Warranty Registration: register online today for a chance to win a FREE Tripp Lite product—www.tripplite.com/warranty

Owner's Manual

NetCommander™ IP Console KVM Switch

Model:

B070-016-19-IP

Table of Contents

TRIPP·LITE

90 YEARS

Manufacturing Excellence.

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

1. Introduction

Tripp Lite's NetCommander™ IP Console KVM Switch is ideal for controlling multiple servers over inexpensive Cat5e cable from a single console (keyboard, mouse and display). It includes the following premium features:

- 16-port IP KVM switch with built-in keyboard, monitor and touch pad console
- Access and control multiple computers from a single console (local or remote).
- Achieves BIOS-level control of any server, regardless of server condition and network connectivity.
- Compatible with all major operating systems.*
- Supports many hardware and software configurations for the remote client, target server and KVM switch, including USB and PS/2 port connections.
- Secures control of target server from any location via Web browser and standard IP connection.
- Allows up to 5 users to share a remote session.
- Supports the highest security standards for encryption (256-bit AES and HTTPS) and authentication for remote users. Advanced OSD management with multi-layer security for local users.
- Uses inexpensive and commonly available Cat5 patch cables (maximum distance 100 ft.) to connect to each computer.

** Mac computers can be connected to the KVM, but they can only be accessed via the local console. Mac computers cannot be remotely accessed, nor can they be used to remotely access connected computers. UNIX-based computers can be connected to the KVM, and they can be accessed either locally or remotely. They cannot be used to remotely access connected computers.*

2. Important Safety Instructions

SAVE THESE INSTRUCTIONS

This manual contains instructions and warnings that should be followed during the installation and operation of this product. Failure to comply may invalidate the warranty and cause property damage and/or personal injury.

Installation Warnings

- Install the KVM switch in a controlled indoor environment, away from moisture, temperature extremes, flammable liquids and gasses, conductive contaminants, dust and direct sunlight.
- Operate the KVM switch at indoor temperatures between 32° F and 104° F (0° C and 40° C).
- When connecting the KVM switch to the facility's power supply circuit, ensure that the circuit is not overloaded.

Rackmount Warnings

- Ensure there is adequate airflow within the rack.
- Mount the KVM switch evenly within the rack to eliminate potentially hazardous uneven mechanical loading conditions.
- Ensure all rackmount equipment is reliably grounded.

Connection Warnings

- 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.
- Ensure that the cables used with the KVM switch are not close to any sources of electrical noise interference such as fluorescent lights, HVAC systems or motors.
- Ensure that the distance between any computer and the KVM switch does not exceed 100 ft.
- Shut down all PS/2 computers before connecting the keyboard, monitor and mouse to ensure they will be recognized by the computer.

Maintenance Warnings

- The KVM switch does not require routine maintenance. There are no user-serviceable parts inside. Only authorized service personnel should open the case for any reason. Disconnect the unit from AC input power before servicing.

3. System Components

The NetCommander IP Console KVM Switch consists of:

- B070-016-19-IP Console KVM Switch
- Rackmount hardware
- 1 serial download cable (DB9 Female to RJ11 Male) for firmware upgrades
- Jumper Cable to connect the Integrated Console Ports and KVM Console Ports
- C13 to 5-15P Power Cord
- Owner's Manual CD

Accessories, available separately from Tripp Lite, include:

- Server interface units (SIU)–PS/2 (model # B078-101-PS2) or USB (model # B078-101-USB)
- Cat5/6 cables (Tripp Lite model # series: N001-, N002-, N201-, N202- or N105-)

4. Compatibility

Connected Computers

- PS/2 and USB computers/servers
- Computers/servers with a HD15 (VGA) port
- All major operating systems*

Computers Remotely Accessing KVM

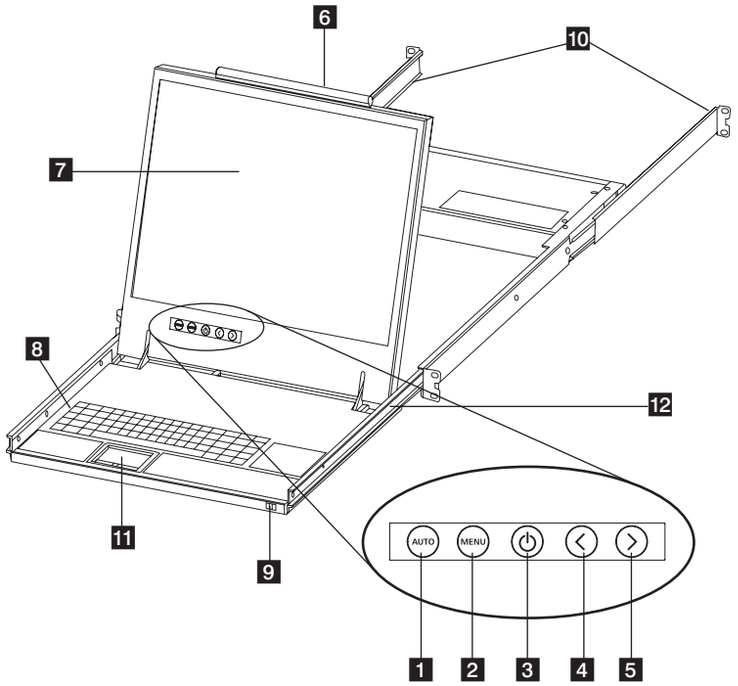
- Supports Windows and 32-bit Linux operating systems
- Windows operating systems can use any 32-bit browser; 64-bit browsers are not supported
- 32-bit Linux operating systems can use Firefox 32-bit; Firefox 64-bit is not supported

**Note:*

1. *Mac computers can be connected to the KVM, but they can only be accessed via the local console. Mac computers cannot be remotely accessed, nor can they be used to remotely access connected computers.*
2. *UNIX-based computers can be connected to the KVM, and they can be accessed either locally or remotely. They cannot be used to remotely access connected computers.*

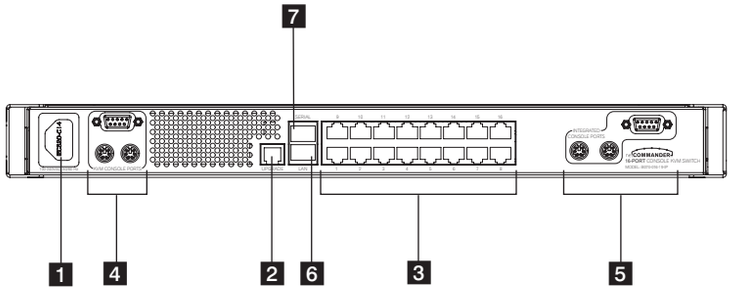
5. Features

Front View



1. **Auto:** When the LCD Menu is closed, pressing the AUTO button will perform an Auto Adjust on the monitor screen. When the LCD Menu is open, pressing the AUTO button will bring you back to the previous screen/selection. If the LCD Menu cannot go back any further, the AUTO button will close down the menu.
2. **Menu:** When the LCD Menu is closed, pressing the MENU button will open it. When the LCD Menu is open, pressing the MENU button will select a highlighted option.
3. **On/Off Button:** Pressing this button will turn the monitor screen on or off.
4. **< :** When the LCD Menu is open, pressing the < button will move the highlight bar to the left. When modifying a selected option, pressing the < button will decrease the option.
5. **> :** When the LCD Menu is open, pressing the > button will move the highlight bar to the right. When modifying a selected option, pressing the > button will increase the option.
6. **Handle:** Pull to slide the module out; push to slide the module in.
7. **19" LCD Monitor:** After sliding the module out, flip up the cover to access the LCD monitor, keyboard and touch pad.
8. **Keyboard**
9. **Slide Release:** Mechanism to lock the drawer closed when the console is not in use. Prevents it from accidentally sliding open. To slide the console out, you must first release it by moving the tab sideways.
10. **Rackmounting Brackets:** There are rackmount brackets to secure the chassis to a system rack located at each corner of the unit.
11. **2-Button Touch Pad:** Left button is left click, right is right click.
12. **Railway Release Tabs:** When the drawer is completely pulled out to the end, the railway system will lock. Push the release tabs on both sides to release the drawer so that it can be pushed back in.

Back View



1. **Power Socket:** The power cord from the AC power source plugs in here.
2. **Firmware Upgrade Port:** Plug the included firmware cable into this port to download firmware upgrade data.
3. **CPU Port Section:** Plug Cat5e cables from each PC or server into these ports.
4. **KVM Console Ports***
5. **Integrated Console Ports***
6. **LAN Port:** This RJ45 port enables connection to 10/100mb Ethernet. The LINK LED illuminates to indicate a LAN connection. The REMOTE LED illuminates to indicate that a remote session is in progress.
7. **Serial Port:** The serial port is not currently functional. It is provided for possible functionalities that may be made available in future firmware upgrades.

** The B070-016-19-IP comes with a jumper cable to connect the KVM Console Ports and the Integrated Console Ports. This cable must be connected for the KVM switch to function.*

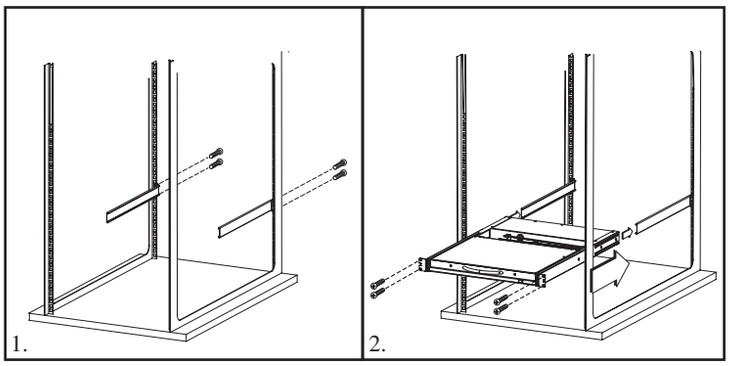
6. Rackmount Installation

The B070-016-19-IP is designed for mounting in a 1U rack system. For convenience, a rack mounting kit is included with your B070-016-19-IP for quick installation. The various mounting options are explained in the sections that follow.

Standard Rackmounting

The standard rackmounting brackets that come attached to the B070-016-19-IP allow the unit to be installed in standard 1U racks by a single individual.

1. Slide out the rear mounting brackets from the console and mount both brackets (separate from the console) to the inside rear of a standard 1U rack system using user-supplied screws.
2. Take the console and gently slide it into the two rear-mounted brackets in the rack and secure the console in place by inserting user-supplied screws.



2-Post Rackmounting

The B070-016-19-IP can also be mounted in a 2-post rack installation using the optional 2-Post Rackmount Kit (model #: B019-000). The mounting hardware allows for the console to be opened with the drawer in any position. Heavy-duty 14-gauge steel provides stability and prevents the console frame from twisting. See the B019-000 instructional manual for detailed mounting instructions.

7. Connection (Single KVM Switch)

Connecting Computers to the KVM Switch

Connect each computer to the KVM switch using a Tripp Lite B078-101-PS2* or B078-101-USB* Server Interface Unit (SIU), and a Cat5e Patch Cable.

