIST	This function allows the Administrator to clear all of the port names that have been entered. As with the RESTORE DEFAULT VALUES, you will be prompted upon accessing this function. If you wish to clear the name list, type in a Y and hit the [Enter] key. If not, press the [Esc] key to go back to the previous menu.
ACTIVATE BEEPER	Turns the beeper sound ON or OFF. Type in Y to turn the Beeper sound on, or N to turn it off. You do not need to hit the [Enter] key after typing in Y or N , the change will be made automatically.
SET QUICK VIEW PORTS	Administrators can use this function to mark ports as <i>Quick View</i> ports. This provides a way to customize which ports are displayed in the OSD main menu, and which are accessible in <i>Auto Scan</i> and <i>Skip Modes</i> . To set ports as <i>Quick View</i> ports, do the following: 1. Highlight the desired port and hit the [Enter] key, or click on it using the touchpad. 2. Press the [Spacebar] to toggle <i>Quick View</i> status ON/OFF. An icon will appear in the QV column next to the selected port when <i>Quick View</i> status is turned on. Once <i>Quick View</i> ports are set, the OSD main page can be set up to display only <i>Quick View</i> ports, or only <i>Quick View</i> ports that are powered ON. Administrators can also set it up so that only <i>Quick View</i> ports, or powered on <i>Quick View</i> ports, are accessible in <i>Auto Scan</i> or <i>Skip Modes</i> .
RESET STATION IDs	This function is used when you change the position of one of the KVM stations in a daisy chain. When you change the position of the station, the OSD does not recognize the change, and will not automatically update the main menu to display the stations in correct order. When this function is used, the KVM will scan the entire installation and update the station numbers accordingly. The port names of the affected stations will be kept; however, you will need to manually update all other settings (SET ACCESSIBLE PORTS, SET QUICK VIEW PORTS, etc.).
SET OPERATING SYSTEM	This allows the Administrator to set the operating system for the port to match that of the connected computer. To set the operating system, do the following: 1. Highlight the desired port or click on it using the touchpad. 2. Press the [Spacebar] to toggle between four options; <i>WIN</i> , <i>MAC</i> , <i>SUN</i> and <i>OTHER</i> . Each port is set to <i>WIN</i> by default. 3. You do not need to press the [Enter] key to save this setting.
FIRMWARE UPGRADE	Note: The KVM has two sets of firmware, one to control IP Access and another to control the KVM's Mainboard, Input/Output Ports and Keyboard. The IP Access firmware must be updated via the Web Management Interface or Remote OSD. The KVM Mainboard, Input/Output Ports and Keyboard firmware must be updated via the local console OSD. In order to upgrade the KVM Mainboard, Input/Output Ports and Keyboard firmware, <i>Firmware Upgrade Mode</i> must be invoked via this setting. When you select this option, the firmware version numbers are displayed on the OSD screen, and a prompt will ask if you wish to continue with a firmware upgrade. If yes, type in Y . If no, type in N .

7. Administration *(continued)*

7.1.3 Local Console OSD F4 Administration (ADM) Page *(continued)*

Setting	Description
KEYBOARD LANGUAGE	Sets the language for an external keyboard connected to the KVM's external keyboard port. To select a keyboard language, double-click on the desired language or highlight it and hit the [Enter] key. You can choose between US English, UK English, German, Swiss German, French, Hungarian, Italian, Japanese, Korean, Russian, Spanish, Swedish and Traditional Chinese.

7.1.4 Local Console Firmware Upgrade

The KVM has two sets of firmware, one to control *IP Access* and another to control the KVM's *Mainboard, Input/Output Ports* and *Keyboard*. The *IP Access* firmware must be updated via the *Web Management Interface* or *Remote OSD*. The *KVM Mainboard, Input/Output Ports* and *Keyboard* firmware must be updated via the local console OSD. To upgrade the KVMs *Mainboard, Input/Output Ports* and *Keyboard* firmware, follow the instructions below:

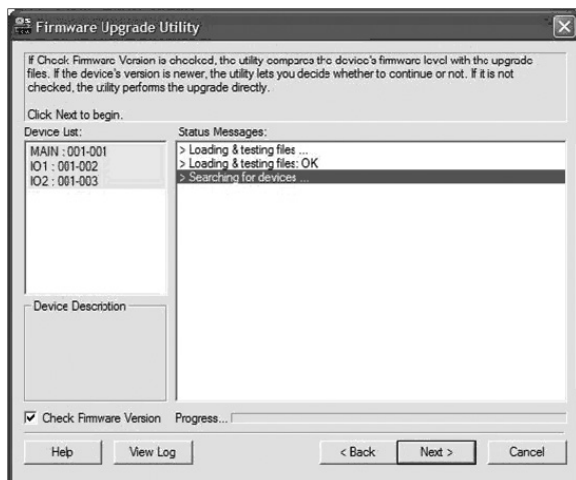
1. From a computer that is not connected to your KVM switch, download the firmware upgrade file from www.tripplite.com/support.

Note: If firmware upgrades are not on www.tripplite.com/support, there are no upgrades available for your unit.

2. Using the included firmware upgrade cable, connect the RJ11 jack on the KVM to a DB9 COM port on the computer you just downloaded the firmware upgrade file to.

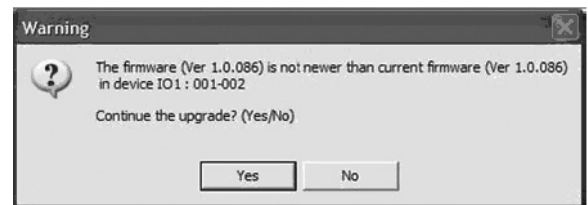
Note: Daisy-chained KVM switches will automatically receive the upgrade via the daisy-chain cables.

3. Shut down all the computers on the KVM installation. Leave all KVM switches powered-ON.
4. Open the local console OSD and navigate to the *F4 ADM* page.
5. Scroll down to the *FIRMWARE UPGRADE* option and press the **[Enter]** key. Press **[Y]** to invoke *Firmware Upgrade Mode*.
6. From the computer you downloaded the firmware upgrade to, run the downloaded file either by double-clicking on it, or by opening a command line and entering the full path to it. The firmware upgrade utility welcome screen appears.
7. Read and agree to the license agreement, and then click **Next** to continue. The firmware upgrade utility main screen appears, and the devices capable of being upgraded are listed in the *Device List* panel on the left side of the screen. There will be three firmware versions displayed for each device.



Note: If you receive a message that a device is not connected to the serial port, you may need to restart the computer the firmware upgrade utility is on.

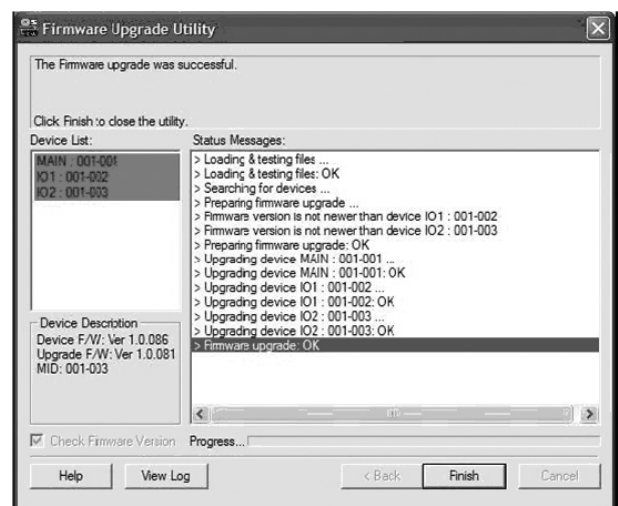
8. Highlight the *Main* firmware version of the desired device, and then click **Next** to begin the upgrade. If you checked the *Check Firmware Version* checkbox, the utility compares the device's firmware level with that of the upgrade files. If it finds that the device's version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to continue or cancel.



If you didn't check the *Check Firmware Version* checkbox, the utility installs the upgrade files without checking the version numbers. As the upgrade proceeds, status messages appear in the *Status Messages* panel, and the progress toward completion is shown on the *Progress* bar.

Note: Each of the three firmware files for the KVM will be upgraded in succession.

1. After the upgrade has completed, a screen appears to inform you that the procedure was successful.



Click **Finish** to close the firmware upgrade utility.

Note: Upgrade the IP firmware via the Remote OSD or the Web Management Interface. (See the Remote OSD Firmware Upgrade or Web Management Interface Firmware Upgrade sections for details.)

7. Administration *(continued)*

7.1.4 Local Console Firmware Upgrade *(continued)*

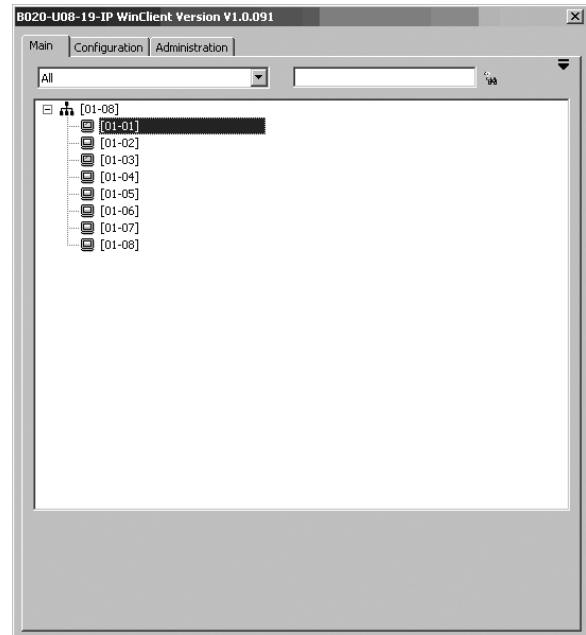
Firmware Upgrade Recovery

In the event of a firmware upgrade failure, or an aborted firmware upgrade, perform a firmware upgrade recovery by doing the following:

1. Power OFF the switch. If it is part of a daisy chain, disconnect it from the chain.
2. Connect the firmware upgrade cable to the firmware upgrade port.
3. Slide the *Firmware Upgrade Recovery Switch* to the *Recover* position.
4. Power the switch back ON and repeat the upgrade procedure.
5. After the switch has been successfully upgraded, power it OFF and then slide the *Firmware Upgrade Recovery Switch* back to the *Normal* position.
6. If the switch is part of a daisy chain, reconnect it to the daisy chain.
7. Power the switch back ON.

7.2 Remote OSD

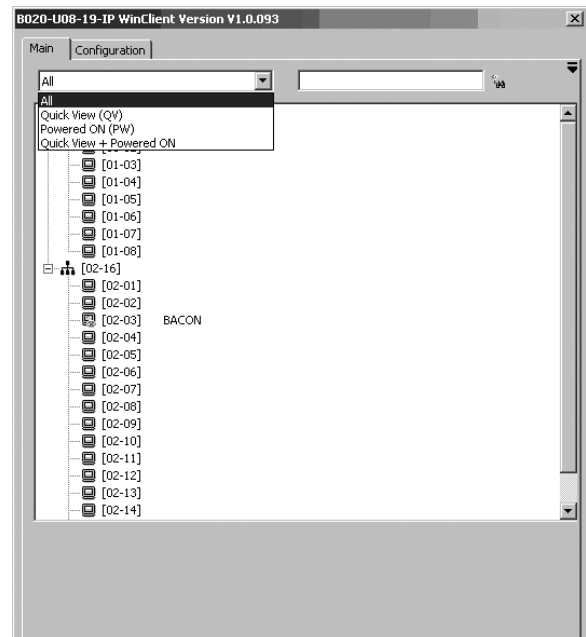
Upon logging into the KVM over IP, you are connected to the first connected computer on the installation that you have access to, and the *Remote OSD* appears with the *Main* tab displayed. (See diagram). *Administrators* have access to all features in the OSD, whereas *Users* only have access to the *Main* tab and *Configuration* tab. The administrative settings of the *Remote OSD* are described in the following section.



7.2.1 Remote OSD List Drop-Down

Just like the *F2 LIST* function in the local console OSD, the remote OSD allows you to determine which ports are listed on the *Main* tab. Simply click on the drop-down menu at the top of the OSD screen and select an option.

Setting	Description
ALL	Lists all of the ports on the installation that are accessible to the logged-on user, whether they are powered-ON or not.
POWERED ON	Lists all of the ports on the installation that are both accessible to the logged-on user and powered-ON.
QVIEW	Lists all of the ports on the installation that are set as <i>Quick View</i> ports by an administrator.
QVIEW + POWERED ON	Lists all of the ports on the installation that are both set as <i>Quick View</i> ports by an administrator and are powered ON.



7. Administration *(continued)*

7.2.2 Remote OSD Configuration Tab

The *Configuration* tab (see diagram) allows administrators and users to set up their working environment. A separate profile for each is stored by the OSD and is activated according to the username and password provided during login. The settings in the *Configuration* tab are described in the table below.



Setting	Description
Set Language	Determines which language the OSD menus are displayed in. Choices are English, Spanish, French, German and Japanese.
OSD Hotkey	Selects which hotkey sequence invokes the OSD; [Scroll Lock, Scroll Lock] or [Ctrl, Ctrl] . The default is [Scroll Lock, Scroll Lock] .
Display Mode	Selects how the <i>Port ID</i> is displayed: the <i>Port Number</i> alone, the <i>Port Name</i> alone, or the <i>Port Number</i> plus the <i>Port Name</i> . The default is the <i>Port Number</i> plus the <i>Port Name</i> .
ID Duration	Determines whether the <i>Port ID</i> displays on the monitor for 3 seconds, or if it is turned off. By default, it is set to display for 3 seconds.
Scan Select	Selects which computers will be accessed under <i>Auto Scan</i> and <i>Skip Modes</i> . ALL: All ports that are accessible to the logged-on user. POWERED ON: Ports that are both accessible to the logged-on user and are powered ON. QUICK VIEW: Ports that are set as <i>Quick View</i> ports by an administrator. QUICK VIEW + POWERED ON: Ports that are both set as <i>Quick View</i> ports by an administrator and are powered ON. The default is ALL .
Scan Duration	Determines how much time is spent on each port during an <i>Auto Scan</i> . Key in a value from 0 - 255 seconds. The default is 5 seconds; a setting of 0 disables the Scan function.
Screen Blanker	If there is no input from the console for the amount of time set with this function, the screen is blanked. Key in a value from 1 - 30 minutes. A setting of 0 disables this function. The default is 0 (disabled).
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. A login is necessary before the KVM switch can be accessed again. Enter a value from 0 - 180 minutes. A setting of 0 disables this function. It is disabled (0) by default.
Beeper	Toggles the beeper sound ON/OFF.

