Owner's Manual

Server Remote Control, External KVM over IP

Model: B051-000

Este manual esta disponible en español en la página de Tripp Lite: www.tripplite.com/support

Ce manuel est disponible en français sur le site Web de Tripp Lite : www.tripplite.com/support

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

Table of Contents

Product Features

- Connects to a computer or KVM switch to provide IP remote access.
- Includes browser-based and non-browser-based applications for accessing the unit remotely.
- Out-of-band control (OOBC) functionality allows connection of a modem, providing access to the KVM switch outside the primary network. Supports modem Dial In, Dial Out and Dial Back.
- Compatible with all major operating systems and VT100-based serial devices.
- Supports both IPv4 and IPv6.
- Supports Link Local IPv6 Address and IPv6 Stateless Auto configuration protocol.
- Provides BIOS-level access to connected computers.
- Features an RS-232 serial port, allowing you to remotely control a serial device, such as a switch or router.
- Virtual Media lets the connected computer access USB 1.1 and 2.0 media, such as DVD/CD drives and flash drives, from the computer being used to access the B051-000, as if it was directly connected.
- Virtual Media can be used to map a Smart Card / CAC reader from the computer remotely accessing the B051-000 to the connected computer.
- Laptop USB console (LUC) port provides console control of the unit.
- Remote authentication support: RADIUS, LDAP, LDAPS and MS Active Directory.
- Track critical events on the installation, such as user logins and system reboot, via SMTP email notification, SNMP traps, the included Windows-based Log Server or Syslog server.
- The Windows-based Log Server records events that take place in the installation and writes them to a searchable database. Administrators and Select accounts who are given access can search for events containing certain text or strings of text, and display them according to date and order of significance.
- Multi-level authentication – Up to 64 accounts can be created, with any combination of Administrators, Users and Select accounts. User account permissions can be customized to provide users with the desired level of access.
- Up to 32 accounts can access the B051-000 at the same time. A Message Board is provided for use in situations where multiple accounts are logged in at the same time. It allows users to communicate among each other, and provides methods for taking over control of KVM functions. Administrators can terminate active sessions.
- Supports a broad range of communication protocols: TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP.
- Allows a dynamic IP address assigned by a DHCP server to be mapped to a host name.
- Advanced encryption technology—1024-bit RSA, 56-bit DES, 256-bit AED and 128-bit SSL.
- Supports TLS 1.2 security protocol.
- Users can customize the encryption used for Keyboard/Mouse, Video and Virtual Media. They can choose between any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4 or Random.
- Access to the B051-000 can be controlled through the use of IP and/or MAC address filters, in which user-defined IP and/or MAC addresses can be granted or denied access to the unit.
- Browser-based and non-browser-based administrator utilities are provided for either the Administrator or select accounts who are given permission to perform functions, such as configuring settings, creating/editing accounts and upgrading firmware.
- Multi-language support—Administrator utility can be displayed in English, German, Russian, Japanese, Korean, Traditional Chinese and Simplified Chinese. A virtual keyboard is provided for use in a remote session. It can be displayed in U.S. English, U.K. English, Chinese, French, German, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Swedish and U.S. International.
- Remote Toolbar provides an easy way to control a remote session and adjust settings, such as Video Quality, that can impact session performance.
- Supports remote video resolutions up to 1920 x 1080 @ 60 Hz with up to 24-bit color depth.
- Supports importing third-party CA certificates.
- Exit macros can be set to be executed upon exiting a remote session.

Package Contents

- B051-000 IP Server Remote Access Unit
- USB / PS/2 Combo KVM Cable Kit, 4 ft.
- USB / PS/2 Combo Console Cable Kit, 10 in.
- USB 2.0 LUC Cable, 6 ft.
- External Power Adapter with NEMA 1-15P Plug & 5 ft. Cord
  (Input: 100–240V, 50/60 Hz, 0.5A; Output: 5.3V 2.4A, Max 13W)
- Rack-Mounting Hardware
- Software CD
- Quick Start Guide
- Owner's Manual

Remote Console Computer Requirements

- Browsers must support 128-bit SSL encryption.
- For the browser-based Java Applet and non-browser AP Java Client, you must install the latest version of Sun's Java Runtime Environment (JRE) and have 250 MB of memory available after installation.
- For the Log Server, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.
- For best results, the computers used to access the switch must have at least a Pentium III 1 GHz processor and their screen resolution set to 1024 x 768.
- For best results, a network transfer speed of at least 512 kbps is recommended.
- For the browser-based Windows Client, at least 60 MB of memory must be available after installation.
- For the non-browser Windows Client, at least 25 MB of memory must be available after installation.

Connected Computer/Server Requirements

Computers/servers to be connected to the B051-000 must have the following:

- VGA, SVGA or Multisync port
- For USB Connections: USB-A port and USB host controller
- For PS/2 Connections: 6-pin mini-DIN keyboard and mouse ports

Supported Video Resolutions

Only the following non-interlaced video signals are supported:

Resolution	Refresh Rates
640 x 480	60, 72, 75, 85, 90, 100, 120
720 x 400	70
800 x 600	56, 60, 72, 75, 85, 90, 100, 120
1024 x 768	60, 70, 75, 85, 90, 100
1152 x 864	60, 70, 75, 85
1280 x 720	60
1280 x 1024	60, 70, 75, 85
1600 x 1050	60
1600 x 1200	60
1920 x 1080	60
1920 x 1200	60

Supported Operating Systems

Compatible with all major operating systems.