**Available Separately from Tripp Lite.*

Connecting Server Interface Units (SIUs) to the KVM Switch

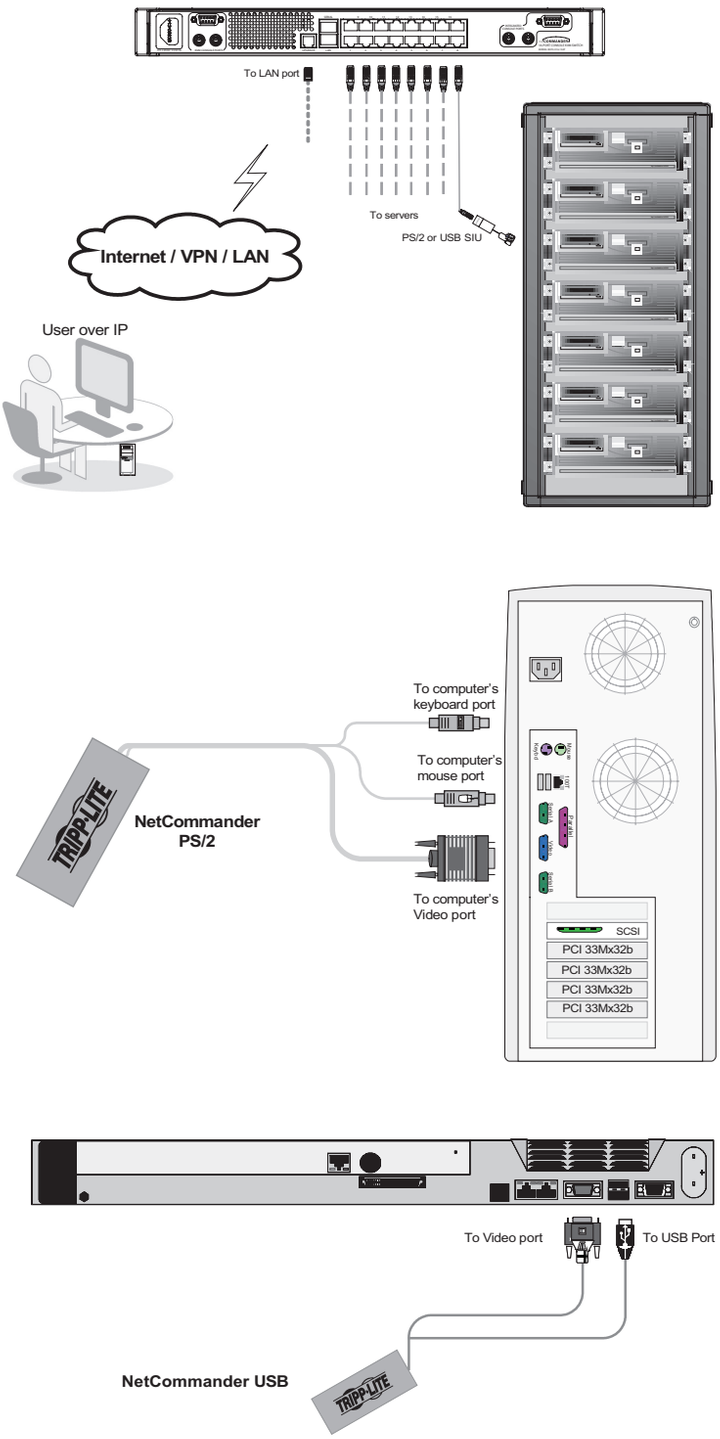
Server Interface Units (SIU) draw their power from the connected computer. In the case of the PS/2 Server Interface Unit (model # B078-101-PS2), the power is drawn from the keyboard port. In the case of the USB Server Interface Unit (model # B078-101-USB), the power is drawn from the USB port. When connected and receiveing power, the green LED on the SIU will illuminate. When the SIU is connected to the active port on the KVM, the orange LED will illuminate.

Connecting a PS/2 Server Interface Unit (SIU) (Model # B078-101-PS/2)

1. Shut down the computer being connected to the SIU.
2. Connect the SIU's VGA connector to the computer's VGA port.
3. Connect the SIU's PS/2 keyboard connector to the computer's PS/2 keyboard port.
4. Connect the SIU's PS/2 mouse connector to the computer's PS/2 mouse port.
5. Connect one end of a Cat5e patch cable to the SIU's RJ45 port and the other end to the KVM switch's RJ45 port. (Note: the Cat5e cable should be no longer than 100 ft.)
6. Repeat steps 1 through 5 for each additional PS/2 computer/server you are connecting to the KVM switch.

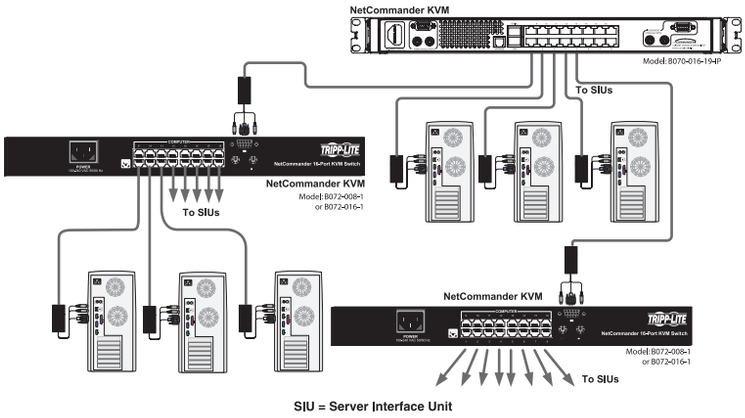
Connecting a USB Server Interface Unit (SIU) (Model # B078-101-USB)

1. Connect the SIU's VGA connector to the computer's VGA port.
2. Connect the SIU's USB connector to the computer's USB port.
3. Connect one end of a Cat5e patch cable to the SIU's RJ45 port and the other end to the KVM switch's RJ45 port. (Note: the Cat5e cable should be no longer than 100 ft.)
4. Repeat steps 1 through 3 for each additional USB computer/server you are connecting to the KVM switch.



8. Connection (Cascading Multiple KVM Switches)

The number of connected computers/servers can be increased to up to 256 by cascading an additional level of KVM switches from the B070-016-19-IP. You can cascade any combination of B072-008-1 and B072-016-1 KVM switches. In a cascade installation, the B070-016-19-IP is the first level KVM, and all KVMs cascaded from it are second level KVMs. To cascade additional KVM switches, follow the instructions below.



Note:

- *If a user has been granted access to a port with a second level KVM connected to it, then they will have access to all of the ports on that KVM. The only security settings available for the second level KVM ports are those found in that KVMs OSD.*
- *Second level KVM port access will be limited to that KVM's OSD menu and keyboard hotkey commands.*
- *The B070-016-19-IP will not store the video and mouse settings for second level KVM ports. The user will need to adjust these settings each time they access a computer/server connected to a second level KVM.*

1. Before connecting a second level KVM, you must first change its hotkey to something different than that of the first level KVM. To do this, you must connect a keyboard and monitor to the console ports on the second level KVM, so that you can access its OSD. When connected, open the second level KVM OSD using the default [Shift] [Shift] hotkey and navigate to the *GENERAL SETTINGS* page of the *F2 SETTINGS* menu. Change the hotkey according to the *Hotkey* section.
2. Connect a Cat5e/6 cable from an available B070-016-19-IP port to a B078-101-PS2 SIU. **Note**: The distance between the first and second level KVMs, and between the second level KVMs and connected computers, must not add up to more than 100 ft..
3. Connect the VGA and PS/2 connectors on the B078-101-PS2 to the console ports of a B072-008-1 or B072-016-1 KVM switch.
4. Open the B070-016-19-IP local OSD and navigate to the *PORTS SETTINGS* page of the *F2 SETTINGS* menu. Highlight the port that you just connected the second level KVM to and set its hotkey according to the *Ports Settings* section.
5. Repeat steps 1 through 4 for each additional second level KVM switch you wish to connect.
6. Connect a computer/server to an available port on a second level KVM switch using Cat5e/6 cable and a B078-101-PS2 or B078-101-USB Server Interface Unit (SIU). **Note**: The distance between the first and second level KVMs, and between the second level KVMs and connected computers, must not add up to more than 100 ft.
7. Repeat step 5 for each computer you are connecting.

9. Initial Settings (Default IP Address)

By default, the B070-016-19-IP is set to have the network's DHCP server pull an IP Address for it. Referencing the unit's Mac address, which can be found on the console's bottom panel, have your network administrator provide you with the IP address assigned by the DHCP server. If the B070-016-19-IP is not connected to a network with a DHCP server, it will boot up with the default IP address 192.168.0.155. To set up your own static IP address, you must login to the B070-016-19-IP Web Configuration Interface, disable DHCP and enter in the desired address information. (See the *Device* section for details.) ***Note****: If you're KVM is connected to a network with a DHCP server, but is not getting an IP address assigned to it, you may need to power off the KVM and then power it back on.*

10. Web Configuration Interface

The Web Configuration Interface is a Java-based utility that allows administrators to configure KVM network and security settings, create and manage user accounts, and upgrade the IP portion of the KVM firmware. The sections that follow tell you how to log into the Web Configuration Interface, and use the different settings available to the KVM administrators.

***Note**: The Web Configuration Interface controls settings/accounts for the IP portion of the KVM only. Settings/account access for the local console are set via the Local Console OSD.*

11. Logging into the Web Configuration Interface

Logging In

1. Open your web browser and enter the IP address assigned to the KVM.

***Note**:*

- *Only SSL connections are allowed, so you must start the IP address with HTTPS, and not HTTP.)*
- *When logging in using a Windows XP computer, add **/ui.jnlp** to the end of the IP address.*

2. If a screen appears that states there is a problem with the web site's security certificate, click on the option to proceed anyway; the certificate can be trusted. The Log On page appears, and the Java-based application begins to install.
3. Prompts will appear asking if you wish to proceed with the Java installation. Click the option to continue. ***Note**: In the prompts that appear, select the option to always trust content from this source to prevent these prompts from appearing every time you log on.*
4. When the installation is complete, the username and password screen appears.

5. Enter in your username and password as given to you by your system administrator, and select from the drop-down menu beneath the username and password fields whether you want to access the *Web Configuration Interface* or to *Remotely Access* the connected computers. Click the *Enter* key to proceed.

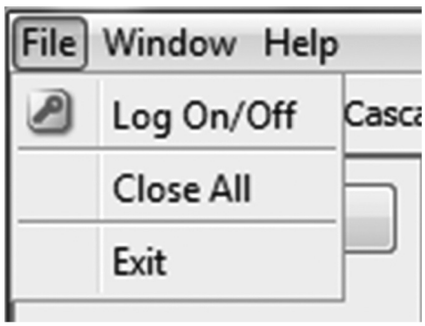
Web Configuration Interface Main Page

When logging into the Web Configuration Interface, it opens with the *Configuration* interface in the main portion of the screen, with the *Device* page displayed.

At the very top of the Web Configuration Interface are menu bars and icons that allow you to perform various functions. These functions, as well as all of the settings in the Web Configuration Interface, are described in the sections that follow.

File Menu

The *File Menu* in the upper-left of the screen includes three items; *Log On/Off*, *Close All* and *Exit*.



Log On/Off – When selected, it will close the Web Configuration interface and display the username and password screen. This function can also be performed by clicking on the *Log On/Off* button directly underneath the *File Menu*.

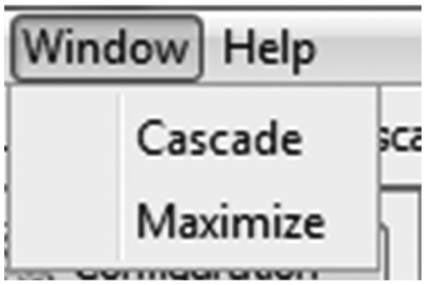
Close All – When selected, it will close the *Configuration* interface in the main part of the screen, but the rest of the Web Configuration Interface will remain open. Click the *Configuration* button to open the *Configuration* interface back up.

Exit – When selected, the Web Configuration Interface is closed altogether.

11. Logging into the Web Configuration Interface *(Continued)*

Window Menu

The *Window Menu* includes two items; *Cascade* and *Maximize*.