7.2.3 Remote OSD Administration Tab

This *Administrator-only* page allows administrators to configure the settings of the KVM switch. When clicked on, the *Administration* tab appears with the *General Settings* screen displayed. On the left of this screen are icons that can be clicked on to display various administrative settings. These icons and the settings they provide access to are described in the sections that follow.



7. Administration *(continued)*

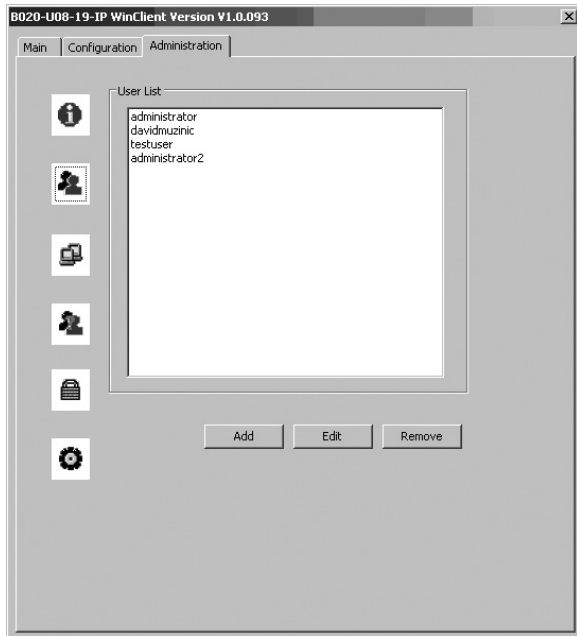
7.2.3 Remote OSD Administration Tab *(continued)*

General Information

The *General Information* screen displays the *Device Name*, *MAC Address*, *Firmware Version*, *IPv4 address* and *IPv6 address* of the KVM switch. The *Device Name* can be customized by an administrator, but defaults at the KVM model name. The *Firmware Version* displayed is that of the *IP Access* firmware.

User Management

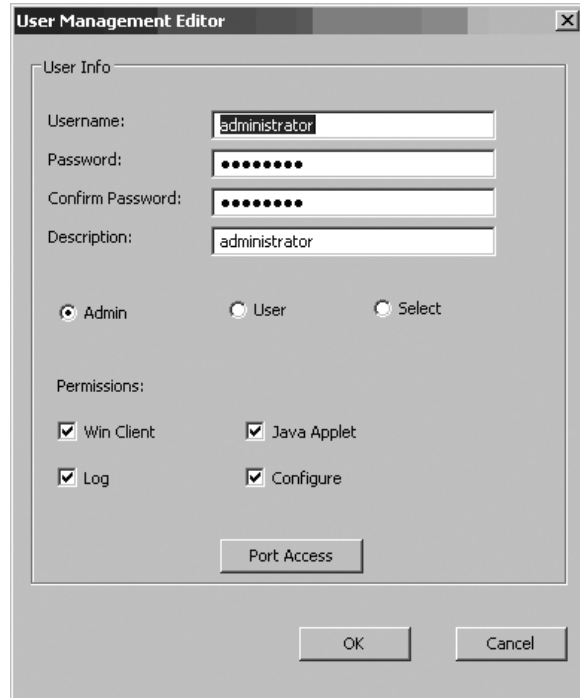
The *User Management* screen allows administrators to *Add*, *Edit* and *Delete User* and *Administrator* accounts. Up to 64 accounts can be established, with any combination of *Administrators* and *Users*.



- To add a new account, click the **Add** button. The *Add User* page appears.



- To edit an existing account, highlight it in the list and click the **Edit** button. The *Edit User* page appears.



- To delete an existing account, highlight it in the list and click the **Remove** button. When clicking the **Remove** button, you are not asked to confirm whether you want to delete the selected account, it is automatically deleted.

The table describes the fields and settings that are found in the *Add User* and *Edit User* screens:

Setting	Description
Username	Enter the account username here. A minimum of 6 and a maximum of 16 characters are allowed.
Password	Enter the account password here. A minimum of 6 and a maximum of 16 characters are allowed.
Confirm Password	Re-enter the account password here. If the two entries do not match, you will be prompted to re-type the password.
Description	Additional information about the user that you may wish to include (optional).
Admin	Check this option to give the account <i>Administrator</i> access rights. <i>Administrators</i> have access to all features and configuration settings of the KVM.
User	Check this option to give the account <i>User</i> access rights. <i>Users</i> have access to both the <i>Windows Client</i> and <i>Java Client</i> , but do not have access to the <i>Log Server</i> or <i>Configuration Settings</i> .
Select	Check this option to <i>Select</i> the account access rights yourself. (See <i>Permissions</i> on page 33 for details.)

7. Administration (continued)

7.2.3 Remote OSD Administration Tab (continued)

User Management – Permissions

The following permissions are included in the *Add User* and *Edit User* screens of the *User Management* tab, and determine what access rights are available to each account:

- **Win Client:** When selected, the corresponding account can access the KVM switch using the *Windows Client* in the *Web Management Interface* and the non-browser *AP Windows Client*.
- **Java Applet:** When selected, the corresponding account can access the KVM switch using the *Java Applet* in the *Web Management Interface* and the non-browser *AP Java Client*.
- **Log:** When selected, the corresponding account can access the *Log File* included in the *Web Management Interface*.
- **Configure:** When selected, the corresponding account can access the *Administrator* settings in the *Local Console OSD*, *Remote OSD* and *Web Management Interface*.

User Management – Port Access

The *Port Access* button at the bottom of the *User Management Add User* and *Edit User* screens allow port access to be customized for each account. Although user accounts can be created, edited and deleted using both the *Web Management Interface* and the *Remote OSD*, the only place *Port Access* settings can be edited is in the *Remote OSD*. In this page, access can be toggled between three access types by clicking on the field next to the corresponding port, or by highlighting the desired port and using the **[+]** or **[-]** keys on the number pad of the keyboard. By default, all accounts have *Full Access* to all computers on the installation.

- **Full Access:** The user has the ability to both view and perform keyboard/mouse operations on the corresponding computer.
- **View Only Access:** The user only has the ability to view the corresponding computer's video.
- **No Access:** The user has no access to the corresponding computer.



Network

The *Network* screen of the remote OSD allows administrators to set the IPv4 or IPv6 network parameters for the KVM switch. In addition to the *IP Address*, *Subnet Mask* and *Default Gateway*, which can be set using the local console OSD, the *Network* screen of the remote OSD allows you to set firewall access ports and the DNS server address. These settings can also be configured using the *Web Management Interface*.

Network – Access Ports

If a firewall is being used, these fields allow administrators to specify port numbers that the firewall will allow. The firewall must be set to allow access to these ports. If an invalid port number (or no port number) is specified in the firewall, the KVM switch will not be found.

An explanation of the Access Port fields is given in the table:

Port	Description
Program	This is the port number that must be specified when connecting to the KVM via the AP Windows or Java client. The default is 9000.
HTTP	This port number is for a browser login. The default is 80.
HTTPS	This port number is for a secure browser login. The default is 443.

Note: A different value must be set for each access port. If there is no firewall, it doesn't matter what these numbers are set to, since they have no effect.

Network – IP Address and DNS Server

The KVM's IP and DNS Server addresses can be assigned automatically by a DHCP server, or given a fixed address by an administrator. By default, the KVM switch is set to have an IP address assigned automatically via DHCP server. If this is the case, you will need to obtain the IP address from your network administrator. If connected to a network without a DHCP server, it boots with a default IP address. The default IPv4 and IPv6 addresses can be found on the sticker on the bottom of the unit. Follow the steps below to configure the KVM's IPv4 or IPv6 settings accordingly, depending on your network.

1. To have the IP address pulled automatically via DHCP server, make sure that the *Obtain an IP address automatically [DHCP]* option is selected.
2. To assign a fixed IP address, make sure the *Use the following IP address [Fixed IP]* option is selected.
3. Fill in the *IPv4 or IPv6 Configuration* fields with information appropriate to your network.
4. If you have set the IP address to be pulled via DHCP server, you can either choose to assign the DNS server address via DHCP as well, or assign a fixed DNS server address. If you have assigned a fixed IP address for the KVM, you must also assign a fixed DNS server address. To have the DNS server address pulled via DHCP server, make sure that the *Obtain DNS server address automatically* option is selected. To assign a fixed DNS server address, make sure that the *Using the following DNS server address* option is selected.
5. Fill in the *Primary DNS server* and *Alternate DNS server* fields with information appropriate for you network.

Note: Specifying the primary DNS Server address is mandatory. The alternate DNS Server address is optional.

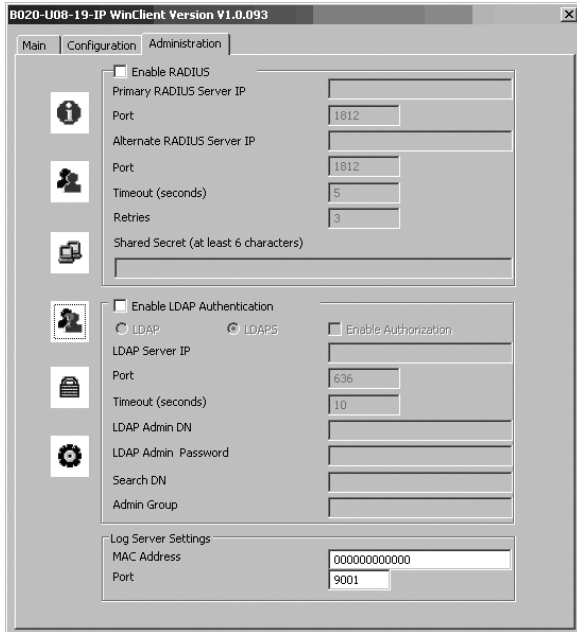
6. After all changes have been made, make sure that the *Reset on exit* checkbox in the *Customization* screen is checked. This checkbox should automatically be checked anytime network settings have been changed.
7. Exit the remote session and logout of the KVM switch. Upon logging out of the KVM, a prompt will appear stating the KVM will be reset. Upon completion of the KVM reset, the new network settings will be saved.

7. Administration *(continued)*

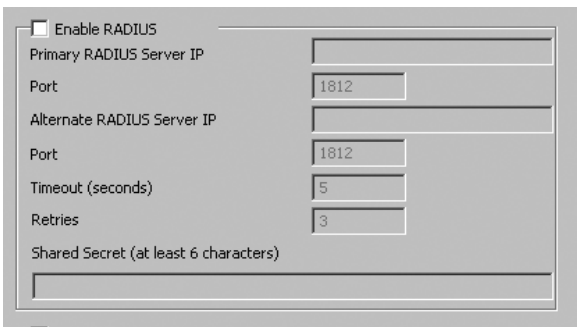
7.2.3 Remote OSD Administration Tab *(continued)*

ANMS

The Advanced Network Management Settings (ANMS) screen allows you to set up login authorization management from an external source. From this screen, administrators can set up remote management via RADIUS and/or LDAP/S, and set up the access port and MAC address for the Windows-based log server.



ANMS - RADIUS



To allow authorization through a RADIUS server, do the following:

1. Check the *Enable RADIUS* checkbox.
2. Fill in the *Primary RADIUS Server IP* and *access Port*, and the *Alternate RADIUS Server IP* and *access Port*.
3. In the *Timeout (seconds)* field, set the time in seconds that the KVM waits for a reply from the RADIUS server before it times out.
4. In the *Retries* field, enter the number of times you want the KVM to try and reconnect with the RADIUS server before it gives up.
5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the KVM and the RADIUS Server.

On the RADIUS server, set the access rights for each user according to the information in the table:

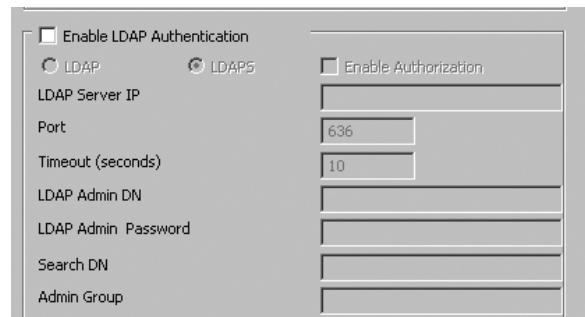
Character	Description
C	Gives the corresponding account administrator privileges.
W	Gives the corresponding account access to the KVM switch via the Windows browser and non-browser applications.
J	Gives the corresponding account access to the KVM switch via the Java browser and non-browser applications.
L	Gives the corresponding account access to the log server on the Web Management Interface.
V	Gives the corresponding account view-only access to all ports on the KVM switch.
PN/xxxx	Denies the corresponding account access to a port.
SN/xx	Denies the corresponding account access to a station.
PV/xxxx	Gives the corresponding account view-only access to a port.
SV/xx	Gives the corresponding account view-only access to a station.
PF/xxxx	Gives the corresponding account full access to a port.
SF/xx	Gives the corresponding account full access to a station.

RADIUS Server access rights examples are given in the following table:

RADIUS Access Rights	Description
C	The corresponding account has administrator access to the KVM.
W, J, L	The corresponding account can access the system via the Windows and Java browser and non-browser applications, and can access the log server on the Web Management Interface.
PN/0102	The corresponding account is denied access to port 2 on station 1.
PF/A	The corresponding account is given full access to all ports on the installation.
SV/02	The corresponding account is given view-only access to station 2.

Note: Characters are not case sensitive. Characters are comma delimited.

ANMS – LDAP/S



7. Administration (continued)

7.2.3 Remote OSD Administration Tab (continued)

To allow authentication and authorization via LDAP/S, do the following:

1. Check the *Enable LDAP Authentication* checkbox.
2. Select LDAP or LDAPS.
3. Determine whether to enable authorization or not.
 - If the *Enable Authorization* checkbox is checked, the LDAP/S server directly returns a 'permission' attribute and authorization for the account that is logging in. With this selection, the LDAP schema must be extended.
 - If the *Enable Authorization* checkbox is not checked, the LDAP/S server indicates whether the account that is logging in is a member of the KVM Admin Group or not. If yes, the account has full access rights. If no, the account has user access rights (See the *User Management* section of this manual for details on account permissions).
4. Enter the appropriate IP address and access port for the LDAP or LDAPS server in the LDAP Server IP and Port fields. The default port number for LDAP is 389, and is 636 for LDAPS.
5. In the *Timeout (Seconds)* field, enter the time in seconds that the KVM waits for an LDAP or LDAPS server reply before it times out.
6. Consult the LDAP/S administrator about the appropriate entry for the *LDAP Administrator DN* field. For example, the entry might look like this: cn=LDAPAdmin,ou=B022-U08-IP,dc=tripplite,dc=com
7. In the *LDAP Admin Password* field, key in the LDAP administrator's password.
8. In the *Search DN* field, set the distinguished name of the search base (i.e. the domain name where the search starts for the user name).
Note: If the Enable Authorization checkbox is not checked, this field must include the entry where the KVM Admin Group is created. Consult the LDAP/S administrator about the appropriate entry for this.
9. In the *Admin Group* field, key in the group name for KVM administrator accounts. *Note: If the Enable Authorization checkbox is not checked, this field is used to authorize accounts that are logging in. Accounts that are in this group have full access rights to the KVM. Accounts that are not in this group have user access rights to the KVM (See the User Management section of this manual for details on account permissions). Consult the LDAP/S administrator about the appropriate entry for this.*
10. On the LDAP server, set the access rights for each user (The following sections describe how to configure LDAP/S for use with the KVM switch).

ANMS – LDAP/S Configuration

To allow authentication and authorization via LDAP or LDAPS, the active directory's LDAP Schema must be extended so that an extended attribute name for the KVM—*permission*—is added as an optional attribute to the person class.

Note: Authentication refers to the identity verification of the person logging into the KVM switch, whereas Authorization refers to the assigning of device permissions.

In order to configure the LDAP server, you will have to complete the following procedures:

1. Install the Windows Support Tools.
2. Install the Active Directory Schema Snap-In.
3. Extend and Update the Active Directory Schema.

Each of these procedures is described in the following sections:

Install the Windows Support Tools

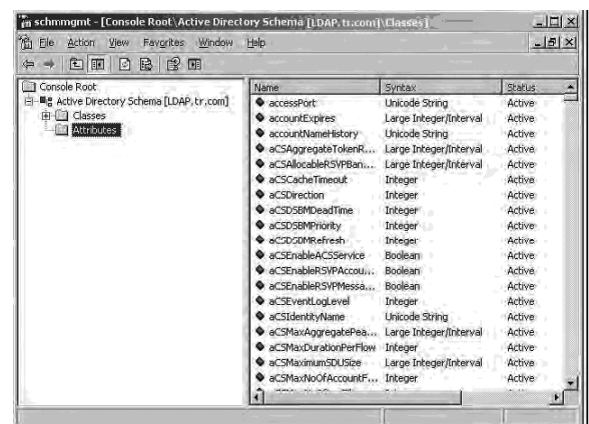
1. On the Windows Server, open the **Support** → **Tools** folder.
2. In the right panel of the dialog box that comes up, double click **SupTools.msi**.
3. Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-In

1. Open a Command prompt.
2. Key in **regsvr32 schmmgmt.dll** to register schmmgmt.dll on your computer.
3. Open the *Start* menu. Click **Run** and key in **mmc /a**. Click **OK**.
4. In the *File* menu of the screen that appears, click **Add/Remove Snap-in**, and then click **Add**.
5. Under *Available Standalone Snap-ins*, double click **Active Directory Schema**, click **Close** and then click **OK**.
6. On the screen you are in, open the *File* menu and click **Save**.
7. When prompted where to save, specify the *C:\Windows\system32* directory.
8. Key in the filename **schmmgmt.msc**.
9. Click **Save** to complete the procedure.

Extend and Update the Active Directory Schema – Create a New Attribute

1. Open **Control Panel** → **Administrative Tools** → **Active Directory Schema**.
2. In the left panel of the screen that comes up, right-click **Attributes**.
3. Select **New** → **Attribute**.



7. Administration *(continued)*

7.2.3 Remote OSD Administration Tab *(continued)*

4. A warning message appears. Click **Continue** to bring up the *Create New Attribute* dialog box.
5. Fill in the dialog box and click **OK**. The *Common Name* and *LDAP Display Name* fields can be populated as *B022-U08-IP-AccessRight* or *B022-U16-IP-AccessRight*. The *Syntax* field should be *Unicode String*, the *Minimum* field should be set to *1*, and the *Maximum* field to *255*.



Extend and Update the Active Directory Schema – Extend the Object Class with the New Attribute

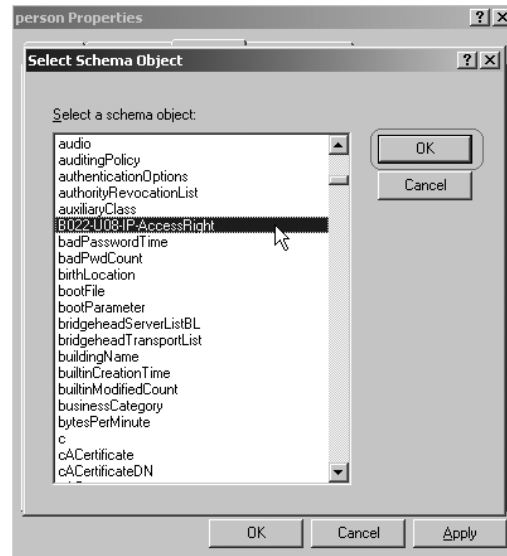
1. Open **Control Panel → Administrative Tools → Active Directory Schema**.
2. In the left panel of the screen that comes up, select *Classes*.
3. In the right panel, right-click **person** and select *Properties*. Select the *General* tab of the *person Properties* screen, and fill in the fields according to the example:



4. Select the *Attributes* tab of the *person Properties* screen and click the **Add** button.

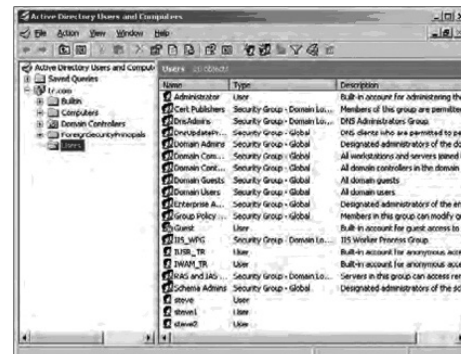


5. Select *B022-U08-IP-AccessRight* or *B022-U16-IP-AccessRight* from the list that appears. Click **OK**.



Extend and Update the Active Directory Schema – Edit Active Directory Users with the Extended Schema

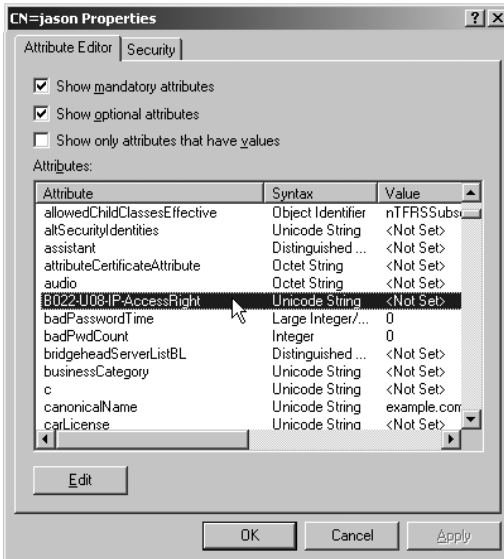
1. Run **ADSI Edit**. (Installed as part of the *Support Tools*).
2. Open **domain**, and navigate to the *cn=users dc=tripplite dc=com* node.
3. Locate and highlight the user you wish to edit. (Our example uses *jason*.)



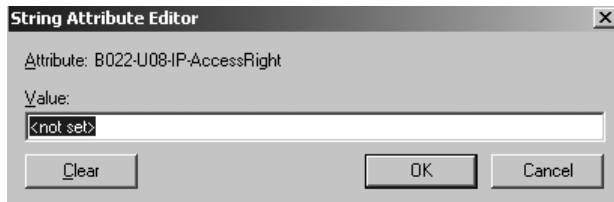
7. Administration *(continued)*

7.2.3 Remote OSD Administration Tab *(continued)*

- Right-click on the user's name and select *properties*.
- Select the *Attribute Editor* tab of the screen that appears. Select *B022-U08-IP-AccessRight* or *B022-U16-IP-AccessRight* from the list that appears. Click **Edit**.



- Replace the value shown with the desired KVM permission attribute value. (See table below for details.)



Permission Attribute Value

The *Permission Attribute Value* is made up of two parts; the IP address of the KVM switch that the user will be accessing and a string of characters that indicates the access rights the user has. The following rules apply to the makeup of the permission attribute value entry:

- An ampersand (&) connects the KVM represented by the IP address to the access rights represented by the string of characters.
- The characters of the access rights string can be entered in either upper or lower case. The available characters and what access rights they represent are listed in the following table.
- Each character in the access rights string is separated by a comma (.). There are no spaces before or after the comma.
- If a user has access rights to more than one KVM, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Character	Description
C	Gives the corresponding account administrator privileges.
W	Gives the corresponding account access to the KVM switch via the Windows browser and non-browser applications.
J	Gives the corresponding account access to the KVM switch via the Java browser and non-browser applications.
L	Gives the corresponding account access to the log server on the Web Management Interface.
V	Gives the corresponding account view-only access to all ports on the KVM switch.
PN/xxxx	Denies the corresponding account access to a port.
SN/xx	Denies the corresponding account access to a station.
PV/xxxx	Gives the corresponding account view-only access to a port.
SV/xx	Gives the corresponding account view-only access to a station.
PF/xxxx	Gives the corresponding account full access to a port.
SF/xx	Gives the corresponding account full access to a station.

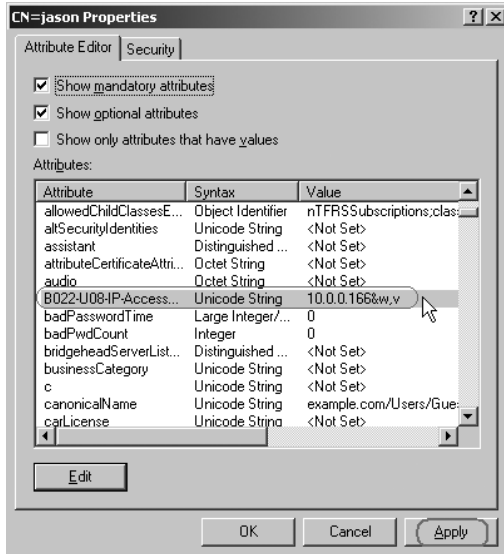
LDAP Server access rights examples are given in the following table:

Access Rights	Description
10.0.0.168&c	The corresponding account has administrator access to the KVM assigned to IP address 10.0.0.168. The account does not have access to any other KVM's administered by the LDAP/S server.
10.0.0.164&c; 10.0.0.166&w,j	The corresponding account has administrator access to the KVM assigned to IP address 10.0.0.164. The corresponding account can access the KVM assigned to IP address 10.0.0.166 via the Windows and Java browser and non-browser applications. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
v,l;10.0.0.164&j	The corresponding account has view-only and log server access rights on all KVMs administered by the LDAP/S server. The corresponding account can access the KVM assigned to IP address 10.0.0.164 via the Java browser and non-browser applications.
10.0.0.168&PN/0102	The corresponding account is denied access to port 2 on station 1 of the KVM chain assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
10.0.0.168&PF/A	The corresponding account is given full access to all ports on the KVM assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
10.0.0.168&SV/02	The corresponding account is given view-only access to station 2 of the KVM chain assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.

7. Administration (continued)

7.2.3 Remote OSD Administration Tab (continued)

- Click **OK**. When you return to the attribute editor page, the *B022-U08-IP-AccessRight* or *B022-U16-IP-AccessRight* entry now reflects the new permissions.



- After entering in the desired KVM permission attribute value, click **Apply** to save the change and complete the procedure.
- Repeat these steps for any other users you wish to assign KVM permissions to.

ANMS – OpenLDAP Server

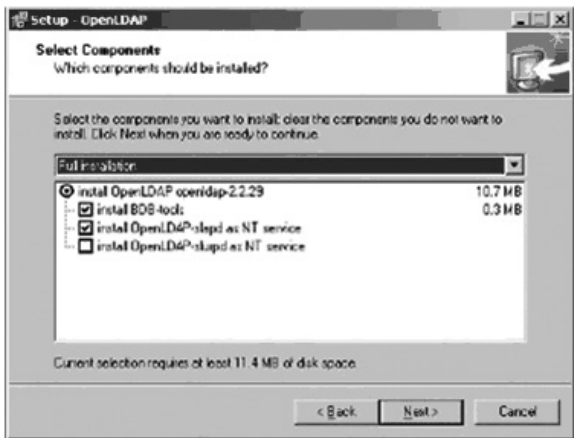
OpenLDAP is an open source LDAP server designed for UNIX platforms. A Windows version can be downloaded from: http://download.bergmans.us/openldap/openldap-2.2.29/openldap-2.2.29-db-4.3.29-openssl-9.8awin32_Setup.exe.

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is:

c:\Program Files\OpenLDAP.

When the Select Components dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service* options.



OpenLDAP Server Configuration

The main OpenLDAP configuration file, *slapd.conf*, has to be customized before launching the server. The modifications to the configuration file will do the following:

- Specify the unicode data directory. The default is *.ucdata*.
- Choose the required LDAP schemas. The core schema is mandatory.
- Configure the path for the OpenLDAP *pid* and *args* start up files. The first contains the server *pid*, the second includes command line arguments.
- Choose the database type. The default is *bdb* (*Berkeley DB*).
- Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix *dc=tripplite,dc=com*, the fully qualified name of all entries in the database will end with *dc=tripplite,dc=com*.
- Define the name of the administrator entry for the server (*rootdn*), along with its password (*rootpw*). This is the server's super user. The *rootdn* name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the *rootdn* is an entry.)