Cascade – When selected, the *Configuration* interface is minimized. This function can also be performed by clicking the *Cascade* button directly underneath the *Window Menu*.

Maximize – When selected, the *Configuration* interface is maximized. This function can also be performed by clicking the *Maximize* button directly underneath the *Window Menu*.

Help Menu

The *Help Menu* includes only one item; *About*.

About – When selected, the *About* screen appears, which provides you with information pertaining to the KVM's IP firmware.

12. Device

The *Device* screen is where the administrator can set the KVM network settings. The fields located in this screen are described below.

Device Name: By default, the KVM device name starts with the letter D, and is followed by a 6-digit number that can be found on the sticker on the underside of the KVM. You can change the device name using this field. If the DHCP server is published in the DNS server, you may connect to the KVM using the device name by entering it in as a URL. (e.g. https://devicename) In addition, where you have access to the server, your KVMs device name will appear on the DHCP server's interface, making it easy to locate.

TCP Port: Enter in a TCP port number here between 800 and 65535. By default, the TCP port is 900. ***Note****: The firewall or router security access list for connected computers must enable inbound communication through the selected TCP port for the B070-016-19-IP. Computers accessing the KVM over IP from a secured LAN need to open the selected port for outbound communication.*

Enable DHCP: When checked, the KVM has its IP address automatically assigned by the DHCP server. If the B070-016-19-IP is not connected to a network with a DHCP server, it will boot up with the default IP address 192.168.0.155. Uncheck this box to set a static IP address for the KVM. This checkbox is checked by default.

MAC Address: The MAC address of the KVM is displayed here. The MAC address can also be found on the sticker on the underside of the KVM.

IP Address, Subnet Mask and Default Gateway: Enter in the desired static IP address, Subnet Mask and Default Gateway for the KVM in these fields.

After making any changes to the settings on this page, click the *Save* button to save the changes and restart the KVM switch so that the changes can be implemented.

13. Users

The *Users* page allows administrators to add, edit, delete and block users in the KVM installation. There are two types of accounts that can be created: Administrator and User. Up to 200 total accounts can be created, with any combination of user types. The following section describes the differences between these account types, and details how to add, edit, delete and block accounts.

Administrator – Administrators are the only type of user that can access the Web Configuration Interface, of which they have unrestricted access. Administrators also have unrestricted access to all ports on the installation, allowing them to connect to, view and operate connected computers.

User – Users do not have access to the Web Configuration Interface. Users can both remotely view and operate connected computers, but their access is limited to the ports assigned to them by an administrator in the Web Configuration Interface. Users have access to all of the settings in the remote toolbar except for the *Advanced* section of the *Manual Mouse Settings*. (See *Remote Toolbar* section for details.)

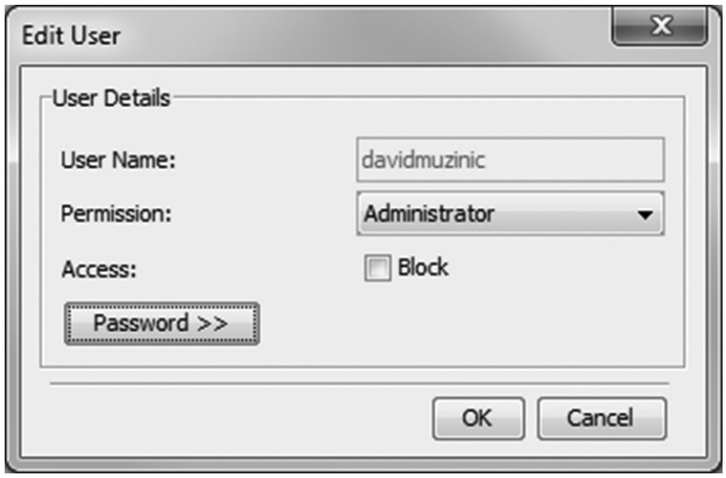
Adding an account:

1. Click the *Add* button to activate Add User screen.

2. Enter in a username and password for the new account, entering the password a second time for confirmation. Under *Standard Security Policy*, the password must be 6 characters or more, and must not include the username. Stricter password specifications can be implemented if an administrator activates the *High Security Policy* in the *Security Settings* section of the Web Configuration Interface. (See *Security* section for details on *High Security* Policy.) Usernames and passwords can contain unlimited characters, but must not include the following special characters: **& < > " { }**
3. Select the desired account type from the *Permission* drop-down menu.
4. Click the *Cancel* button at any time to stop the new account from being added. Click the *OK* button to add the new account to the account list.
5. Click the *Save* button at the top of the screen to save your changes.

Editing an account:

1. Highlight the desired account in the account list and click the *Edit* button to activate Edit User screen.



2. Edit the desired account information.
3. Click the *Cancel* button at any time to stop the changes from being saved. Click the *OK* button to apply the changes.
4. Click the *Save* button at the top of the screen to save your changes.

Deleting an account:

1. Highlight the desired account in the account list and click the *Delete* button.
2. A prompt will appear asking if you want to delete the selected user. Click *Yes* to delete the account, or *No* to keep it.
3. Click the *Save* button at the top of the screen to save your changes.

Blocking an account:

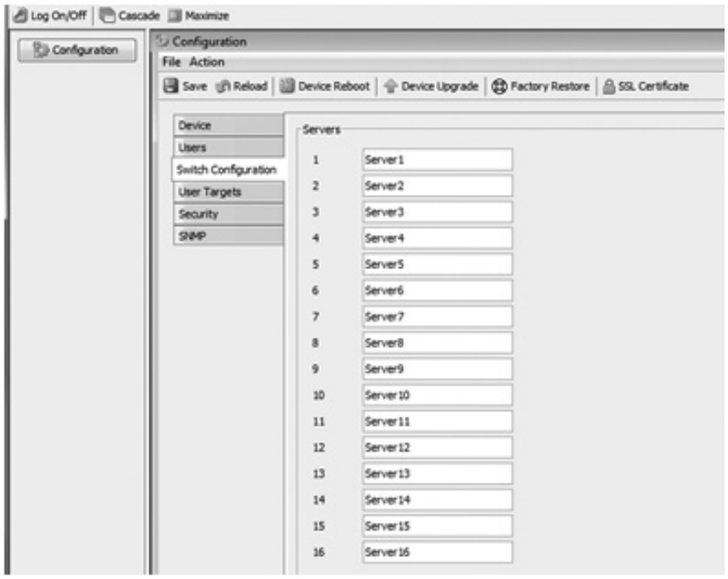
Instead of deleting an account, which removes it from the KVM entirely, an administrator can block an account. Blocking an account allows the account information to remain in the KVM, but blocks that account from accessing the KVM. The account can then be restored at any time in the future by an administrator. To block/unblock an account, follow the steps below.

1. Highlight the desired account and click the *Edit* button.
2. In the *Edit User* screen, check the *Block* checkbox, and then click the *OK* button.
3. Click the *Save* button at the top of the screen to save your changes.

14. Switch Configuration

Server Name

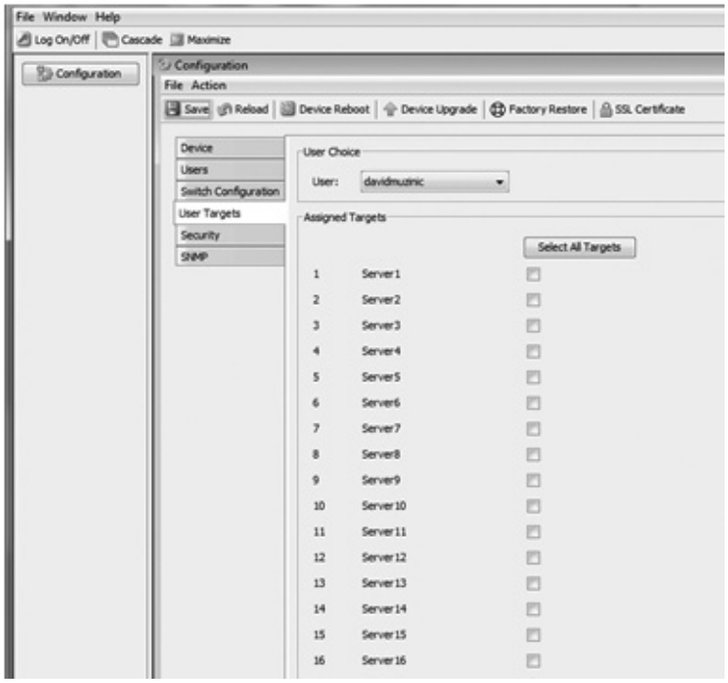
The *Switch Configuration* page allows users to give each port a unique name, making it easier to differentiate between them. By default, ports are named as *Server 1, Server 2, Server 3,* etc. To edit port names, simply highlight the name of the desired port on the *Switch Configuration* page and type in whatever name you want. To save the new port name, click the *Save* button.



15. User Targets

The *User Targets* page allows administrators to choose which ports an account has access to. Although this feature allows administrators to deny other administrators access to ports on the KVM, it allows administrators to set their own port access rights, which gives them the ability to undo any changes to their port access settings made by another administrator. To assign port access rights to an account, follow the steps below. **Note**: If an account is given access to a port that has a second level KVM cascaded from it, they will have access to each port on that KVM. Security settings for ports on a second level KVM must be set within its own OSD.

1. Select the desired account from the drop-down list at the top of the page. The ports that the selected account currently has access to will be checked.
2. Check the ports you want the account to have access to, or uncheck ports that you don't want the account to access. You can click the *Select All Targets* button to check all of the ports at once.
3. Click the *Save* button to save the port access rights for the selected account.



16. Security

The Security Settings Screen allows the Administrator to modify settings such as Account Blocking, Password Policy and Idle Timeout.

Account Blocking: This allows the administrator to adjust the settings that cause a user to be blocked from access after entering an incorrect username and/or password. The administrator can select how many attempts the user gets to enter the correct information, the time frame within which those attempts must be made and how long the user is forbidden access after failing to enter the correct information in the given time period.

Password Policy: You have the option of a standard or high security level password. The table below shows the parameters of the 2 options.

Standard Security Policy	High Security Policy
6 characters or more. Cannot include the user name.	8 characters or more must include at least 1 digit and 1 upper case letter and 1 “special” character as follows ! @ # $ % ^ * ( ) _ - + = [ ] ’ : ; ? / . Cannot include the username.

Note: The following “special” characters: & < > ” { } cannot be used in either the user name or password. Check the box to enable the high security password policy. Unchecked, the standard security policy applies.

Idle Timeout: Select the Timeout inactivity period after which the user is disconnected from the system. Choose **No Timeout** to disable Timeout. During a Timeout, a user will not be able to make changes in the Web Configuration Interface, nor will they be able to move throughout the Interface’s pages without re-entering their username and password.

Click **Save & Restart** to save any configuration changes done to the **Security Settings** page. The NetCommander IP system restarts with the new changes.

17. SNMP

From this page you can activate or deactivate SNMP logging.

Enable traps: Check to enable SNMP traps of KVM Access events and operation.

Community: Type the SNMP community

SNMP Manager IP: Enter the SNMP Server IP address

The following table lists the events that are recorded and sent via SNMP traps.