An example configuration file follows:

```
ucdata-path .ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

database bdb
suffix "dc=tripplite,dc=com"
rootdn "cn=Manager, dc=tripplite,dc=com"
rootpw secret
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP Server, run *slapd* (the OpenLDAP Server executable file) from the command line. *slapd* supports a number of command line options, the most important option is the *d* switch that triggers debug information. For example, a command of *slapd -d 256* would start OpenLDAP with a debug level of 256, as shown in the following screenshot:

Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.



7. Administration (continued)

7.2.3 Remote OSD Administration Tab (continued)

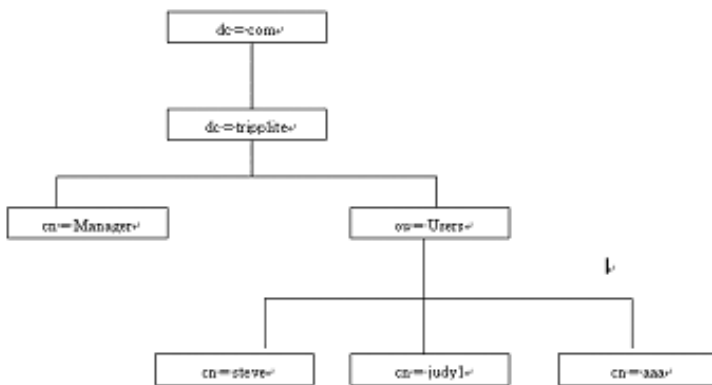
Customizing the OpenLDAP Schema

The schema that *slapd* uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes. In the case of the KVM, the *User* class and the *permission* attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the KVM switch is shown in the following figure:

```
#####
##
## Copyright (C) 2008 TrippLite
## All Rights Reserved.
## Author: Judy
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
#####
* TRIPPLITE OID:=(1.3.6.1.4.1.21317)
*
attributetype (1.3.6.1.4.1.21317.1.1.4.2.2
  NAME 'permission'
  EQUALITY caseIgnoreMatch
  SUBSTYX caseIgnoreSubstringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE)
objectclass (1.3.6.1.4.1.21317.1.1.4.1.2
  NAME 'User'
  SUP organizationalPerson
  STRUCTURAL
  MAY (permission$ userCertificate)
```

LDAP Data Structure

An LDAP directory stores information in a tree structure known as the *Directory Information Tree (DIT)*. The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree is shown in the figure:



DIT Creation

The *LDAP Data Interchange Format (LDIF)* is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The following figure illustrates an LDIF file that creates the DIT for the KVM directory tree:

```
#####
##
## Copyright (C) 2008 TrippLite
## All Rights Reserved.
## Author: Judy
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
#####
dn: dc=trippLite,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization

dn: cn=Manager,dc=trippLite,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: Manager
sn: Manager

dn: ou=Users,dc=trippLite,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Users

dn: cn=steve,ou=Users,dc=trippLite,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: User
cn: steve
sn: steve
permission: w,v,p,i,c,l
userPassword:password
ou: Users
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the KVM.

```
#####
##
## Copyright (C) 2008 TrippLite
## All Rights Reserved.
## Author: Judy
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
#####
dn: cn=judy1,ou=Users,dc=trippLite,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: User
cn: judy1
sn: judy1
userPassword:password

dn: cn=ccc,dc=trippLite,dc=com
objectClass: groupOfNames
cn: ccc
member: cn=judy1,cn=users,dc=trippLite,dc=com

dn: cn=bbb,dc=trippLite,dc=com
objectClass: groupOfNames
cn: bbb
member: cn=ccc,dc=trippLite,dc=com

dn: cn=aaa,dc=trippLite,dc=com
objectClass: groupOfNames
cn: aaa
member: cn=bbb,dc=trippLite,dc=com
```