Event Text	Code	Description
“System Boot”	1010	Reported upon device boot up.
“Server Busy ask for disconnect...”	1030	Reported when a user with take over privileges attempts to login during an active session. The message is sent before the user chooses whether to take over control of the KVM.
“User login succeeded”	1040	Reported upon every successful user login to the device.
“Login failed wrong user name or password”	1050	Reported upon a login failure due to a wrong username or password.
“Login not succeeded server busy”	1060	Reported when a login is denied because the active session is held by an account with higher privileges. (Takeover not allowed)
“Logout”	1070	Reported when a user logs out of their remote session.
“Disconnected by another user”	1110	Reported when a takeover has been successfully performed and the previous user’s session is disconnected.
“Hardware failure”	1200	Reported due to internal device hardware failure. Try disconnecting attached devices and reboot.
“Hard reset power cycle command”	1220	Reported when a power cycle command is issued. This is only relevant when a special power cycle product is attached to the device. (e.g. KBPower)
“Viewer login”	1230	Reported when a user accesses the KVM in view only mode while an active session is in place.
“Viewer logout”	1240	Reported when a user accessing the KVM in view only mode logs out of their remote session.
“Global access disabled”	1250	Reported when the device has been blocked for access by an administrator. Remote access to the KVM is disabled until the administrator unblocks it.
“Block User Account”	1260	Reported when a user is blocked from accessing the KVM due to too many failed login attempts.
“Successful User Login”	2010	Reported when a user successfully logs into the Web Configuration Interface.
“Login is not successful – wrong user access level”	2020	Reported when a user is denied access to the Web Configuration Interface because they are not an administrator and not authorized to access it.
“Wrong user name or password”	2030	Reported when a user is denied access to the Web Configuration Interface due to an incorrect username or password.
“Login is not successful because server is busy”	2040	Reported when a user is denied access to the Web Configuration Interface because an active session is in place.
“DHCP server setting has been changed”	2060	Reported when the DHCP server network setting is changed.
“Network IP address changed”	2070	Reported when the IP address network setting is changed.
“Network Subnet Mask changed”	2080	Reported when the Subnet Mask network setting is changed.
“Network Default Gateway changed”	2090	Reported when the Default Gateway network setting is changed.
“User Logged out from Config”	2100	Reported when a user logs out of the Web Configuration Interface.
“TCP Port was changed”	2110	Reported when the TCP port network setting is changed.
“Remote Access type was changed”	2120	Reported when an account’s permission is changed.
“Security settings changed”	2140	Reported when a security setting is changed.
“Restore default factory settings successful”	2150	Reported when the factory default settings are successfully restored.
“Restore default factory settings failed”	2160	Reported when restoring the factory default settings fails.
“Firmware Upgrade successful”	2170	Reported when a firmware upgrade succeeds.
“Firmware Upgrade failed”	2180	Reported when a firmware upgrade fails.

18. Save

To apply any configuration changes you make, you must click the *Save* button at the top of the screen. Certain changes, such as *Device* page and *Security* page changes, require the KVM to be rebooted. When clicking the *Save* button after these types of changes, a prompt will appear to inform you that a reboot is needed. Click *Yes* to continue with the changes and reboot, or *No* to cancel.

19. Reload

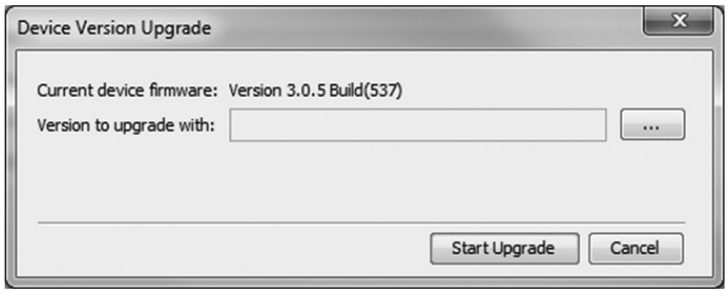
Click the Reload button at the top of the screen to restore the selected pages default values.

20. Device Reboot

Click the Device Reboot to reboot the KVM switch.

21. Device Upgrade

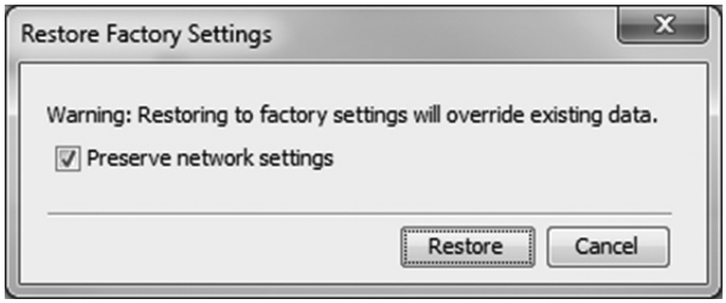
The B070-016-19-IP has two sets of firmware; one to control IP access and another to control the KVM's Mainboard and OSD. This section of the Web Configuration Interface allows you to update the KVM switches IP firmware. The non-IP firmware is updated using the KVM OSD. (See *Local Firmware Upgrade* section for details on updating the non-IP firmware)



1. Go to www.tripplite.com/support and find the available firmware upgrades for the B070-016-19-IP, and save them on a computer not connected to the KVM switch.
2. Log in to the Web Configuration Interface and click on the *Device* button. The current IP firmware version is displayed in the center of this page.
3. Click the *Browse* button and navigate to and select the file you just downloaded.
4. Once the new firmware upgrade file is selected, click the *Start Upgrade* button. Upon completion, click the *Device Reboot* button to finish the upgrade. Depending on the upgrade, the following settings may be erased: *User settings, server names* and *mouse/video adjustments*. *Network Settings* will remain intact.

22. Factory Restore

The *Factory Restore* function will reset all of the settings and accounts added by administrators to the Web Configuration Interface. There is a check box that allows you to leave the network settings unchanged, while resetting everything else. If this box is not checked, performing a restore will clear the network settings information.



Warning: Once reset, the data cannot be retrieved.

To restore factory settings

1. Click the *Factory Restore* button.
2. Check the box if you want to preserve Network settings.
3. Click **Restore**. Device settings are now restored to their defaults.

23. SSL Certificate

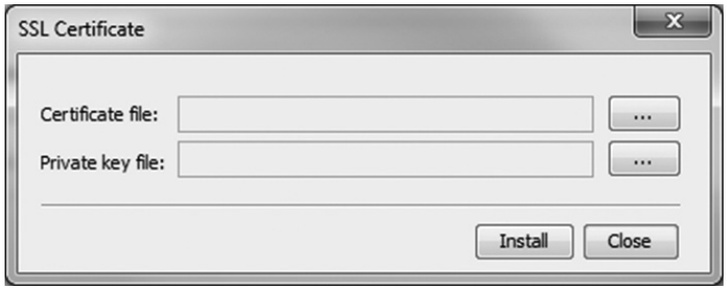
Click on the SSL Certificate button at the top of the screen to pull up the screen that allows you to install your own certificate. The fields on this page are described below.

Certificate File: Browse to locate the Certificate file.

Private File: Browse to locate the Private Key file in PEM format.

Remove any passwords from the Private Key file.

Click **Save** to apply your changes.



24. Logging In

Note: *Windows operating systems can use any 32-bit browser to remotely access connected computers; 64-bit browsers are not supported. 32-bit Linux-based computers can only use Firefox 32-bit when remotely accessing connected computers; Firefox 64-bit is not supported.*

1. Open your web browser and enter the IP address assigned to the KVM.

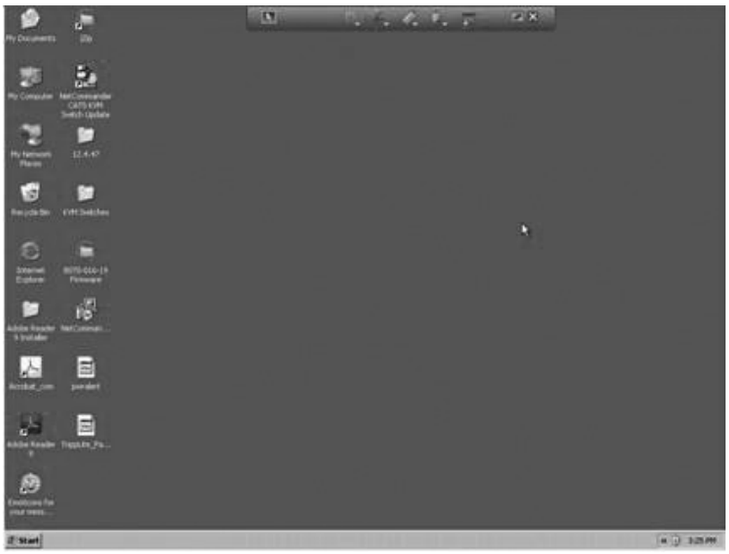
Note*:*

- *Only SSL connections are allowed, so you must start the IP address with HTTPS, and not HTTP.)*
- *When logging in using a Windows XP computer, add* ***/ui.jnlp*** *to the end of the IP address.*

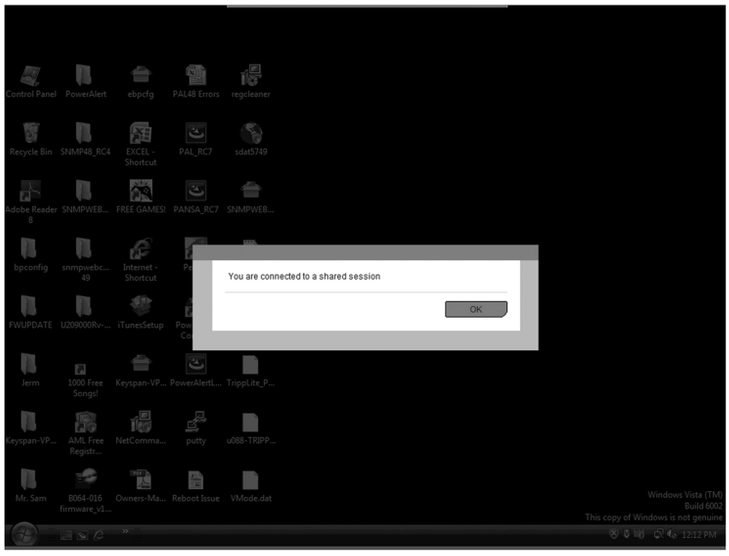
2. If a screen appears that states there is a problem with the web site's security certificate, click on the option to proceed anyway; the certificate can be trusted. The Log On page appears, and the Java-based application begins to install.
3. Prompts will appear asking if you wish to proceed with the Java installation. Click the option to continue. ***Note****: In the prompts that appear, select the option to always trust content from this source to prevent these prompts from appearing every time you log on.*
4. When the installation is complete, the username and password screen appears.

5. Enter in your username and password as given to you by your system administrator (if this is the first time the KVM is being accessed, use the default username *admin* and password *access*), and select the *Remote Access* option from the drop-down menu beneath the username and password fields. Click the *Enter* key to proceed. When first connecting to the KVM, an *Auto Video Adjust* will be performed. When this is complete, moving your mouse should cause the local and remote mouse pointers to align. If you're local and remote mouse pointers do not sync up, or if you are experiencing slow response time, you may need to adjust the performance, video and/or mouse settings via the remote toolbar. These settings are explained later in this manual.

Remote Session Screen



When you initiate a remote session for the first time, the screen of the first computer in the installation that you have access to is displayed. Subsequent remote sessions will open with the screen of the last computer that you accessed in your previous session displayed. The NetCommander KVM allows up to 5 users to login at the same time and share a remote session. When you login to a shared session, the remote screen appears with a prompt that informs you that you're connected to a shared session.



When in a shared session, the control of the mouse and keyboard is transferred from user to user. As soon as one user stops using the keyboard and mouse, another user can immediately jump in and control the remote session. The following sections describe the various aspects of a remote session.

25. Remote Toolbar

The NetCommander KVM provides a toolbar that allows the remote session to be manipulated. The features on the toolbar allow you to toggle between accessible ports, adjust the video settings of the remote session, align the local and remote mouse pointers, etc. When a remote session is initiated, the toolbar is collapsed, and a thin bar appears at the top-center of the screen. To expand the toolbar, simply move the mouse pointer over the blue bar at the top-center of the screen. The following sections describe the different settings found on the toolbar and how to use them.