7. Administration *(continued)*

7.2.3 Remote OSD Administration Tab *(continued)*

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., B022-U08-IP.schema) in the /*OpenLDAP/ schema* directory.
2. Add the new schema to the *slapd.conf* file, as shown in the figure:

```
ucdata-path /ucdata
include /schema/core.schema
include /schema/cosine.schema
include /schema/inetorgperson.schema
include /schema/openldap.schema
include /schema/schema

# Define global ACLs to disable default read access.
access to dn children="ou=Users,dc=tripplite,dc=com"
by dn="cn=Manager,dc=tripplite,dc=com" write
by self read
by anonymous auth
by * none

pidfile /run/slapd.pid
argfile /run/slapd.args

#####
# BDB database definitions
#####

database bdb
suffix "dc=tripplite,dc=com"
rootdn "cn=Manager,dc=tripplite,dc=com"
rootpw secret
directory /data
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in *init.ldif* with the *ldapadd* command, as shown in the following example: *ldapadd -f init.ldif -x -D "cn=Manager,dc=tripplite,dc=com" -w secret*

ANMS – Log Server Settings

Also included in the ANMS screen are settings that are required for the Windows-based log server; *MAC Address* and *Port*. If these settings are not entered correctly, the log server will not be able to communicate with and pull log information from the KVM switch.

- **MAC Address:** Enter the MAC address of the computer that the Windows-based log server was installed on here.
- **Port:** Enter the firewall access port being used to communicate with the Windows-based log server here.

Security

The *Security* page controls IP access by filtering the range of IP addresses and/or MAC addresses that can access the KVM switch. IP and MAC address filters control access to the KVM switch based on the IP and/or MAC addresses of the computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed.

If any filters have been configured, they appear in the *IP filter* and/or *MAC filter* list boxes.

To remove a filter from the list, simply click on it and hit the corresponding *Remove* button.

Note: When clicking the *Remove* button, you are not prompted to confirm the removal of the filter, it is automatically removed.

To edit a filter, simply click on it and hit the corresponding *Edit* button.

Adding/Editing a Filter

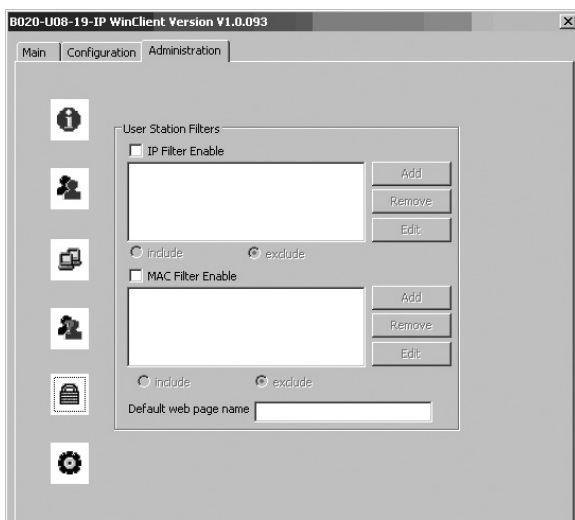
1. Check the *IP Filter Enable* or *MAC Filter Enable* checkbox.
2. Click on the corresponding **Add** button, or highlight the desired filter and click on the corresponding **Edit** button. The *IP Filter* or *MAC Filter* entry box appears.



3. IP filters contain *From* and *To* address fields, which allow you to filter a range of IP addresses. If you only want to filter a single IP address, just enter the same address into both the *From* and *To* fields. MAC filters only allow you to filter one MAC address at a time. If you are adding a new filter, simply fill in the address fields and click OK. If you are editing an existing filter, replace the old address with the correct address and click **OK**.
4. Select the *include* or *exclude* option underneath the filter list. This will determine if all filters in the list are *excluded* from accessing the KVM, or if only those addresses in the list are *included* among those that can access the KVM.

Security – Default Webpage Name

The *Default Webpage Name* (also called a Login String) allows administrators to specify a login string that must be included after the IP address when accessing the KVM via web browser. For example, a default webpage name of *abcdefg* for a KVM with an IP address of 192.168.0.126 would require the following URL to be entered when accessing the KVM via web browser: *192.168.0.126/abcdefg*



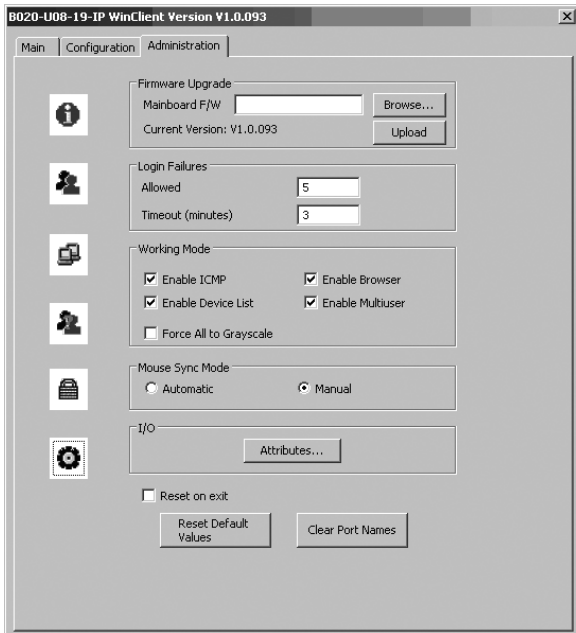
7. Administration *(continued)*

7.2.3 Remote OSD Administration Tab *(continued)*



Customization

The *Customization* screen allows administrators to upgrade the IP firmware of the KVM and configure settings related to KVM operation. The sections that follow discuss the settings you will find on this page.



Customization – Firmware Upgrade

To upgrade the KVM's IP firmware, follow these steps:

1. Download the firmware upgrade file from the Tripp Lite website.
2. Open the *Remote OSD* and navigate to the *Customization* tab.
3. Click the **Browse** button and select the firmware upgrade file you just downloaded from the Tripp Lite website.
4. Click the **Upload** button in the *Customization* tab. A prompt appears to inform you the firmware upgrade process is underway. Upon completion, a prompt will appear stating the upgrade was successful, and that you will need to log out and reset the KVM.
5. Upon logging out of the KVM, a reset is performed to complete the upgrade process.

Customization – Login Failures

- **Allowed:** Enter into this field the number of unsuccessful login attempts that will be allowed from a remote computer.
- **Timeout (minutes):** Enter into this field the number of minutes a user must wait before attempting to login again after exceeding the maximum number of unsuccessful logins.

Customization – Working Mode

The *Working Mode* section allows administrators to toggle particular KVM functions ON/OFF. The table describes the functions that can be controlled:

Function	Description
Enable ICMP	When enabled, the KVM can be pinged and an IP address can be assigned with the ARP command. If it is not enabled, the device cannot be pinged, nor can it be assigned an IP address with the ARP command. The default is Enabled.
Enable Device List	When enabled, the KVM will show up in the list of recognized devices in the non-browser Windows client main screen. If not enabled, the non-browser Windows client will not be able to display it in the list of recognized devices. The default is Enabled.
Force All to Grayscale	When enabled, the remote display for all users and ports is displayed in black and white. In low bandwidth situations, forcing video to grayscale can reduce the amount of data being transferred over the network and improve keyboard/mouse response time. The default is Disabled.
Enable Browser	When enabled, users are able to access the KVM switch via web browser. If browser access is not enabled, users must use either the Windows or Java non-browser clients to access the switch. The default is Enabled.
Enable Multiuser	When enabled, more than one user can log into the KVM at the same time. The default is Enabled. <i>Note: This does not allow multiple users to simultaneously access different ports on the KVM switch, it only allows multiple users to login at the same time. When logged in at the same time, the first user to access the KVM switch will have control of the selected port, and all other users will be able to view that port.</i>

Customization – Mouse Sync Mode

Determines how the local and remote mouse pointer movement becomes synchronized.

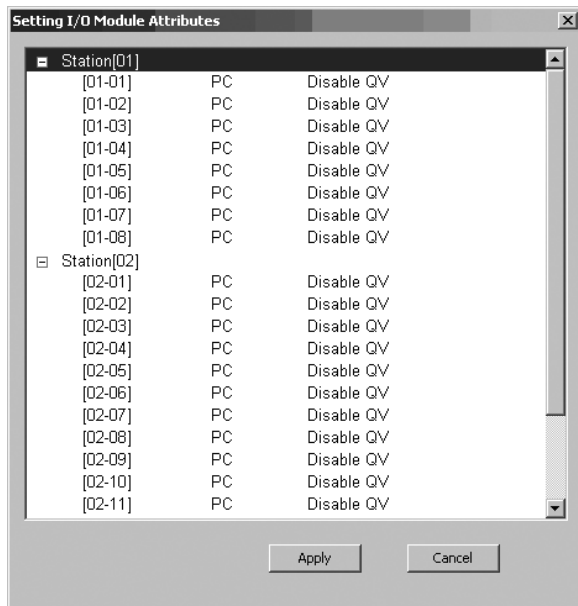
Note: In order to be able to remotely access computers connected to the KVM via the PS/2 connectors on the KVM cable kit, this setting must be set to Manual. It is set to Manual by default.

Selecting *Automatic* provides automatic syncing of the local and remote mouse pointers, eliminating the need to constantly re-sync the two movements manually. If *Automatic* syncing isn't able to keep the pointers in sync, selecting *Manual* provides you with a number of methods to bring them back into sync. (See the Mouse Synchronization section in this manual for details.)

7. Administration (continued)

7.2.3 Remote OSD Administration Tab (continued)

Customization – I/O



Clicking the Attributes button in the I/O panel brings up a dialog box that allows you to set the port operating systems and Quick View ports. These settings can only be edited in the Local Console OSD or the Remote OSD. You will not be able to edit them in the Web Management Interface. The port numbers are listed in the column on the left and the port attributes are shown to the right.

The first column to the right of the port numbers specifies the operating system of the computer connected to the corresponding port. Click on this field to toggle between PC, Mac1, Mac2 and Sun. The default is PC.

Note: If your Mac computer does not respond properly when Mac1 is selected, you should set it to Mac2.

The next column shows whether the corresponding port is a Quick View port. The default is Disable QV. To toggle Quick View status ON/OFF, simply click on this field.

Customization – Reset on Exit, Reset Default Values and Clear Port Names

Reset on Exit

Check the checkbox next to the Reset on Exit option and click the Apply button to set the KVM up for reset upon logging out.

Note: This checkbox is automatically checked when Network settings have been configured. Clearing the check mark before logging out will prevent the Network settings from being implemented; however, the next time you log in, the edited Network settings will still be present and the Reset on Exit checkbox will once again be checked. To avoid Network settings being saved unintentionally, you should always make sure that the information that appears in the Network settings fields is correct before logging out.

Reset Default Values

Click this button to restore all of the OSD settings to their default values.

Clear Port Names

Click this button to delete all of the port names that have been entered in the installation.

7.3 Web Management Interface

When logging into the KVM switch via web browser, you are first taken to the Web Management Interface, with the General Information page displayed. In addition to providing Windows Client and Java Applet applications used in accessing the connected computers, the Web Management Interface allows administrators to configure the KVM switch, view the log file and manage user accounts. This chapter discusses the different sections found in the interface and how you can use them to manage the KVM switch.

7.3.1 General Information

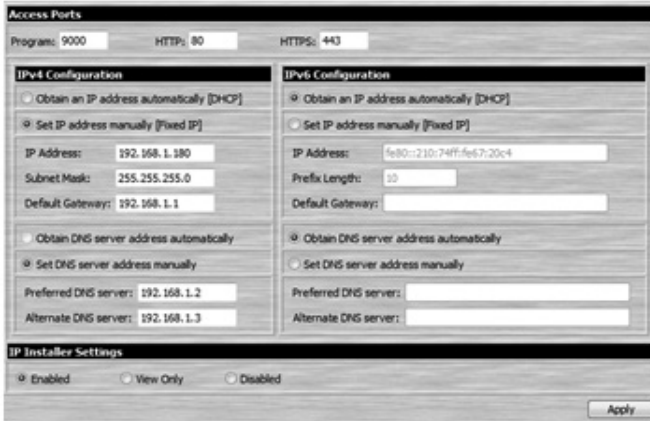
As previously mentioned, the General Information page is the first page you see upon logging into the Web Management Interface. When navigating through the Web Management Interface, you can always display the General Information page by clicking on the icon at the top of the screen. The information on this page is discussed in the table:

Field	Description
Device Name	To make it easier to manage installations that have more than one KVM connected to the network, you are given the option of entering a unique device name. To assign a device name for the KVM switch, simply type the desired name in this field (16 characters max). By default, the device name is the model name of the KVM.
MAC Address	The KVM's MAC address displays here. A MAC address label can also be found on the bottom panel of the console.
Firmware Version	Indicates the current IP firmware version. This firmware controls the IP functionality of the KVM switch, whereas a separate version, upgradeable via the Local Console OSD, controls the basic KVM and console functionality. New firmware files can be downloaded from www.tripplite.com/support as they become available. You can reference this number to see if the version on the website is newer than that on your KVM.
IPv4 Address	Displays the IPv4 address assigned to the KVM. By default, the KVM is set to have an IP address assigned automatically via DHCP server. If connected to a network without a DHCP server, it boots with a default IP address. On IPv4 networks, the default IP is 192.168.0.60 (See the Network section of this manual for details on assigning a fixed IP address).
IPv6 Address	Displays the IPv6 address assigned to the KVM. By default, the KVM is set to have an IP address assigned automatically via DHCP server. If connected to a network without a DHCP server, it boots with a default IP address. The default IPv4 and IPv6 addresses can be found on the sticker on the bottom of the unit.

7. Administration (continued)

7.3.2 Network

Clicking on the *Network* icon at the top of the screen brings you to the *Network* page. From here you can set access ports that will be allowed by a firewall, configure the KVM's IP address and DNS server address, and set the *IP Installer* settings. *IP Installer* settings can only be changed using the *Web Management Interface*.



Access Ports

If a firewall is being used, these fields allow administrators to specify port numbers that the firewall will allow. The firewall must be set to allow access to these ports. If an invalid port number (or no port number) is specified in the firewall, the KVM switch will not be found. An explanation of the ports you can set via this page is given in the table:

Port	Description
Program	This is the port number that must be specified when connecting to the KVM via the AP Windows or Java Client. The default is 9000.
HTTP	This port number is for a browser login. The default is 80.
HTTPS	This port number is for a secure browser login. The default is 443.

Note: A different value must be set for each access port. If there is no firewall, it doesn't matter what these numbers are set to, since they have no effect.

IP Address and DNS Server

The KVM's IP and DNS Server addresses can be assigned automatically by a DHCP server, or given a fixed address by an administrator. By default, the KVM switch is set to have an IP address assigned automatically via DHCP server. If this is the case, you will need to obtain the IP address from your network administrator. If connected to a network without a DHCP server, it boots with a default IP address. The default IPv4 and IPv6 addresses can be found on the sticker on the bottom of the unit. Follow the steps below to configure the KVM's IPv4 or IPv6 settings accordingly, depending on your network.

1. To have the IP address pulled automatically via DHCP server, make sure that the *Obtain an IP address automatically [DHCP]* option is selected.
2. To assign a fixed IP address, make sure the *Use the following IP address [Fixed IP]* option is selected.
3. Fill in the *IPv4 or IPv6 Configuration* fields with information appropriate to your network.
4. If you have set the IP address to be pulled via DHCP server, you can either choose to assign the DNS server address via DHCP as well, or assign a fixed DNS server address. If you have assigned a fixed IP address for the KVM, you must also assign a fixed DNS server address. To have the DNS server address pulled via DHCP server, make sure that the *Obtain DNS server address automatically* option is selected. To assign a fixed DNS server address, make sure that the *Using the following DNS server address* option is selected.
5. Fill in the *Primary DNS server* and *Alternate DNS server* fields with information appropriate for your network.
Note: Specifying the primary DNS Server address is mandatory. The alternate DNS Server address is optional.
6. After all changes have been made, make sure that the *Reset on exit* checkbox in the *Customization* screen is checked. This checkbox should automatically be checked anytime network settings have been changed.
7. Exit the remote session and logout of the KVM switch. Upon logging out of the KVM, a prompt will appear stating the KVM will be reset. Upon completion of the KVM reset, the new network settings will be saved.

7. Administration *(continued)*

7.3.2 Network *(continued)*

IP Installer Settings

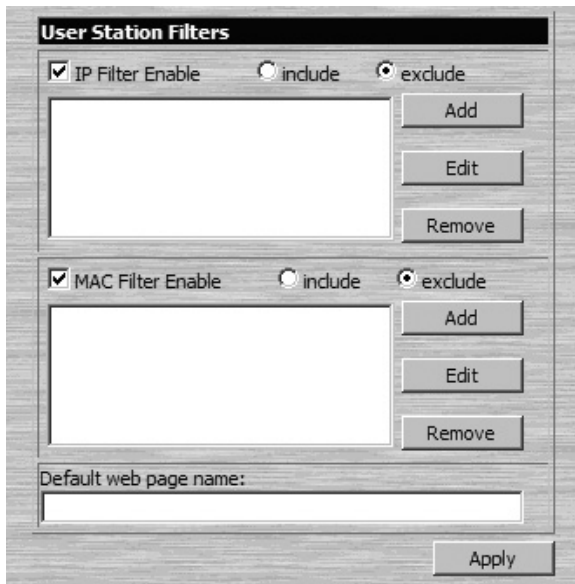
An *IP Installer* utility is provided on the CD that comes with the KVM switch, which gives you a simple way to ascertain and configure the KVM's IP address. When invoked, the *IP Installer* scans the network for devices and displays the ones it finds. The settings found in this page limit what the *IP Installer* is allowed to do. These settings are described in the table:

Setting	Description
Enabled	When this setting is checked, the <i>IP Installer</i> can be used to both view and configure the IP address information of the KVM switch.
View Only	When this setting is checked, the <i>IP Installer</i> can be used to view the IP address information of the KVM switch, but can not be used to configure the IP address.
Disabled	When this setting is checked, the <i>IP Installer</i> is not permitted to view or configure the IP address information of the KVM switch.

Note: After making any network changes, make sure that the Reset on exit checkbox in the Customization page is checked before logging out of the KVM switch. This resets the KVM switch upon logout, allowing network changes to take effect without having to power the unit ON and OFF.

7.3.3 Security

The *Security* page controls IP access by filtering the range of IP addresses and/or MAC addresses that can access the KVM switch. IP and MAC address filters control access to the KVM switch based on the IP and/or MAC addresses of the computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed.



- If any filters have been configured, they appear in the *IP filter* and/or *MAC filter* list boxes.
- To remove a filter from the list, simply click on it and hit the corresponding *Remove* button.

Note: When clicking the Remove button, you are not prompted to confirm the removal of the filter, it is automatically removed.

- To edit a filter, simply click on it and hit the corresponding *Edit* button.

Adding/Editing a Filter

1. Check the *IP Filter Enable* or *MAC Filter Enable* checkbox.
2. Click on the corresponding **Add** button, or highlight the desired filter and click on the corresponding **Edit** button. The *IP Filter* or *MAC Filter* entry box appears.



3. IP filters require you to enter a *Start IP Address* and an *End IP Address*, which allows for ranges of IP addresses to be filtered. If you only want to filter a single IP address, just enter the same address in twice. MAC filters only allow you to filter one MAC address at a time. If you are adding a new filter, simply fill in the address fields and click **OK**. If you are editing an existing filter, replace the old address with the correct address and click **OK**.
4. Select the *include* or *exclude* option next to the *IP Filter Enable* or *MAC Filter Enable* checkbox. This will determine if all filters in the list are *excluded* from accessing the KVM, or if only those addresses in the list are *included* among those that can access the KVM.

Default Webpage Name

In addition to IP and MAC address filtering, the *Security* page allows you to set a *Default Webpage Name* (also called a Login String). The *Default web page name* is a login string specified by an administrator that must be included after the IP address when accessing the KVM via web browser. For example, a default webpage name of *abcdefg* for a KVM with an IP address of 192.168.0.126 would require the following URL to be entered when accessing the KVM via web browser:
192.168.0.126/abcdefg

7. Administration (continued)

7.3.4 ANMS

The Advanced Network Management Settings (ANMS) page allows you to set up login authorization management from an external source. From this screen, administrators can set up remote management via RADIUS and/or LDAP/S, and set up the access port and MAC address for the Windows-based log server.

The screenshot shows the ANMS configuration interface with three main sections:

- RADIUS Settings:** Includes an 'Enable' checkbox, fields for Primary RADIUS Server IP, Alternate RADIUS Server IP, Timeout (seconds) set to 5, Retries set to 3, and a Shared Secret field.
- LDAP Authentication Settings:** Includes an 'Enable' checkbox, radio buttons for LDAP and LDAPS (LDAPS is selected), and an 'Enable Authorization' checkbox. Fields include LDAP Server IP, Port (35), Timeout (seconds) set to 10, LDAP Admin DN, LDAP Admin Password, Search DN, and Admin Group.
- Log Server Settings:** Includes a field for Log Server MAC Address (000000000000) and Port (9001).

RADIUS Settings

To allow authorization for a RADIUS server, do the following:

1. Check the *Enable* checkbox.
2. Fill in the *Primary RADIUS Server IP* and access *Port*, and the *Alternate RADIUS Server IP* and access *Port*.
3. In the *Timeout (seconds)* field, set the time in seconds that the KVM waits for a reply from the RADIUS server before it times out.
4. In the *Retries* field, enter the number of times you want the KVM to try and reconnect with the RADIUS server before it gives up.
5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the KVM and the RADIUS Server.
6. On the RADIUS server, set the access rights for each user according to the information in the table:

Character	Description
C	Gives the corresponding account administrator privileges.
W	Gives the corresponding account access to the KVM switch via the Windows browser and non-browser applications.
J	Gives the corresponding account access to the KVM switch via the Java browser and non-browser applications.
L	Gives the corresponding account access to the log server on the Web Management Interface.
V	Gives the corresponding account view-only access to all ports on the KVM switch.
PN/xxxx	Denies the corresponding account access to a port.
SN/xx	Denies the corresponding account access to a station.
PV/xxxx	Gives the corresponding account view-only access to a port.
SV/xx	Gives the corresponding account view-only access to a station.
PF/xxxx	Gives the corresponding account full access to a port.
SF/xx	Gives the corresponding account full access to a station.

RADIUS Server access rights examples are given in the following table:

RADIUS Access Rights	Description
C	The corresponding account has administrator access to the KVM.
W, J, L	The corresponding account can access the system via the Windows and Java browser and non-browser applications, and can access the log server on the Web Management Interface.
PN/0102	The corresponding account is denied access to port 2 on station 1.
PF/A	The corresponding account is given full access to all ports on the installation.
SV/02	The corresponding account is given view-only access to station 2.

Note: Characters are not case sensitive. Characters are comma delimited.

ANMS – LDAP/S

The screenshot shows the LDAP Authentication settings section:

- Enable LDAP Authentication
- Radio buttons for LDAP and LDAPS (LDAPS is selected).
- Enable Authorization
- LDAP Server IP: []
- Port: 636
- Timeout (seconds): 10
- LDAP Admin DN: []
- LDAP Admin Password: []
- Search DN: []
- Admin Group: []

To allow authentication and authorization via LDAP/S, do the following:

1. Check the Enable LDAP Authentication checkbox.
2. Select LDAP or LDAPS.
3. Determine whether to enable authorization or not.
 - If the *Enable Authorization* checkbox is checked, the LDAP/S server directly returns a 'permission' attribute and authorization for the account that is logging in. With this selection, the LDAP schema must be extended.
 - If the *Enable Authorization* checkbox is not checked, the LDAP/S server indicates whether the account that is logging in is a member of the KVM Admin Group or not. If yes, the account has full access rights. If no, the account has user access rights (See the *User Management* section of this manual for details on account permissions).
4. Enter the appropriate IP address and access port for the LDAP or LDAPS server in the LDAP Server IP and Port fields. The default port number for LDAP is 389, and is 636 for LDAPS.
5. In the *Timeout (Seconds)* field, enter the time in seconds that the KVM waits for an LDAP or LDAPS server reply before it times out.
6. Consult the LDAP/S administrator about the appropriate entry for the *LDAP Administrator DN* field. For example, the entry might look like this: cn=LDAPAdmin,ou=B022-U08-IP,dc=tripplite,dc=com
7. In the *LDAP Admin Password* field, key in the LDAP administrator's password.

7. Administration (continued)

7.3.4 ANMS (continued)

- In the *Search DN* field, set the distinguished name of the search base (i.e. the domain name where the search starts for the user name).
Note: If the Enable Authorization checkbox is not checked, this field must include the entry where the KVM Admin Group is created. Consult the LDAP/S administrator about the appropriate entry for this.
- In the *Admin Group* field, key in the group name for KVM administrator accounts. *Note: If the Enable Authorization checkbox is not checked, this field is used to authorize accounts that are logging in. Accounts that are in this group have full access rights to the KVM. Accounts that are not in this group have user access rights to the KVM (See the User Management section of this manual for details on account permissions). Consult the LDAP/S administrator about the appropriate entry for this.*
- On the LDAP server, set the access rights for each user (The following sections describe how to configure LDAP/S for use with the KVM switch).

LDAP/S Server Configuration

To allow authentication and authorization via LDAP or LDAPS, the active directory's LDAP Schema must be extended so that an extended attribute name for the KVM – *permission* – is added as an optional attribute to the person class.

Note: Authentication refers to the identity verification of the person logging into the KVM switch, whereas Authorization refers to the assigning of device permissions.

In order to configure the LDAP server, you will have to complete the following procedures:

- Install the Windows Support Tools
- Install the Active Directory Schema Snap-In
- Extend and Update the Active Directory Schema

Each of these procedures is described in the following sections:

Install the Windows Support Tools

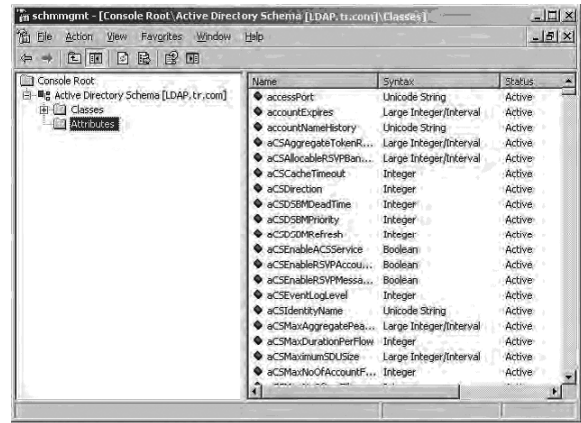
- On your Windows server CD, open the **Support** → **Tools** folder.
- In the right panel of the dialog box that comes up, double click **SupTools.msi**.
- Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-In

- Open a Command prompt.
- Key in **regsvr32 schmmgmt.dll** to register schmmgmt.dll on your computer.
- Open the *Start* menu. Click **Run** and key in **mmc /a**. Click **OK**.
- In the *File* menu of the screen that appears, click **Add/Remove Snap-in**, and then click **Add**.
- Under *Available Standalone Snap-ins*, double click **Active Directory Schema**, click **Close** and then click **OK**.
- On the screen you are in, open the *File* menu and click **Save**.
- When prompted where to save, specify the *C:\Windows\system32* directory.
- Key in the filename **schmmgmt.msc**.
- Click **Save** to complete the procedure.

Extend and Update the Active Directory Schema – Create a New Attribute

- Open **Control Panel** → **Administrative Tools** → **Active Directory Schema**.
- In the left panel of the screen that comes up, right-click **Attributes**.



- Select **New** → **Attribute**.
- A warning message appears. Click **Continue** to bring up the *Create New Attribute* dialog box.



- Fill in the dialog box and click **OK**. The *Common Name* and *LDAP Display Name* fields can be populated as *B022-U08-IP-AccessRight* or *B022-U16-IP-AccessRight*. The *Syntax* field should be *Unicode String*, the *Minimum* field should be set to *1*, and the *Maximum* field to *255*.

7. Administration (continued)

7.3.4 ANMS (continued)

Extend and Update the Active Directory Schema – Extend the Object Class with the New Attribute

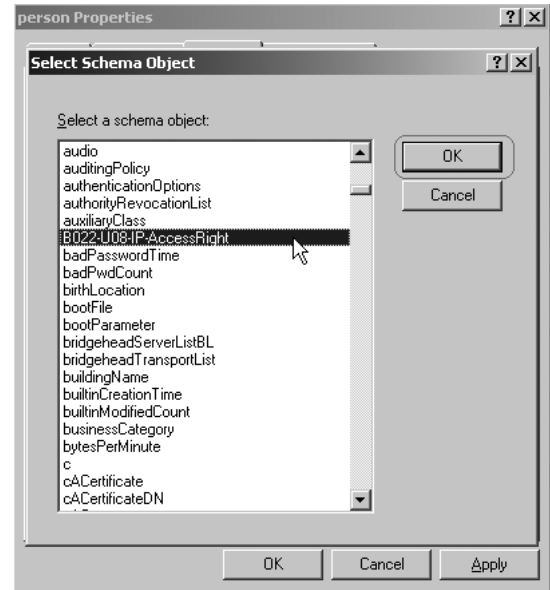
1. Open **Control Panel** → **Administrative Tools** → **Active Directory Schema**.
2. In the left panel of the screen that comes up, select *Classes*.
3. In the right panel, right-click **person** and select *Properties*. Select the *General* tab of the *person Properties* screen, and fill in the fields according to the example:



4. Select the *Attributes* tab of the *person Properties* screen and click the **Add** button.

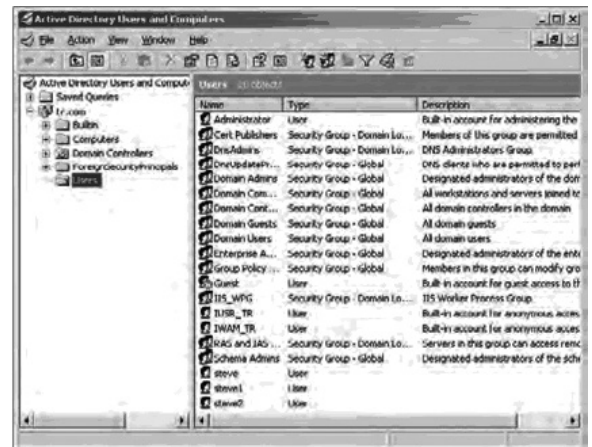


5. Select **B022-U084P-AccessRight** or **B022-U16-IP-AccessRight** from the list that appears. Click **OK**.



Extend and Update the Active Directory Schema – Edit Active Directory Users with the Extended Schema

1. Run **ADSI Edit**. (Installed as part of the *Support Tools*).
2. Open *domain*, and navigate to the *cn=users dc=tripplite dc=com* node.
3. Locate and highlight the user you wish to edit. (Our example uses *jason*.)

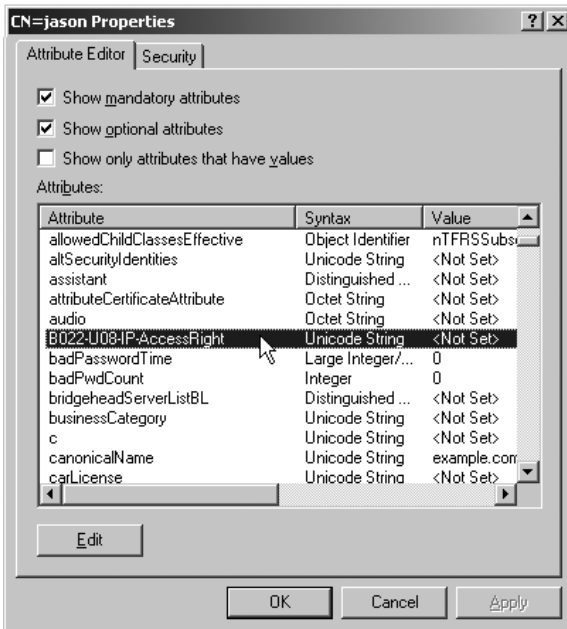


4. Right-click on the user's name and select *properties*.

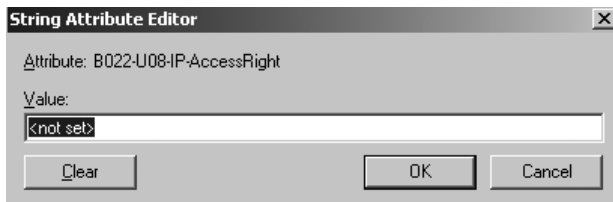
7. Administration *(continued)*

7.3.4 ANMS *(continued)*

- Select the *Attribute Editor* tab of the screen that appears. Select B022-U08-IP-AccessRight or B022-U16-IP-AccessRight from the list that appears. Click **Edit**.



- Replace the value shown with the desired KVM permission attribute value. (See table below for details.)



Permission Attribute Value

The *Permission Attribute Value* is made up of two parts; the IP address of the KVM switch that the user will be accessing and a string of characters that indicates the access rights the user has. The following rules apply to the makeup of the permission attribute value entry:

- An ampersand (&) connects the KVM represented by the IP address to the access rights represented by the string of characters.
- The characters of the access rights string can be entered in either upper or lower case. The available characters and what access rights they represent are listed in the following table.
- Each character in the access rights string is separated by a comma (.). There are no spaces before or after the comma.
- If a user has access rights to more than one KVM, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Character	Description
C	Gives the corresponding account administrator privileges.
W	Gives the corresponding account access to the KVM switch via the Windows browser and non-browser applications.
J	Gives the corresponding account access to the KVM switch via the Java browser and non-browser applications.
L	Gives the corresponding account access to the log server on the Web Management Interface.
V	Gives the corresponding account view-only access to all ports on the KVM switch.
PN/xxxx	Denies the corresponding account access to a port.
SN/xx	Denies the corresponding account access to a station.
PV/xxxx	Gives the corresponding account view-only access to a port.
SV/xx	Gives the corresponding account view-only access to a station.
PF/xxxx	Gives the corresponding account full access to a port.
SF/xx	Gives the corresponding account full access to a station.

LDAP Server access rights examples are given in the following table:

Access Rights	Description
10.0.0.168&c	The corresponding account has administrator access to the KVM assigned to IP address 10.0.0.168. The account does not have access to any other KVMs administered by the LDAP/S server.
10.0.0.164&c; 10.0.0.166&w,j	The corresponding account has administrator access to the KVM assigned to IP address 10.0.0.164. The corresponding account can access the KVM assigned to IP address 10.0.0.166 via the Windows and Java browser and non-browser applications. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
v,l;10.0.0.164&j	The corresponding account has view-only and log server access rights on all KVMs administered by the LDAP/S server. The corresponding account can access the KVM assigned to IP address 10.0.0.164 via the Java browser and non-browser applications.
10.0.0.168&PN/0102	The corresponding account is denied access to port 2 on station 1 of the KVM chain assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
10.0.0.168&PF/A	The corresponding account is given full access to all ports on the KVM assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.
10.0.0.168&SV/02	The corresponding account is given view-only access to station 2 of the KVM chain assigned to IP address 10.0.0.168. The corresponding account does not have access to any other KVMs administered by the LDAP/S server.

7. Administration (continued)

7.3.4 ANMS (continued)

- Click **OK**. When you return to the attribute editor page, the B022-U08-IP-AccessRight or B022-U16-IP-AccessRight entry now reflects the new permissions.



- After entering in the desired KVM permission attribute value, click **Apply** to save the change and complete the procedure.
- Repeat these steps for any other users you wish to assign KVM permissions to.

OpenLDAP Server

OpenLDAP is an open source LDAP server designed for UNIX platforms. A Windows version can be downloaded from: http://download.bergmans.us/openldap/openldap-2.2.29/openldap-2.2.29-db-4.3.29-openssl-9.8awin32_Setup.exe.

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is:

`c:\Program Files\OpenLDAP.`

When the Select Components dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service* options.

OpenLDAP Server Configuration

The main OpenLDAP configuration file, `slapd.conf`, has to be customized before launching the server. The modifications to the configuration file will do the following:

- Specify the unicode data directory. The default is `./ucdata`.
- Choose the required LDAP schemas. The core schema is mandatory.
- Configure the path for the OpenLDAP `pid` and `args` start up files. The first contains the server `pid`, the second includes command line arguments.
- Choose the database type. The default is `bdb` (Berkeley DB).
- Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix `dc=tripplite,dc=com`, the fully qualified name of all entries in the database will end with `dc=tripplite,dc=com`.

- Define the name of the administrator entry for the server (`rootdn`), along with its password (`rootpw`). This is the server's super user. The `rootdn` name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the `rootdn` is an entry.)

An example configuration file is provided:

```
ucdata-path ./ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

database bdb
suffix "dc=tripplite,dc=com"
rootdn "cn=Manager,dc=tripplite,dc=com"
rootpw secret
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP Server, run `slapd` (the OpenLDAP Server executable file) from the command line. `slapd` supports a number of command line options, the most important option is the `d` switch that triggers debug information. For example, a command of `slapd -d 256` would start OpenLDAP with a debug level of 256, as shown in the following screenshot:

Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.



Customizing the OpenLDAP Schema

The schema that `slapd` uses may be extended to support additional syntaxes, matching rules, attribute types and object classes. In the case of the KVM, the `User` class and the `permission` attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the KVM switch is shown in the figure below.

```
#####
##
## Copyright (C) 2008 Tripplite
## All Rights Reserved
## Author: Jody
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
#####
* 'TRIPPLITE OID'=(1.3.6.1.4.1.21317)
*

attributetype (1.3.6.1.4.1.21317.1.1.4.2.3
  NAME 'permission'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE)

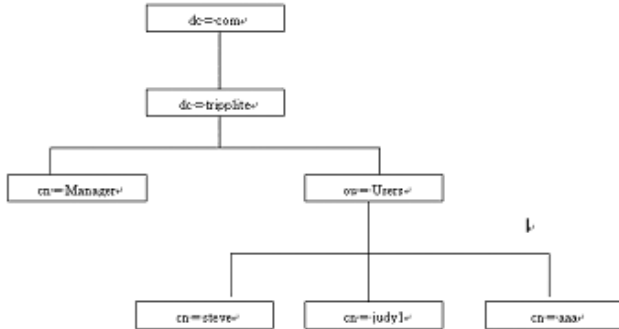
objectclass (1.3.6.1.4.1.21317.1.1.4.1.2
  NAME 'User'
  SUP organizationalPerson
  STRUCTURAL
  MAY (permission$ userCertificate
```

7. Administration (continued)

7.3.4 ANMS (continued)

LDAP Data Structure

An LDAP directory stores information in a tree structure known as the *Directory Information Tree (DIT)*. The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree is shown in the figure below.