Pin Toolbar – Click on this icon to switch between displaying the toolbar all the time and allowing it to disappear after a few seconds. The toolbar is set to disappear after a few seconds by default.

Session Profile – Clicking on this icon will display a drop-down list with three choices; *Session Profile*, *Log Off* and *About*….

Session Profile

Selecting the session profile option pulls up a screen that allows you to configure how a remote session is displayed when you login, and to make your session exclusive, preventing other users from logging in at the same time. The contents of this screen are described below.

- **Local Mouse Pointer** – Choose how the local mouse pointer is displayed in a remote session. Checking *None* will display the remote computer's mouse pointer only. Checking *Dot* will display the local mouse pointer as a dot, and the remote mouse pointer as an arrow. Checking *Default* will display both local and remote mouse pointers as arrows.
- **On Connect** – Check the *Auto Hide* option to cause the toolbar to hide itself after a few seconds starting from the next time a remote session is initiated. When unchecked, the toolbar will be continuously displayed. Check the *Full Screen* option to display the remote session in full screen mode starting from the next time a remote session is initiated. When unchecked, the remote session will be displayed inside your web browser.
- **Exclusive Session** – When you are the only one logged into a remote session, checking this checkbox will prevent others from logging in at the same time. When unchecked, up to 5 users can share a remote session.
- **Log Off** – Selecting this option will log you out of the KVM Switch.

About

Select this option to pull up a screen that displays firmware versions of the KVM switch.

Video – Clicking on this icon allows you to adjust the video settings of the remote session. The settings in this section are described below.

Refresh

In the event that the video of the remote computer does not fully refresh on its own, select this option to manually refresh it.

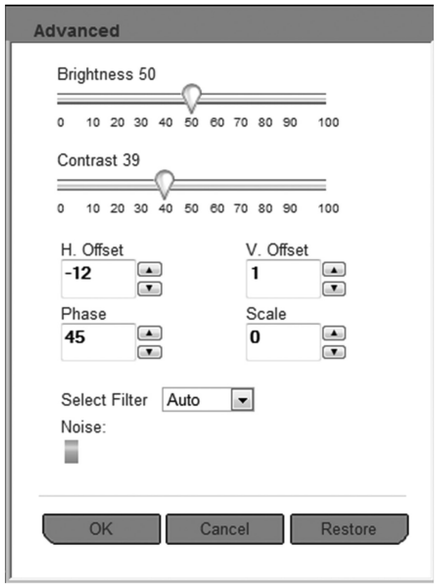
Video Adjust

Upon switching ports, a *Auto Video Adjust* is performed to bring the remote computer's video in line with that of the local computer. In the event that the initial *Auto Video Adjust* is not successful, or does not initiate on its own, select this option to manually perform an *Auto Video Adjust*.

25. Remote Toolbar *(Continued)*

Advanced

If an *Auto Video Adjust* does not result in acceptable video settings, selecting this option will bring up a screen that allows you to manually adjust these settings.

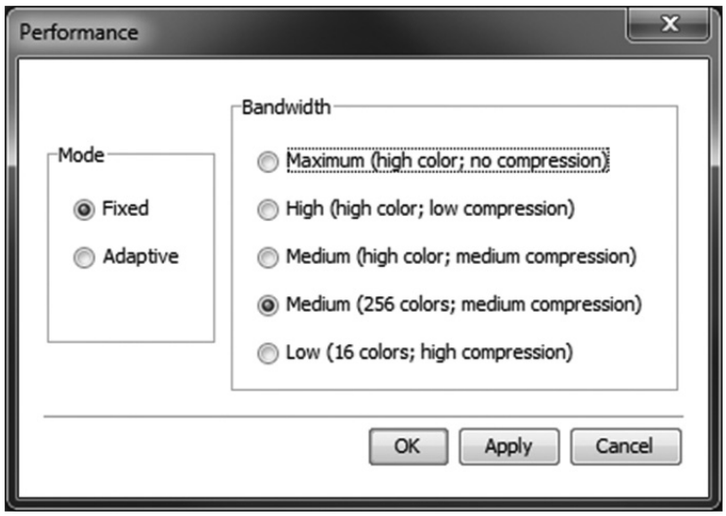


The table below describes the settings in the *Advanced* screen.

Setting	Description
Brightness	Position the slider bar to adjust the video *Brightness* from a setting between 0 and 100.
Contrast	Position the slider bar to adjust the video *Contrast* from a setting between 0 and 100.
H. Offset	Use the up and down arrows to adjust the horizontal positioning of the remote video.
V. Offset	Use the up and down arrows to adjust the vertical positioning of the remote video.
Phase	Use the up and down arrows to define the point at which each pixel is sampled.
Scale	Use the up and down arrows to define the scale resolution of the remote image.
Select Filter	Choose the level of filter that you wish to place on the remote video. A higher filter will produce a poorer image, but can help improve keyboard and mouse response time. By default, this setting is set to *Auto*, which determines the filter level based on the current noise level.
Noise	This bar represents the amount of video noise present when a static screen is displayed. The more noise, the slower your keyboard and mouse response time will be. ***Note**: If the video noise level is above zero, the* Calibration *function (See* Calibrate *on page 20 for details) in the* Mouse *drop-down may not work.*

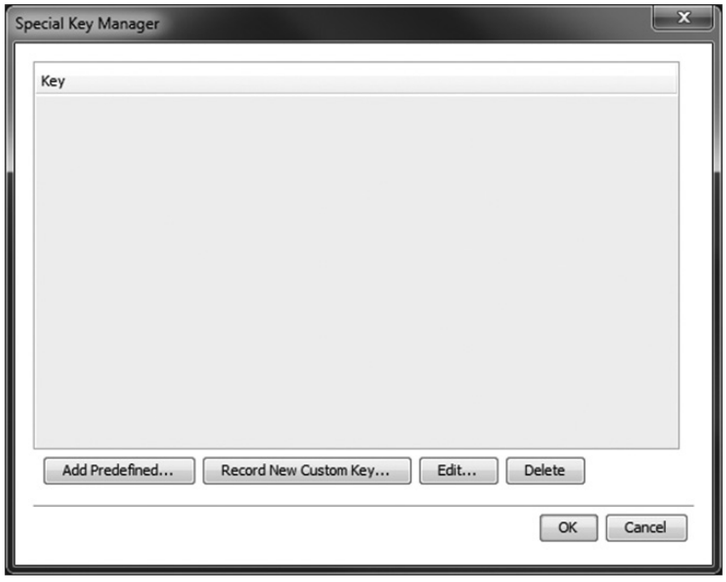
Performance

Selecting the *Performance* option pulls up a screen that allows you to determine the amount of color that is displayed in the remote video.



When the *Fixed* performance mode is checked, you can select from the bandwidth options on the right of the screen. A higher setting results in more colors being displayed and a better quality picture, but can hinder keyboard and mouse response time. In slower networks, where keyboard and mouse response time is choppy, selecting a low bandwidth can help improve performance. When the *Adaptive* performance mode is checked, the bandwidth is automatically set by the KVM according to the network conditions.

 **Keys** – Click on this icon to display a list of keyboard key sequences that can be sent directly to the remote computer, without affecting the local computer. For example, when pressing the [Control] [Alt] [Delete] command on the keyboard, the command gets sent to the local computer instead of the remote computer. By selecting this command from the *Keys* drop-down, you can perform the command on the remote computer. To add/remove a command from the list, select the *Special Keys* option in the *Keys* drop-down. The following screen appears.



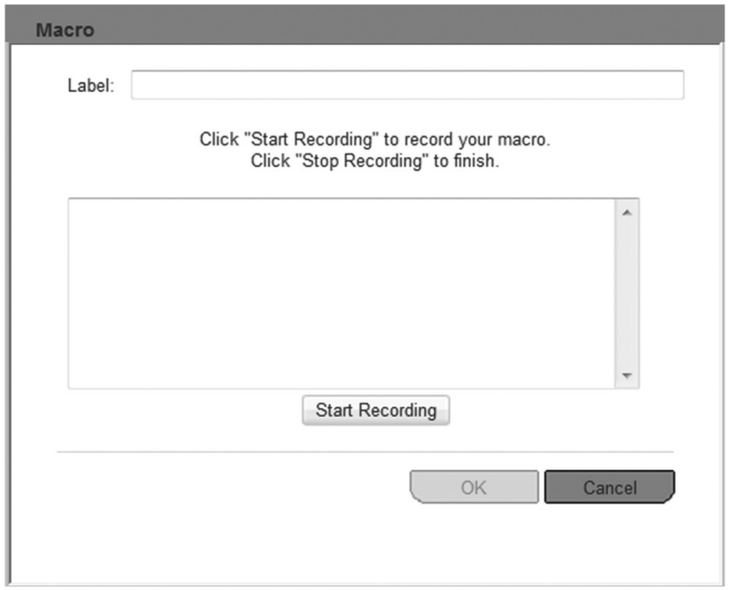
25. Remote Toolbar *(Continued)*

Adding a Predetermined Command

1. Click the *Add Predefined* button to pull up a pre-defined list of keyboard key sequences to choose from.
2. Select a command from the list and click on the *OK* button to add it to the *Keyboard* drop-down list.

Creating a New Command

1. Click on the *Record New Custom Key* button to display the screen below.



2. Enter a name for the new command in the *Label* field.
3. Click on the *Start Recording* button.
4. Press the desired command keys. As keys are pressed, they are displayed in the command area in the center of the screen.
5. When you are done entering in the key sequence, click on the *Stop Recording* button.
6. To add the command to the *Keys* drop-down list, click on the *OK* button. Click on the Cancel button to exit without saving the command.

Editing a Command

1. Select the desired command from the list and click on the *Edit* button.
2. The record screen appears, with the current sequence in the command area in the center of the screen. Click on the *Start Recording* button.
3. Press the desired command keys. As keys are pressed, the old sequence is removed and the new keys are displayed in the command area.
4. When you are done editing the key sequence, click on the *Stop Recording* button.
5. To add the edited command to the *Keys* drop-down list, click on the *OK* button. Click on the *Cancel* button to exit without saving the command.

Deleting a Command

1. Select the desired command from the list and click the *Delete* button. A prompt appears asking you to confirm the deletion.
2. Click the *OK* button to delete the command, or click the *Cancel* button to exit without deleting the command.

 **Mouse** – Clicking this icon allows you to *Calibrate* and *Align* the local and remote mouse pointers automatically, as well as to manually adjust the mouse settings.The following sections explain these features, and also provide general tips for synchronizing the local and remote mice.