DIT Creation

The *LDAP Data Interchange Format (LDIF)* is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure illustrates an LDIF file that creates the DIT for the KVM directory tree.

```
#####
##
##
## Copyright (C) 2008 TrippLite
## All Rights Reserved.
## Author: Judy
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
##
#####

dn: dc=triplite, dc=com
objectclass: top
objectclass: dcObject
objectclass: organization

dn: cn=Manager, dc=triplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Manager
sn: Manager

dn: ou=Users, dc=triplite, dc=com
objectclass: top
objectclass: organizationalUnit
ou: Users

dn: cn=steve, ou=Users, dc=triplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: steve
sn: steve
permission: w,r,p,c,d
userPassword:password
ou: Users
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the KVM:

```
#####
##
##
## Copyright (C) 2008 TrippLite
## All Rights Reserved.
## Author: Judy
## Date: November 27, 2008
## Summary: Define the LDAP schema
##
##
#####

dn: cn=judy1, ou=Users, dc=triplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: judy1
sn: judy1
userPassword:password

dn: cn=ccc, dc=triplite, dc=com
objectclass: groupOfNames
cn: ccc
member: cn=judy1, cn=users, dc=triplite, dc=com

dn: cn=bbb, dc=triplite, dc=com
objectclass: groupOfNames
cn: bbb
member: cn=ccc, dc=triplite, dc=com