25. Remote Toolbar *(Continued)*

Calibrate

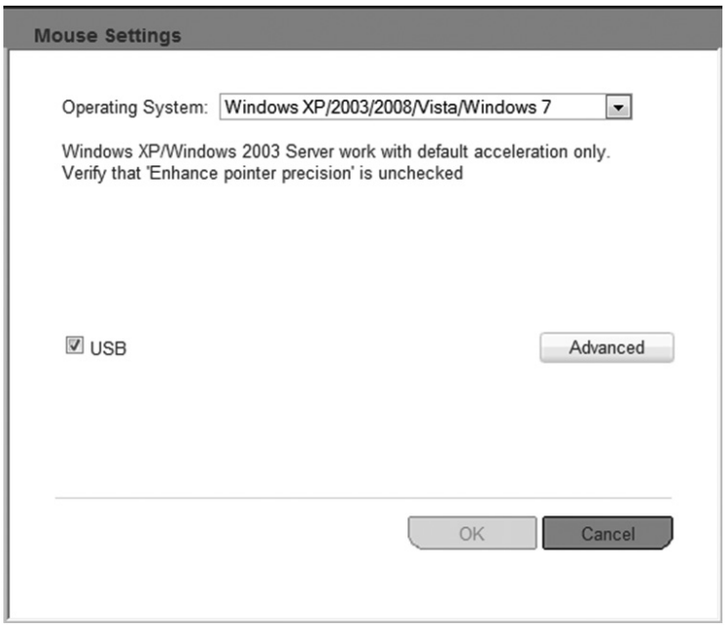
For remote computers running Windows NT4, 98 or 2000, selecting the *Calibrate* feature will automatically detect the remote mouse speed settings and make the necessary adjustments to align the local and remote mouse pointers. If the mouse settings on the remote computer were ever changed, or if the remote computer is running an operating system other than Windows NT4, 98 or 2000, you will have to adjust the mouse settings manually via the *Mouse Settings*….. screen. (See *Mouse Settings*….. below for details.) To calibrate the local and remote mouse pointers, click on the Calibrate feature in the *Mouse* drop-down menu. A prompt will appear on the screen to inform you that calibration is taking place. If the two mouse pointers don't align after the prompt disappears, try moving the mouse cursor around the screen, which can cause them to align. If that doesn't work, click on the *Align* feature in the *Mouse* drop-down menu to bring the two together. (See *Align* below for details) If they still do not align, follow the manual mouse synchronization steps in the *Mouse Settings*…. section below.

Align

When logging into the KVM or accessing a new port, the local and remote mouse pointers may not be aligned. This does not always mean that they are not set up properly. Click on the *Align* feature in the *Mouse* drop-down menu to bring them together. If this does not bring the local and remote mouse pointers into alignment, follow the steps in the *Calibration* (See above) and/or *Mouse Settings*…. (See below) sections.

Mouse Settings……

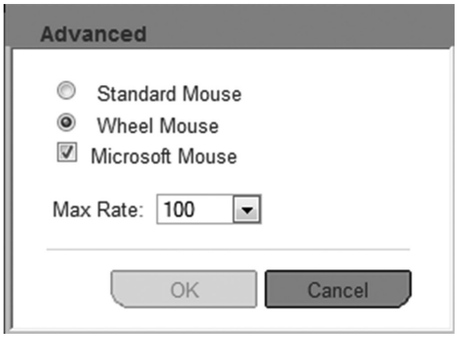
If you are unable to get the local and remote mouse pointers to align using the *Calibrate* and/or *Align* features, you will need to manually adjust the mouse settings. Click on the *Mouse Settings*… feature in the *Mouse* drop-down to bring up the following screen.



- **Operating System** – Select the operating system of the selected remote computer from this drop-down menu. The screen will update to display settings appropriate to the selected operating system. If the mouse settings of the remote computer have never been changed, leave the *Default* checkbox that appears checked. If the mouse settings of the remote computer have ever been changed (even if they were changed and then returned to the original settings), uncheck the *Default* checkbox and edit the settings to match that of the remote computer.

- **USB** – This checkbox should be checked if the remote computer is connected using a B078-101-USB SIU, or a B078-101-PS2 SIU with a PS/2 to USB adapter.

- **Advanced** – Clicking the *Advanced* button brings up the screen below, which allows you to select what type of mouse is connected to the local console port on the NetCommander IP. For example, select *Standard Mouse* when using a 2-button mouse or 2-button touchpad. Select *Wheel Mouse* for any mouse/touchpad with 3 or more buttons. Check *Microsoft Mouse* if the mouse being used is made by Microsoft.



- **Max Rate** – This defines the maximum mouse report rate. A setting of *Default* is compatible with the majority of operating systems. For older versions of Sun, use a *Max Rate* setting of 20.

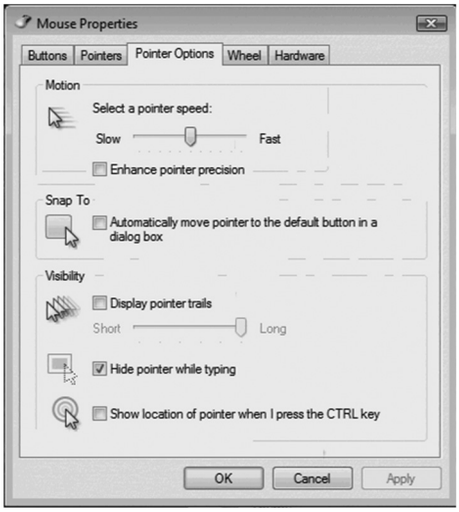
Once all of the mouse settings have been set, click the *OK* button to return to the remote screen. Upon moving the mouse, the local and remote mouse pointers should align. If needed, use the *Align* feature in the *Mouse* drop-down menu to bring them together.

25. Remote Toolbar *(Continued)*

Mouse Troubleshooting Tips

If the local and remote mouse pointers do not align after performing the mouse functions described in the previous sections, try the following.

- Ensure that the remote computer's *Enhanced Pointer Precision* setting is unchecked. If checked, the local and remote mouse pointers will not align. This setting can be found in your computer's *Mouse Properties* screen. The image below shows this screen from a Windows Vista computer.

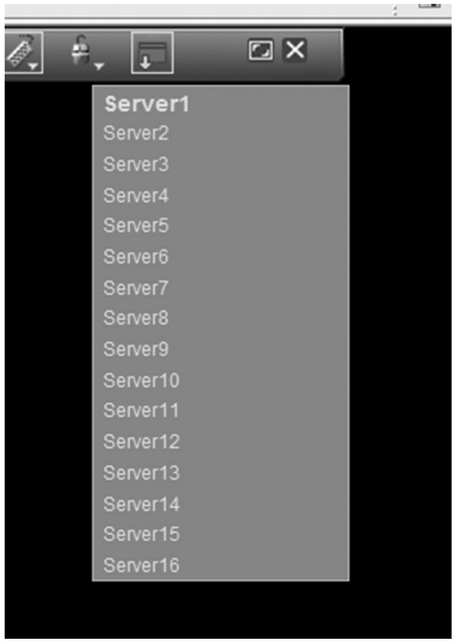


- If the video *Noise* level (See *Advanced* section under *Remote Toolbar* for details) is above zero, the *Calibrate* function may not work. If you are having trouble calibrating the local and remote mouse pointers, try performing a *Video Adjust*, and then try again. If this does not help, you may need to manually adjust the video settings in the *Advanced* screen. (See *Advanced* section under *Remote Toolbar* for details.)

- There are times when a *Video Adjust* does not properly align the remote video. If the screen is not aligned properly (you will see a black bar on a side of the remote screen, and part of the remote screen will not be displayed), the local and remote mouse pointers will not align. Try performing another *Video Adjust* to bring the screen into alignment. If this still does not work, you will need to manually adjust the *H. Offset and/or V. Offset* settings in the *Advanced* screen to bring the screen into alignment. (See *Advanced* section under *Remote Toolbar* for details.)

- Although the chart in the back of this manual shows the supported video resolutions and refresh rates, there are times where lowering the refresh rate on the remote computer will help to improve local and remote mouse alignment.

- If you are using non-shielded Cat5/6 cable, try using Tripp Lite N105-Series Cat5e shielded patch cable. Any noise that exists in the cabling can affect local and remote mouse alignment, and switching to shielded cabling eliminates that noise.



 **Server List** – Clicking this icon will display a list of the accessible ports on the installation. If you are not given access to a port, it will not display in the list. Simply select the desired port to switch to it.

 **Full Screen** – Click on this icon to toggle *Full Screen* mode off/on.

 **Log Out** – Click on this icon to log out of your remote session.

26. Local Console

When using the built-in console to locally access connected computers, there are two methods you can use; *Keyboard Hotkeys* and *On-Screen Display (OSD)*.

Keyboard Hotkeys

Keyboard Hotkeys allow you to toggle between ports using the keyboard. To access the first accessible port after the currently selected port, press and release the [Shift] key, and then press and release the plus [+] key. To access the first accessible port prior to the currently selected port, press and release the [Shift] key, and then press and release the minus [-] key.

On-Screen Display (OSD)

To access the OSD, press and release the [Shift] key twice. When activated, the OSD main page opens with the port list displayed. Ports that have a powered-on computer connected to them will be displayed using Blue text. Ports that do not have a computer connected to them, or that have a powered-off computer connected, will be displayed using Gray text. By default, ports that are displayed in Gray will not be accessible to the user. If you want to be able to access these ports, you need to turn off the *Auto Skip* setting in the *General* section of the OSD. (See *General* section under *On-Screen Display OSD F2 Settings* for details.)

To the right of the *Port Number* and *Name* columns is a *Type* column. The *Type* column displays a C next to ports that have a computer connected to them, and an S next to ports with a KVM connected to them. In order for the *Type* column to display a port as a KVM switch, you must change its *HKEY* setting in the *Port Settings* screen. (See *Ports* section under *On-Screen Display OSD F2 Settings* for details.)

Selecting a Port

To select a port in the OSD main page, use the [↓] and [↑] keys to highlight the desired port, and then press the [Enter] key.

27. On-Screen Display (OSD) Functions

When in the OSD main menu, there are various functions that can be performed using the keyboard keys. These functions are described in the following sections.

F1 – HELP

Press the [F1] key to pull up the *HELP* screen. The *HELP* screen displays the functions that are available, and what keys are used to activate them.

F2 – SETTINGS

Press the [F2] key to pull up the OSD *SETTINGS* screen. From this screen you can configure the KVM and add/edit user accounts. The *F2 – SETTINGS* section is described in detail in the *On-Screen Display (OSD) F2 Settings* section.

F4 – SCAN

Press the [F4] key to initiate an *Auto Scan*. When initiated, an *Auto Scan* automatically switches between accessible ports at a pre-determined time interval. By default, each port is scanned for 30 seconds. The scan interval can be edited in the *Time* settings screen. (See *Time* section under *On-Screen Display OSD F2 Settings* for details) During an *Auto Scan*, press the [F4] key to stop the scan at the currently selected port.

F5 – TUNING

As computers are located further away from the KVM switch, the video can become distorted. In the event you are experiencing poor video quality, the *TUNING* function can be used to correct it. Press the [F5] key to display the currently selected port, with the *TUNING* bar displayed. Use the [←] and [→] keys to make the necessary adjustments. When you are finished, press the [Esc] key to go back to the OSD. ***Note****: Tuning is performed on a port-by-port basis. You will need to adjust each port individually.*

F6 – MOVE LABEL

By default, the label that displays each ports *Port Name* appears in the top-center of the screen, but it can be moved anywhere on the screen that you want. Press the [F6] key to display the currently selected port and its label. Use the [↑], [↓], [←] and [→] keys to move the label to the desired location, and then press the [Esc] key to go back to the OSD. ***Note****: Setting the label location is performed on one port at a time. You can move the label to different locations on different ports.*

F10 – NEW MONITOR – DDC2

In the event that one of the connected computers does not display an image on the console monitor (e.g. You get the error message 'Unable to Display Video Mode'), you may need to update the DDC information being used by the console monitor. To do this, follow the steps below.

1. Remove the SIU VGA connectors from the connected computers, while leaving the PS/2 and /or USB connectors plugged in.
2. Open the OSD main menu and press the [F10] key. The OSD will flash the message "Please Wait." When that message disappears, the update is complete.
3. Reconnect the SIU VGA connectors to the connected computers. You should now be able to display video from all of the remote computers.

28. On-Screen Display (OSD) F2 SETTINGS

Press the [F2] key to pull up the OSD *SETTINGS* screen. From this screen you can configure the KVM and add/edit user accounts. The pages that follow describe the sections of the *F2 SETTINGS* page, and the settings included in them. ***Note****: When local security is turned on, the KVM administrator is the only one that can access the* F2 SETTINGS *page.*

General

Highlight the *General* option and press the [Enter] key to open the *GENERAL SETTINGS* page. This page allows you to turn the KVMs local security settings on/off, as well as to configure some of the basic KVM settings. The table below describes the settings found in this page.

Setting	Description
Security	By default, the *Security* setting is turned off. To activate the *Security* setting, highlight it and press the [Spacebar] key. Upon pressing the [Spacebar] key, you will be prompted to enter the administrator password in order to change the *Security* setting. The default administrator password is *ADMIN*. For security purposes, it is recommended that you update the administrator password to something unique. (See the *Security Settings* section for details) ***Note****: When security is activated, the keyboard hotkey commands are disabled, leaving the OSD as the only way for you to locally access the connected computers. Upon pressing the [Shift] [Shift] invocation command, you will be prompted to enter your password before the OSD can be accessed. The security settings in this OSD are exclusive to the local console, and do not affect the remote access security settings.*
Hotkey	By default, the hotkey used in keyboard hotkey commands and to open the OSD is the [Shift] key, but this can be changed to any of the four options below. To toggle between commands, highlight the *Hotkey* option and press the [Spacebar] key. **(SH-SH)** • Press and release the [Shift] key twice to open the OSD. • Press and release the [Shift] key, and then press and release the plus [+] key to switch to the next accessible port. • Press and release the [Shift] key, and then press and release the minus [-] key to switch to the previous accessible port. **(CL-CL)** • Press and release the Left [Ctrl] key twice to open the OSD; or, press and release the Right [Ctrl] key, and then press and release the Left [Ctrl] key. • Press and release either [Ctrl] key, and then press and release the plus [+] key to switch to the next accessible port. • Press and release either [Ctrl] key, and then press and release the minus [-] key to switch to the previous accessible port. **(CLF11)** • Press and release either [Ctrl] key, and then press and release the [F11] key to open the OSD. • Press and release either [Ctrl] key, and then press and release the plus [+] key to switch to the next accessible port. • Press and release either [Ctrl] key, and then press and release the minus [-] key to switch to the previous accessible port. **(PRSCR)** • Press and release the [Print Screen] key once to open the OSD. • When you choose [Print Screen] as your hotkey, the keyboard hotkey commands are disabled, leaving the OSD as the only way to access the connected computers.
Autoskip	By default, the *Autoskip* setting is enabled, which prevents users from accessing ports that either don't have a computer connected to them, or that have a powered-off computer connected to them. To toggle this setting on/off, highlight it and press the [Spacebar] key.
Serial Port	By default, the *Serial Port* setting is enabled, which allows a local firmware upgrade to be performed. To toggle this setting on/off, highlight it and press the [Spacebar] key. ***Note****: This setting affects the firmware upgrade port only, and has nothing to do with the* Serial *port on the back of the unit.*
Keyboard Language	By default, the *Keyboard Language* setting is set to *US English*, but it can be changed to *French (FR)* or *German (DE)*. To toggle between these three language settings, highlight the *Keyboard Language* setting and press the [Spacebar] key.
Switch Name	By default, the switch name is *NETCOMMANDER 16IP*, but this can be changed. Simply move the OSD cursor to the *Switch Name* and type in the desired name. Delete any characters that you don't want. The *Switch Name* can be up to 18 characters in length, with spaces counting as characters.
F7 – Defaults	You can restore the default settings of the local OSD by pressing the [F7] key. When pressed, you will be prompted to confirm that you wish to continue. If yes, press the [Y] key to restore the default values. ***Note****: All of the local OSD settings, including* Security *and* User Settings*, will be restored.*

28. On-Screen Display (OSD) F2 SETTINGS *(Continued)*

Ports

Highlight the Ports option and press the [Enter] key to open the Port Settings page. This page allows you to edit port names, set the remote computer keyboard type, and set the hotkey for ports that have second level KVM switches connected to them. The table below describes each of these settings.

Column	Description
NAME	The first column displays the name associated to each port. You can change this by moving the cursor to the desired port name and simply typing over the existing name with the desired name. Port names can be up to 15 characters in length, with spaces counting as characters.
KB	The second column displays the keyboard type associated with each port. By default, each port is set to PS, which works with Intel-based computers and UNIX servers connected using a B078-101-USB. To toggle this setting between the options listed below, move the cursor to the desired port, press the [Tab] key to move to the KB column, and then press the [Spacebar] key. • **PS** – Intel-based computers and UNIX servers connected using a B078-101-USB • **U1** – HP UX • **U2** – Alpha UNIX, SGI or Open VMS • **U3** – IBM AIX
HKEY	By default, the *HKEY* setting for each port is *NO*, which means that a computer is connected to it. When a second level KVM is connected to a port, you need to update this setting to display its hotkey. To toggle this setting between the various hotkeys, move the cursor to the desired port, press the [Tab] key to move to the *HKEY* column, and then press the [Spacebar] key.

Time

Highlight the *Time* option and press the [Enter] key to open the *Time Settings* page. This page lists all of the KVM ports on the left, and 3 time columns on the right, which are described below.

SCN – Sets the amount of time spent on the selected port during an *Auto Scan*. The default scan interval is 30 seconds. A setting of 000 causes the corresponding port to be skipped during an *Auto Scan*.

LBL – Sets the amount of time that the port's label is displayed on the screen for. The default label display time is 30 seconds. A setting of 999 causes the label to be displayed continuously. A setting of 000 causes the label not to appear at all.

T/O – When *Security* is enabled, you set the KVM to logout after a specified amount of time. When this time is reached, entering the OSD invocation command brings up a prompt asking you to enter a password, which is required to regain access to the KVM. The default timeout value is 30 seconds. A setting of 999 disables the timeout function. ***Note****: A setting of 000 causes the KVM to logout immediately, not allowing the user enough time to hit the OSD invocation command to pull up the password prompt. It is recommended that you always keep the timeout setting at 5 seconds or higher. If you set the timeout setting at 000 and get locked out of the KVM, turn the unit off and then back on. When turned back on, you will be able to use the OSD invocation command to pull up the password prompt and regain access to the OSD.*

To set the time periods mentioned above, follow the steps below.

1. Move the cursor to the desired port row and press the [Tab] key to jump to the desired column.
2. When the cursor is moved to the desired column, simply type in the time interval.

Users

The *Users* option can only be accessed when Security is enabled in the *General Settings* page. (See *General* under *On-Screen Display OSD F2 Settings* section for details.) Highlight the *Users* option and press the [Enter] key to open the *User Settings* page. In the column on the left side of the screen, all of the ports on the KVM are listed. On the right side of the screen, there are 6 columns; one for each *user* account. For example, column 1 represents the first *user* account that is displayed in the *Security Settings* page. (See the *Security Settings* section for details.) The letters in each column represent the access rights that the corresponding *user* account has for the corresponding port. There are three types of access a *user* can be given to a port, which are described below.

- **Y** – A *Y* signifies that the corresponding *user* account has full access rights to the corresponding port.
- V – A *V* signifies that the corresponding *user* account has view-only access rights to the corresponding port, meaning that they can view the remote video, but are not allowed to control the connected computer with the keyboard and mouse.
- N – A *N* signifies that the corresponding *user* account is not allowed to access the corresponding port.

To change the *User* settings, the *administrator* must follow the steps below.

1. In the *User Settings* page, use the [↓] and [↑] keys to move the cursor to the desired port row.
2. Use the [←] and [→] keys to move the cursor to the desired account column.
3. Press the [Spacebar] key to toggle between the different access types.

28. On-Screen Display (OSD) F2 SETTINGS *(Continued)*

Security

The *Security* option can only be accessed when *Security* is enabled in the *General Settings* page. (See *General* under *On-Screen Display OSD F2 Settings* section for details) Highlight the *Security* option and press the [Enter] key to open the *Security Settings* page. The *Security Settings* page displays all of the available accounts for the KVM; 1 *administrator*, 1 *supervisor* and 6 *users*. The first column lists the account *Name*, the second column lists the account *Password*, and the third column lists the account *Type*. The three available account types are described below.

- **Administrator –** There is one *administrator* account available. The *administrator* has full access to all ports and settings on the KVM. The *administrator* is the only account that can access the *F2 SETTINGS* menu in the OSD.
- **Supervisor** – There is one *supervisor* account available. The *supervisor* has full access to all ports on the installation, but is not allowed to access the *F2 SETTINGS* menu in the OSD. The *supervisor* is allowed to access the *F1 HELP, F4 SCAN, F5 TUNING, F6 MOVE LABEL* and *F10 NEW MONITOR DDC* functions in the OSD.
- **User** – There are six *user* accounts available. *Users'* port access rights are limited to those assigned to them by the *administrator*. *Users* are not allowed to access the *F2 SETTINGS* menu in the OSD, but can access the *F1 HELP, F4 SCAN, F5 TUNING, F6 MOVE LABEL* and *F10 NEW MONITOR DDC* functions.

To change the *Security* settings, the *administrator* must follow the steps below.

1. In the *Security Settings* page, use the [↓] and [↑] keys to move the cursor to the desired account row.
2. To edit the account *Name*, simply type the desired name over the current one, and delete any unnecessary characters. ***Note****: The account* Name *is for organizational purposes only. The* Password *is the only thing an account needs to enter to gain access to the KVM.*
3. To edit the account *Password*, press the [Tab] key to move the cursor to the *Password* column, and then enter in the desired password over the current one. Delete any unnecessary characters.

29. Local Firmware Upgrade

The NetCommander IP KVM switch uses two types of firmware, one for the IP portion of the KVM, and the other for the local portion. This section describes how to perform a firmware upgrade on the local portion of the KVM.

Firmware Upgrade Computer Requirements:

- Windows 2000 or higher operating system
- Pentium 166 or higher with 16MB RAM and 10MB free hard drive space
- Available DB9 serial port

Firmware Upgrade Software Requirements:

- Firmware Upgrade Utility – This Windows-based application reads the current firmware and installs the new firmware of the KVM and Server Interface Units (SIUs). ***Note****: The Firmware Upgrade Utility is compatible with Windows 32-bit operating systems only.*
- Firmware Upgrade File – This file contains the actual firmware for the KVM and SIUs.

Performing a Firmware Upgrade

There are several steps to performing a firmware upgrade on your KVM switch and SIUs; *Physical Installation, Current Firmware Verification* and *Firmware Upgrade*. Each of these steps is described in the sections that follow. ***Note****: Each KVM switch in a cascaded installation must be upgraded separately.*

Physical Installation

The first step in performing a firmware upgrade is to physically connect the KVM switch to a computer that is not a part of the KVM installation. (Not connected via Cat5e/6 cable and a SIU) To do this, follow the steps below.

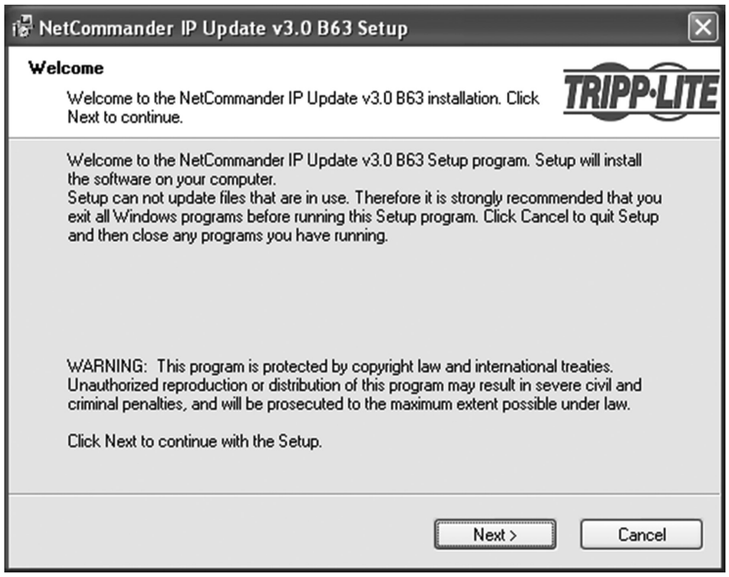
1. Make sure that the *Serial Port* setting in the *General Settings* page of the OSD is enabled. (See *General* under *On-Screen Display OSD F2 Settings* section for details.) If this setting is disabled, you will not be able to perform a firmware upgrade.
2. Connect the RJ11 *Firmware Upgrade* port on the back of the KVM to a DB9 serial port on the upgrade computer using the included RJ11 to DB9 firmware upgrade cable.