dn: cn=aaa, dc=triplite, dc=com
objectclass: groupOfNames
cn: aaa
member: cn=bbb, dc=triplite, dc=com
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., B022-U08-IP.schema) in the / *OpenLDAP/ schema/* directory.
2. Add the new schema to the *slapd.conf* file, as shown in the figure:

```
ucdata-path /ucdata
include /schema/core.schema
include /schema/cosine.schema
include /schema/inetorgperson.schema
include /schema/openldap.schema
include /schema/schema

# Define global ACLs to disable default read access.
access to dn children="ou=Users, dc=triplite, dc=com"
by dn="cn=Manager, dc=triplite, dc=com" write
by self read
by anonymous auth
by * none

pidfile /run/slapd.pid
argfile /run/slapd.args

#####
# BDB database definitions
#####

database bdb
suffix "dc=triplite, dc=com"
rootdn "cn=Manager, dc=triplite, dc=com"
rootpw secret
directory /data
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in *init.ldif* with the *ldapadd* command, as shown in the following example: *ldapadd -f init.ldif -x -D "cn=Manager, dc=triplite, dc=com" -w secret*

Log Server Settings

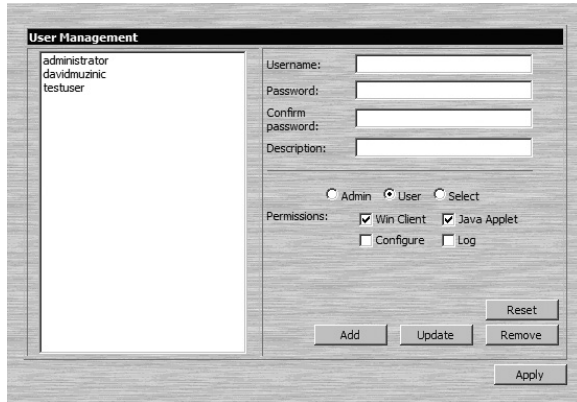
Also included in the *ANMS* screen are settings that are required for the Windows-based log server; *MAC Address* and *Port*. If these settings are not entered correctly, the log server will not be able to communicate with and pull log information from the KVM switch.

- **MAC Address:** Enter the MAC address of the computer that the Windows-based log server was installed on here.
- **Port:** Enter the firewall access port being used to communicate with the Windows-based log server here.

7. Administration (continued)

7.3.5 User Management

The *User Management* page allows administrators to *Add*, *Edit* and *Delete User* and *Administrator* accounts. Up to 64 accounts can be established, with any combination of *Administrators* and *Users*. The *Port Access* settings can not be configured using the *Web Management Interface*, and must be configured via the *Remote OSD*.



- To add a new account, fill in the account information and click the **Add** button. The new account shows up in the list.
- To edit an existing account, highlight it in the list, and then update the account information that appears on the right side of the page. When all information has been updated, click on the **Update** button.
- To delete an existing account, highlight it in the list and click the **Remove** button. When clicking the **Remove** button, you are not asked to confirm whether you want to delete the selected account. It is automatically deleted.
- To clear the account information on the right side of the page without affecting the selected account, click the **Reset** button. In addition to clearing all account information, this de-selects any accounts that were selected prior to clicking the **Reset** button. It's as if you just entered the *User Management* page for the first time.
- When you are done adding, updating or removing information from the *User Management* page, click the **Apply** button to apply your changes.

The table describes the account information fields and settings that are found in the *User Management* page.

Setting	Description
Username	Enter the account username here. A minimum of 6 and a maximum of 16 characters are allowed.
Password	Enter the account password here. A minimum of 6 and a maximum of 16 characters are allowed.
Confirm Password	Re-enter the account password here. If the two entries do not match, you will be prompted to re-type the password.
Description	Additional information about the user that you may wish to include (optional).
Admin	Check this option to give the account <i>Administrator</i> access rights. <i>Administrators</i> have access to all features and configuration settings of the KVM.
User	Check this option to give the account <i>User</i> access rights. <i>Users</i> have access to both the <i>Windows Client</i> and <i>Java Client</i> , but do not have access to the <i>Log Server</i> or <i>Configuration Settings</i> .
Select	Check this option to <i>Select</i> the account access rights yourself. (See <i>Permissions</i> below for details.)

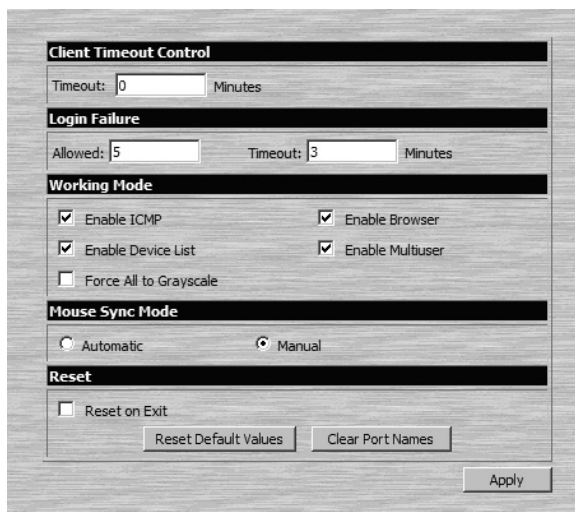
Permissions

The following permissions are included in the *User Management* page, and determine what access rights are available to each account:

- **Win Client:** When selected, the corresponding account can access the KVM switch using the *Windows Client* in the *Web Management Interface* and the non-browser *AP Windows Client*.
- **Java Applet:** When selected, the corresponding account can access the KVM switch using the *Java Applet* in the *Web Management Interface* and the non-browser *AP Java Client*.
- **Log:** When selected, the corresponding account can access the *Log File* included in the *Web Management Interface*.
- **Configure:** When selected, the corresponding account can access the *Administrator* settings in the *Local Console OSD*, *Remote OSD* and *Web Management Interface*.

7.3.6 Customization

The *Customization* screen allows administrators to configure settings related to KVM operation. The sections that follow discuss the settings you will find on this page.



Client Timeout Control

If there is no keyboard/mouse input for the amount of time specified here, the logged-in user is automatically logged out, and must enter their username and password in order to regain access to the KVM switch. The default is 0, which disables the *Timeout* function.

Note: The Timeout function can only be set in the Web Management Interface and the Local Console OSD.

Login Failure

- **Allowed:** Enter into this field the number of unsuccessful login attempts that will be allowed from a remote computer.
- **Timeout (minutes):** Enter into this field the number of minutes a user must wait before attempting to log in again after exceeding the maximum number of unsuccessful logins.

7. Administration *(continued)*

7.3.6 Customization *(continued)*

Working Mode

The *Working Mode* section allows administrators to toggle particular KVM functions ON/OFF. The table describes the functions that can be controlled:

Function	Description
Enable ICMP	When enabled, the KVM switch can be pinged and an IP address can be assigned with the ARP command. If it is not enabled, the device cannot be pinged, nor can it be assigned an IP address with the ARP command. The default is Enabled.
Enable Device List	When enabled, the KVM switch will show up in the list of recognized devices in the AP Windows Client main screen. If not enabled, the AP Windows Client will not be able to display it in the list of recognized devices. The default is Enabled.
Force All to Grayscale	When enabled, the remote display for all users and ports is displayed in black and white. In low bandwidth situations, forcing video to grayscale can reduce the amount of data being transferred over the network and improve keyboard/mouse response time. The default is Disabled.
Enable Browser	When enabled, users are able to access the KVM switch via web browser. If browser access is not enabled, users must use either the AP Windows or Java clients to access the switch. The default is Enabled.
Enable Multiuser	When enabled, more than one user can log into the KVM switch at the same time. The default is Enabled. <i>Note: This does not allow multiple users to simultaneously access different ports on the KVM switch, it only allows multiple users to log in at the same time. When logged in at the same time, the first user to access the KVM switch will have control of the selected port, and all other users will be able to view that port.</i>

Mouse Sync Mode

Determines how the local and remote mouse pointer movement becomes synchronized.

Note: In order to be able to remotely access computers connected to the KVM via the PS/2 connectors on a KVM cable kit, this setting must be set to Manual. It is set to Manual by default.

Selecting *Automatic* provides automatic syncing of the local and remote mouse pointers, eliminating the need to constantly re-sync the two movements manually. If *Automatic* syncing isn't able to keep the pointers in sync, selecting *Manual* provides you with a number of methods to bring them back into sync. (See the Mouse Synchronization section of this manual for details.)

Reset

Reset on Exit

Check the checkbox next to the *Reset on Exit* option and click the **Apply** button to set the KVM up for reset upon logging out.

Note: This checkbox is automatically checked when Network settings have been configured. Clearing the check mark before logging out will prevent the Network settings from being implemented; however, the next time you log in, the edited Network settings will still be present and the Reset on Exit checkbox will once again be checked. To avoid Network settings being saved unintentionally, you should always make sure that the information that appears in the Network settings fields is correct before logging out.

Reset Default Values

Click this button to restore all of the OSD settings to their default values.

Clear Port Names

Click this button to delete all of the port names that have been entered in the installation.

7. Administration (continued)

7.3.7 Maintenance

The *Maintenance* page allows administrators to upgrade the IP firmware of the KVM switch, as well as backup and restore the KVM configuration settings and user profiles.

Note: The Backup and Restore functions can only be performed using the Web Management Interface.

Firmware Upgrade

To upgrade the KVMs IP firmware, follow the steps below:

1. Download the firmware upgrade file from www.tripplite.com/support.
2. Open the *Web Management Interface* and navigate to the *Maintenance* page.
3. Click the **Browse** button and select the firmware upgrade file you just downloaded from the Tripp Lite website.
4. Click the **Upload** button. A prompt appears to inform you the firmware upgrade process is underway. Upon completion, a prompt will appear stating the upgrade was successful, and that you will need to log out and reset the KVM.
5. Upon logging out of the KVM, a reset is performed to complete the upgrade process.

Backup Configuration / User Accounts

This section of the page gives you the ability to back up the KVM's configuration settings and user profile information.

To perform a backup, do the following:

1. Enter a password into the *Password* field. This password will be required when using the backup file to restore the KVM configuration settings and/or user profile information.
2. Select what type of backup you wish to create; *Backup Configuration*, *Backup User Accounts*, *Backup Port Names*, or *Backup All*.
3. Click the **Save** button to create the backup file.
4. A prompt will appear asking if you want to save the file or find a program to open it. Click the **Save** button, give the file a unique name and save it in a convenient location.

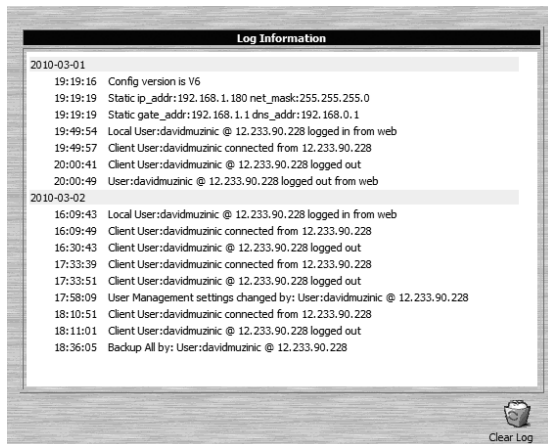
Restore Configuration / User Accounts

To erase the configuration settings and/or user profile information currently stored on the KVM and replace it with that from a backup file, do the following:

1. In the *Password* field, key in the password that you entered when creating the backup file.
2. Click the **Browse** button, navigate to the backup file and select it.
3. After selecting the backup file, click the **Restore** button. After the file is restored, a message appears to inform you that the procedure succeeded.

7.3.8 Log

Important transactions that occur on the KVM switch, such as logins and internal status messages, are kept in an automatically generated log file located in the *Web Management Interface*. In addition to this, a more expansive, searchable Windows-based *Log Server* is included in the CD that comes with the KVM. See the *Log Server* section of this manual for details.) To view the built-in log file, simply click on the *Log* icon on the left side of the *Web Management Interface* screen.



A maximum of 512 events are kept in this log file. New events are recorded and placed at the bottom of the list, whereas older events are placed at the top of the list. When a new event is recorded after there are already 512 events in the log file, the oldest record is discarded to make room for the new one. To clear the log file, click on the **Clear Log** icon in the lower-right corner of the screen.

7. Administration *(continued)*

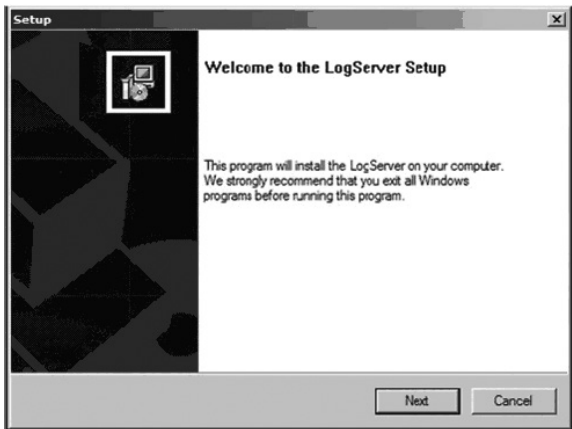
7.4 Log Server

The Windows-based *Log Server* is an administrative utility that records all the events that take place on the selected unit and writes them to a searchable database. This chapter describes how to install and configure the *Log Server*.

Note: The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to function properly.

To install the *Log Server*, do the following:

1. From the computer that you want to use to host the *Log Server*, open the CD that came with the KVM switch and open the *Log Server Installer* file. If any security warning dialog boxes appear, ignore them and click **Run** or **Open**. A *Log Server* setup screen appears.



2. Click the **Next** button, and then follow the on-screen instructions to complete the installation and have the *Log Server* program icon placed on your desktop.
3. After installation, and before opening the *Log Server* for the first time, go to the *ANMS* page in the *Web Management Interface* or *Remote OSD* and enter the MAC address of the computer you installed the *Log Server* on and an access port that can be used to get through a firewall. (See *ANMS* section of this manual for details.)
4. Double-click the *Log Server* desktop icon. The first time you open the *Log Server*, a screen similar to the one below appears:



The screen is divided into three components:

- A Menu Bar at the top.
- A panel that will contain a list of all KVM units in the middle.
- A panel that will contain an Events List at the bottom.

Menu Bar

The Menu bar consists of four drop-down menus:

- Configure
- Events
- Options
- Help

Configure

The *Configure* menu consists of three functions; *Add*, *Edit* and *Delete*.

Add

Select the *Add* function when you need to add a new KVM to the list of units that the *Log Server* records events for.

Note: You must first add a KVM via the Add function before the Log Server can start recording its events.

When you open the *Add* function the following dialog box will appear:



Descriptions of the fields in this dialog box are shown in the table:

Field	Description
Address	This can either be the IP address of the KVM or its DNS name (if the network administrator has assigned it a DNS name). This value must be entered into the ANMS settings screen in order for the KVM to communicate with the <i>Log Server</i> . (See the <i>ANMS</i> section of this manual for details.)
Port	Key in the port number that was specified in the <i>Log Server</i> portion of the <i>ANMS</i> settings screen. If this differs from the port entered in the <i>ANMS</i> settings screen, the <i>Log Server</i> will not be able to communicate with the KVM.
Description	This field is provided so that you can enter in additional information that will help differentiate this KVM switch from all other KVMs that the <i>Log Server</i> is recording information for.
Limit	This specifies the number of days that an event is kept in the database before it can be deleted. To remove all events that have passed the expiration date set in this field, use the <i>Maintenance</i> function in the <i>Events</i> menu.

Edit

Select the *Edit* function when you need to change the information for an existing KVM switch. To edit an existing KVM, simply highlight it in the *Log Server* list and open the *Edit* function from the *Configure* menu. A dialog box will appear that shows the exact information that was entered for the KVM when it was added using the *Add* function. Edit this information and click **OK**.

Delete

To delete a KVM switch, simply highlight it in the *Log Server* list and open the *Delete* function from the *Configure* menu. A dialog box will appear which will display the KVMs information and ask you to click **OK** to delete it. If you want to remove it from the list of KVMs being tracked by the *Log Server*, click **OK**.

7. Administration (continued)

7.4 Log Server (continued)

Events

The *Events* menu consists of two items; *Search* and *Maintenance*.

Search

Search allows you to search for events containing specific words or strings. When you access this function, a screen similar to the one that follows appears:



A description of the items from the *Search* screen is given in the table:

Item	Description
Search Options	<p>New search: When selected, the search is performed on all the events in the database for the selected KVM.</p> <p>Search last results: This is a secondary search performed on the events that resulted from the last search.</p> <p>Search excluding last results: This is a secondary search performed on all the events in the database for the selected KVM excluding the events that resulted from the last search.</p>
Server List	KVM switches are listed in the <i>Log Server</i> list according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority List	<p>Determines what types of search results are displayed, according to their level of importance to the security of the installation; <i>Most</i>, <i>Medium</i> or <i>Least</i>. If nothing is selected, all results will display, and they will be color-coded according to level of importance:</p> <ul style="list-style-type: none"> Most important: Entries highlighted in red are the most relevant to the security of the installation. Medium importance: Entries highlighted in blue are somewhat relevant to the security of the installation. Least importance: Entries highlighted in black are least relevant to the security of the installation.
Start Date	Select the date that you want the search to start from. The format follows the MM/DD/YYYY convention (e.g. 11/04/2012).
Start Time	Select the time that you want the search to start from.
End Date	Select the date that you want the search to end. The format follows the MM/DD/YYYY convention (e.g. 11/04/2012).
End Time	Select the time that you want the search to end.
Pattern	Key in text here that you want the search to filter the events by.
Results	The events that matched your search terms are listed here.
Search	After you have entered in all of your search terms, click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to export search results as a text file.
Exit	Click this button to exit the <i>Search</i> dialog box.

Maintenance

This function allows the Administrator to remove all records that have passed their expiration limit. In order to delete old files from the log server, the maintenance function must be performed.

Options

The *Options* menu consists of only one function: *Network Retry*.

Network Retry

Network Retry allows you to set the number of seconds that the *Log Server* should wait before attempting to connect in the event that the previous connection attempt failed. When you click this item, a dialog box appears:

Key in the desired number of seconds and click **OK** to finish.



Help

The *Help* menu consists of two options: *Contents* and *About Log Server*.

Contents

Selecting the *Contents* function will bring up an online help file. The help file contains instructions about how to setup, operate and troubleshoot the *Log Server*.

About Log Server

Selecting the *About Log Server* option will pull up a dialog box that gives you the version number of the *Log Server*.

The Log Server Main Screen

The *Log Server Main Screen* is divided into two main panels: an upper (List) panel that displays all of the KVM switches that have been added to the *Log Server* and a lower (Event) panel that displays the log events for the currently selected KVM. To select a KVM from the list, simply click on it.



7. Administration *(continued)*

7.4 Log Server *(continued)*

The List Panel

The *List panel* contains the following fields:

Field	Description
Recording	Determines whether the <i>Log Server</i> records log events for the corresponding KVM switch. If this checkbox is checked, the field displays <i>Recording</i> , and log events are recorded. If this checkbox is not checked, the field displays <i>Paused</i> , and log events are not recorded for the corresponding KVM. <i>Note: Even if a KVM is not currently selected, if its Recording checkbox is checked, the Log Server will still record its log events.</i>
Address	This is the IP address or DNS name that was given to the KVM switch when it was added to the <i>Log Server</i> .
Port	This is the port number that was assigned to the KVM switch when it was added to the <i>Log Server</i> .
Connection	If the <i>Log Server</i> is connected to the corresponding KVM switch, this field displays <i>Connected</i> . If it is not connected, this field displays <i>Waiting</i> . A connection status of <i>Waiting</i> means that the <i>Log Server</i> is not communicating with the KVM, and will not record its events. This occurs when the <i>Log Server's</i> MAC address and/or port number have not been set properly. The MAC address and port for the <i>Log Server</i> computer must be entered into the KVM's <i>ANMS</i> settings screen. In addition, the KVM's IP address and port must be entered when adding it to the <i>Log Server</i> . If the port numbers in the <i>ANMS</i> menu and the <i>Log Server</i> do not match, the two will not be able to communicate.
Days	This field displays the number of days that the KVM's log events are to be kept in the database before it is eligible for deletion.
Description	This field displays the descriptive information entered for the corresponding KVM switch when it was added to the <i>Log Server</i> .

The Event Panel

The lower panel displays event information for the currently selected KVM switch.

8. Specifications

Specification	B022-U08-IP	B022-U16-IP
Computer Ports	(x8) HD18 (Female)	(x16) HD18 (Female)
KVM Cable Kit Model	P778-Series	P778-Series
KVM Cable Kit Connectors	KVM Side: HD18 (Male) Computer Side: HD15 (Male), USB A (Male), (x2) PS/2 (Male)	KVM Side: HD18 (Male) Computer Side: HD15 (Male), USB A (Male), (x2) PS/2 (Male)
Included Cable Kits	(x2) P778-006 (6 ft.)	(x2) P778-006 (6 ft.)
Port Selection	OSD, Hotkey, Pushbutton	OSD, Hotkey, Pushbutton
External Console Ports	HD18 (Male)	HD18 (Male)
External Console Cable	Yes	Yes
External Console Cable Connectors	KVM Side: HD18 (Female) Computer Side: HD15 (Female), (x2) USB A (Female), (x2) PS/2 (Female)	KVM Side: HD18 (Female) Computer Side: HD15 (Female), (x2) USB A (Female), (x2) PS/2 (Female)
Additional USB Ports	1	1
Additional USB Ports Version	1	1
LAN Port	RJ45 (Female)	RJ45 (Female)
Firmware Upgrade Port	RJ11 (Female)	RJ11 (Female)
Port Selection Pushbuttons	8	16
Reset Button	Semi-Recessed Pushbutton	Semi-Recessed Pushbutton
Max Resolution Supported	Local Monitor: 2048 x 1536 Remote Monitor: 1600 x 1200 @ 60Hz	Local Monitor: 2048 x 1536 Remote Monitor: 1600 x 1200 @ 60Hz
Power On/Off Switch	No	No
Included Power Cord	Yes (External Power Supply)	Yes (External Power Supply)
Power Consumption	DC 5.3V, 9.5W	DC 5.3V, 11W
Power I/P Rating	100-240V, 50/60Hz, 0.5A	100-240V, 50/60Hz, 0.5A
Operating Temperature	0 to 50 C (32 to 122 F)	0 to 50 C (32 to 122 F)
Storage Temperature	-20 to 60 C (-4 to 140 F)	-20 to 60 C (-4 to 140 F)
Humidity	0 to 80% RH, Non-Condensing	0 to 80% RH, Non-Condensing
Dimensions (H x W x D, in.)	1.73 x 17 x 6	1.73 x 17 x 6
Weight (lbs.)	6.1	6.5

8. Specifications









8.1 OSD Default Settings

Setting	Default
OSD Language	English
OSD Hotkey	[Scroll Lock] [Scroll Lock]*
Port ID Display Position	Upper Left Corner
Port ID Display Duration	3 Seconds
Port ID Display Mode	The Port Number plus the Port Name
Scan Duration	5 Seconds
Scan/Skip Mode	All
Screen Blanker	0 (Disabled)
Logout Timeout	0 (Disabled)
Accessible Ports	F (Full) for all users on all ports
Beeper	Y (Activated)
IP Address	Obtain Automatically (DHCP)
IP Installer	Enabled
Working Mode	Enable ICMP, Enable Device List, Enable Browser and Enable Multiuser
Mouse Sync Mode	Manual

8.2 Keyboard Emulation

Mac Keyboard








The PC compatible (101/104 key) keyboard can emulate the functions of the Mac keyboard. The emulation mappings are listed in the table:

PC Keyboard	Mac Keyboard
[Shift]	[Shift]
[Ctrl]	[Ctrl]
	
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Alt]	[Alt]
[Print Screen]	[F13]
[Scroll Lock]	[F14]
	[=]
[Enter]	[Return]
[Backspace]	[Delete]
[Insert]	[Help]
[Ctrl] 	[F15]

Note: When using key combinations, press and release the first key and then press and release the second key.

Sun Keyboard

The PC compatible (101/104 key) keyboard can emulate the functions of the Sun keyboard when the [Ctrl] key is used in conjunction with other keys. The corresponding functions are shown in the table:

PC Keyboard	Sun Keyboard
[Ctrl] [T]	[Stop]
[Ctrl] [F2]	[Again]
[Ctrl] [F3]	[Props]
[Ctrl] [F4]	[Undo]
[Ctrl] [F5]	[Front]
[Ctrl] [F6]	[Copy]
[Ctrl] [F7]	[Open]
[Ctrl] [F8]	[Paste]
[Ctrl] [F9]	[Find]
[Ctrl] [F10]	[Cut]
[Ctrl] [1]	
[Ctrl] [2]	
[Ctrl] [3]	
[Ctrl] [4]	
[Ctrl] [H]	[Help]
	[Compose]
	

Note: When using key combinations, press and release the first key and then press and release the second key.

9. Warranty & Product Registration

1-YEAR LIMITED WARRANTY

TRIPP LITE warrants its products to be free from defects in materials and workmanship for a period of one (1) year from the date of initial purchase. TRIPP LITE's obligation under this warranty is limited to repairing or replacing (at its sole option) any such defective products. To obtain service under this warranty, you must obtain a Returned Material Authorization (RMA) number from TRIPP LITE or an authorized TRIPP LITE service center. Products must be returned to TRIPP LITE or an authorized TRIPP LITE service center with transportation charges prepaid and must be accompanied by a brief description of the problem encountered and proof of date and place of purchase. This warranty does not apply to equipment which has been damaged by accident, negligence or misapplication or has been altered or modified in any way. EXCEPT AS PROVIDED HEREIN, TRIPP LITE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some states do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser. EXCEPT AS PROVIDED ABOVE, IN NO EVENT WILL TRIPP LITE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Specifically, TRIPP LITE is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise.

PRODUCT REGISTRATION

Visit www.tripplite.com/warranty today to register your new Tripp Lite product. You'll be automatically entered into a drawing for a chance to win a FREE Tripp Lite product!*

* No purchase necessary. Void where prohibited. Some restrictions apply. See website for details.

FCC Notice, Class A

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. The user must use shielded cables and connectors with this equipment. Any changes or modifications to this equipment not expressly approved by Tripp Lite could void the user's authority to operate this equipment.

WEEE Compliance Information for Tripp Lite Customers and Recyclers (European Union)



Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Tripp Lite they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice.