29. Local Firmware Upgrade *(Continued)*

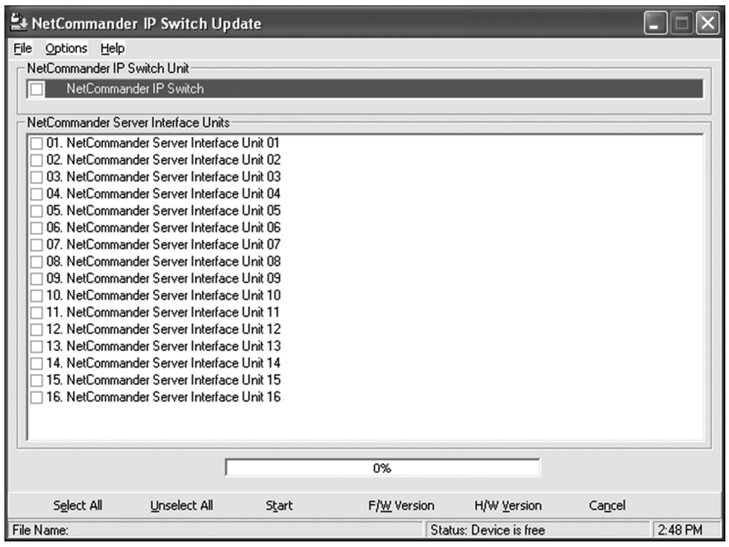
Current Firmware Verification

After the physical connection is made, you need to install the Firmware Upgrade Utility on the upgrade computer (the computer you just connected to the KVM), and then check the current firmware version on your KVM to see if it needs to be updated. To do this, follow the steps below.

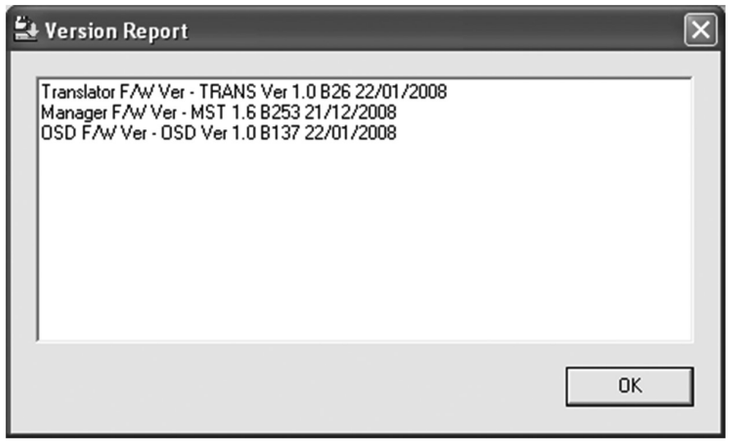
1. On the upgrade computer, go to www.tripplite.com/support and download the latest firmware for the B070-016-19-IP. Both the Firmware Upgrade Utility and KVM/SIU Firmware Upgrade File will be downloaded together.
2. Run the Firmware Upgrade Utility to install it on the upgrade computer. Follow the installation prompts to successfully install the utility.



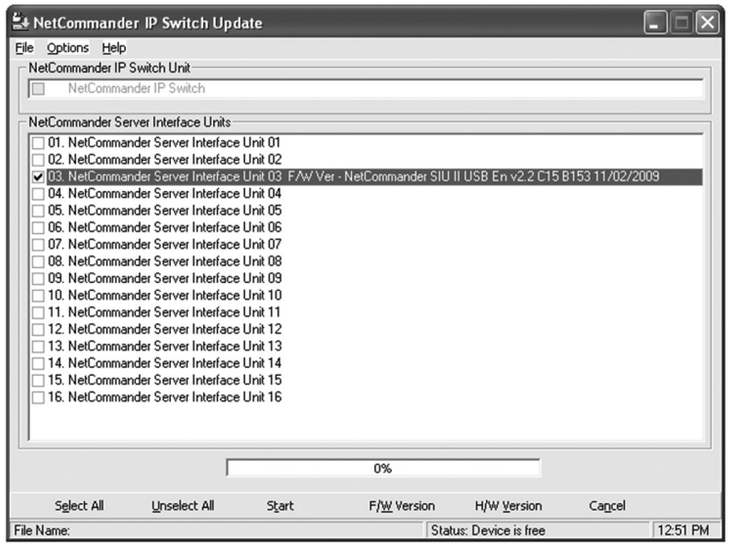
3. When installation is complete, clicking the *Finish* button will automatically open the Firmware Upgrade Utility with the main screen displayed.



4. To check the firmware version of the KVM, check the checkbox at the top of the screen next to the text *NetCommander* IP Switch.
5. Click on the F/W Version button at the bottom center of the screen to pull up a box that displays the current firmware versions. Note: There are three firmware versions associated with the B070-016-19-IP KVM; Translator F/W, Manager F/W and OSD F/W.



6. Compare the current firmware version numbers of the KVM with the firmware version numbers you downloaded to see if your KVM needs to be upgraded.
7. If checking the current firmware version of the connected SIU(s), uncheck the KVM checkbox at the top of the screen, and then check the checkboxes next to each SIU that you wish to determine the firmware of.
8. When you have selected all the desired SIUs, click on the *F/W Version* button at the bottom center of the screen to display their current firmware version numbers.



9. Compare the current firmware version numbers of the SIU(s) with the firmware version numbers you downloaded to see if you need to upgrade your SIU(s) firmware.

29. Local Firmware Upgrade *(Continued)*

Firmware Upgrade

Once you have determined your KVM and/or SIU(s) need to be upgraded, follow the steps below to install the new firmware.

1. In the Firmware Upgrade Utility main screen, open the *Options* drop-down menu at the top of the screen and select the *Com Port* option. Select the com port of the upgrade computer that the Firmware Upgrade Cable is connected to and click OK.
2. Open the *File* drop-down menu at the top of the screen and select the *Open* option. Navigate to and select the firmware upgrade file you downloaded from the Tripp Lite website.
3. Check the checkbox at the top of the screen next to the text *NetCommander IP Switch*.
4. Click on the *Start* button at the bottom center of the screen to begin the upgrade process. A prompt will appear to warn you that the KVM screen will be dark during the upgrade process. Click *OK* to proceed.
5. Towards the end of the upgrade, a prompt will appear asking if you want to set the OSD to its default settings. If yes, click the *Yes* button. If no, click the *No* button. The upgrade will finish, and the new firmware version number will be displayed.
6. If you are upgrading the SIU(s) firmware, uncheck the KVM checkbox at the top of the screen, and then check the checkboxes next to each SIU that you wish to upgrade.
7. Click on the *Start* button at the bottom center of the screen to begin the upgrade process. A prompt will appear to warn you that the KVM screen will be dark during the upgrade process. Click *OK* to proceed. When the upgrade completes, the new firmware version number(s) will be displayed next to the SIU(s).

30. Troubleshooting

Note: Disconnect device from AC mains before service operation!

When using Firmware Update software you may at times get a Communication Error message.

If a Communication Error message does appear during the update procedure, do the following:

1. Ensure that the RS232 Serial cable's RS232 connector is connected to the Switch's Communication port.
2. Ensure that the RS232 Serial cable's DB9F connector is connected to the DB9M Serial port on the CPU's rear panel.
3. Verify there is no Remote session in progress by pressing the Local button.
4. Restart the download process.

Electricity Failure

If the electricity fails during an update to the KVM firmware, do the following:

1. If the electricity fails while the switch firmware is updating, a Communication Error message will appear. Simply resume the firmware update by opening the folder that contains the firmware update file and continue from there.
2. If the electricity fails while the Server Interface Unit firmware is updating, a Not Responding or Upgrade Error message will appear. Restart the upgrade from the beginning.

Monitor Screen Failure

In the event that one of the connected computers does not display an image on the console monitor (your monitor may display an error message saying 'Unable to Display Video Mode'), you may need to update the DDC Information from the console monitor. To do this, follow these steps:

1. Remove the SIU VGA Connectors from all connected computers. Leave the USB or PS/2 connectors attached
2. Open the OSD Main Menu and press the F10 key. The OSD will flash the message 'Please Wait.' When that message stops, the update has taken place
3. Reconnect the SIU VGA Connectors of all the attached computers. You should now be able to display video from all computers

31. Specifications

Technical Specifications

Resolution	**Target Server** – Up to 1600 x 1200 @ 85Hz **Client Computer** – Recommended - resolution should be higher than on Target Server
Security	128-bit SSL encryption
Connections	**Ethernet** – RJ45 – 10/100 Mbit/sec autosensing **Serial** – RJ45 **Local KVM connection** – Screen HDD15, Keyboard./Mouse – MiniDIN6 **Flash** – RJ11 **Server** – RJ45
Weight (with unit packaging)	17 kg/37.5 lbs.
Dimensions (H x D x W)	43 mm x 712 mm x 483 mm/1.7 in. x 28 in. x 19 in.
Power input	100 – 240 VAC 50 / 60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-25°C to 60°C / -13°F to 140°F
Humidity	80% non condensing relative humidity

Video Resolution and Refresh Rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

32. Storage and Service

Storage

The KVM switch must be stored in a clean, secure environment with a temperature less than 40° C (104° F) and a relative humidity less than 90% (non-condensing). Store the KVM switch in its original shipping container if possible.

Service

Your Tripp Lite product is covered by the warranty described in this manual. A variety of Extended Warranty and On-Site Service Programs are also available from Tripp Lite. For more information on service, visit www.tripplite.com/support. Before returning your product for service, follow these steps:

1. Review the installation and operation procedures in this manual to insure that the service problem does not originate from a misreading of the instructions.
2. If the problem continues, do not contact or return the product to the dealer. Instead, visit www.tripplite.com/support.
3. If the problem requires service, visit www.tripplite.com/support and click the Product Returns link. From here you can request a Returned Material Authorization (RMA) number, which is required for service. This simple on-line form will ask for your unit's model and serial numbers, along with other general purchaser information. The RMA number, along with shipping instructions will be emailed to you. Any damages (direct, indirect, special or consequential) to the product incurred during shipment to Tripp Lite or an authorized Tripp Lite service center is not covered under warranty. Products shipped to Tripp Lite or an authorized Tripp Lite service center must have transportation charges prepaid. Mark the RMA number on the outside of the package. If the product is within its warranty period, enclose a copy of your sales receipt. Return the product for service using an insured carrier to the address given to you when you request the RMA.

33. Warranty & Warranty 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

WARNING: The individual user should take care to determine prior to use whether this device is suitable, adequate or safe for the use intended. Since individual applications are subject to great variation, the manufacturer makes no representation or warranty as to the suitability or fitness of these devices for any specific application.

Warranty Registration

Visit www.tripplite.com/warranty today to register the warranty for 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.*

WEEE Compliance Information for Tripp Lite Customers and Recyclers

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.

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

201204110 – 932924 – Rev C