Supported Browsers

Supported browsers for users that remotely log into the B051-000 include:

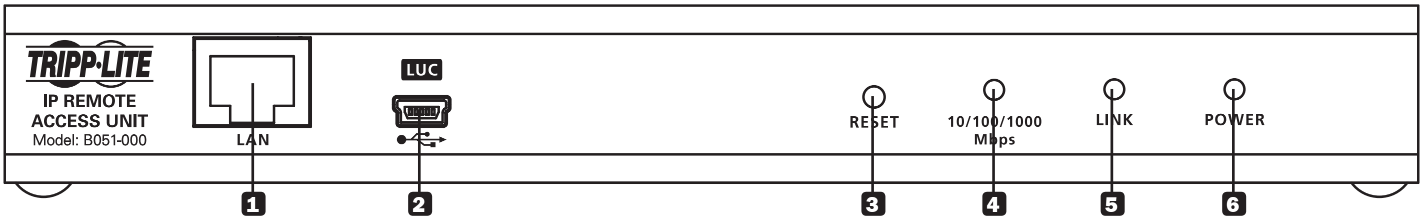
Browser	Version
Internet Explorer*	6 and higher
Chrome	8.0 and higher
Firefox	3.5 and higher
Mozilla	1.7 and higher
Safari	4.0 and higher
Opera	10.0 and higher
Netscape	9.1 and higher

* Internet Explorer 64-bit is not supported, only 32-bit.

Introduction

Components

Front Panel



1 **LAN Port**—Connects the B051-000 to the network via Cat5e/6 cable.

2 **LUC Port**—Allows a laptop to be used as a console for accessing the B051-000.

3 **Reset Button**—***Note:*** *This recessed switch must be pushed with a thin object, such as a paper clip or ballpoint pen.*

- Press and release this button with the unit running to perform a system reset.
- Press and hold this button for more than 3 seconds with the unit running to reset the unit's configuration to factory default settings. This does not clear user account information.
- Press and hold this button while powering on the unit to restore the original firmware version. You should only do this in the event of a firmware upgrade failure that results in the unit becoming inoperable.

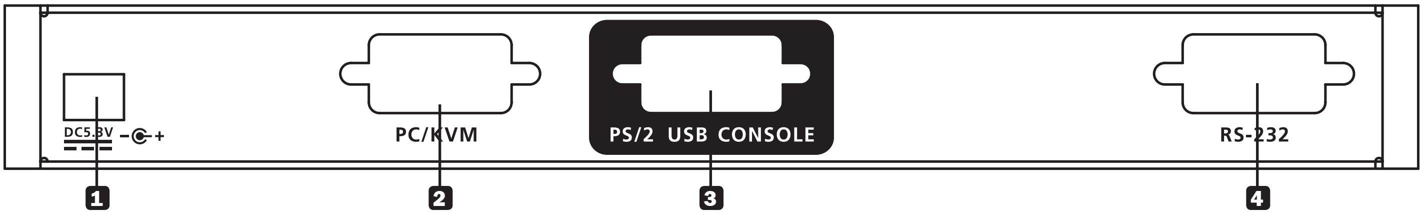
4 **10/100/1000 Mbps LED**—Lights up to indicate the transfer rate of the connected network.

- Illuminates orange when connected to a network with speeds of at least 10 Mbps.
- Illuminates green and orange when connected to a network with speeds of at least 100 Mbps.
- Illuminates green when connected to a network with speeds of at least 1000 Mbps.

5 **Link LED**—Illuminates green when the unit is being remotely accessed.

6 **Power LED**—Illuminates orange when the unit is being powered on.

Back Panel



1 **Power Jack**—Connects the included external power supply.

2 **PC/KVM Port**—Connects the included USB or PS/2 KVM cable kit, which connects a computer or KVM to the unit.

3 **Console Port**—Connects the included USB/PS/2 combo console cable kit. A VGA monitor and USB or PS/2 keyboard/mouse connect to the cable kit.

4 **RS-232 Serial Port**—Connects an RS-232 serial device or a modem for out-of-band operation.

General Safety Instructions

- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- This device is designed for IT power distribution systems with up to 230V phase-to-phase voltage.
- 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 permit adequate ventilation. To ensure reliable operation and protect against overheating, these openings must never be blocked or covered.
- The device should not 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. Use a damp cloth for cleaning. Do not use liquid or aerosol cleaners.
- 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.
- To prevent damage to your installation, ensure that all devices are properly grounded.
- 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.
- Position system cables and power cables carefully to ensure that nothing rests on any cable. 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 ampere rating of all products used on the 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.
- To help protect your system from sudden transient increases and decreases in electrical power, it is recommended that you plug your devices into a Tripp Lite surge protector, line conditioner, or uninterruptible power supply (UPS).
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following precautions:
  - > 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 take 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
- Adjust only those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive repair work by a qualified technician.
- Do not connect the RJ11 connector marked “UPGRADE” to a public telecommunication network.

Hardware Setup

Rack-Mounting Safety Instructions

- 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 into the rack first.
- 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 percent of the branch circuit rating.
- Make sure that all equipment used on the rack, including power strips and other electrical connectors, is properly grounded.
- Ensure that proper airflow is provided for devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer.
- Do not step on or stand on any device when servicing other devices in a rack.

Stacking

The B051-000 can be placed on any level surface that can safely support both its weight and the weight of attached cables. When placing it on a desktop, remove the backing material from the included rubber feet and attach the rubber feet to the bottom panel at the corners.

Note: *To ensure adequate ventilation, allow at least 2 in. (5 cm) on each side and 5.25 in. (13 cm) in back for power cord and cable clearance.*

Hardware Setup

Rack Mounting

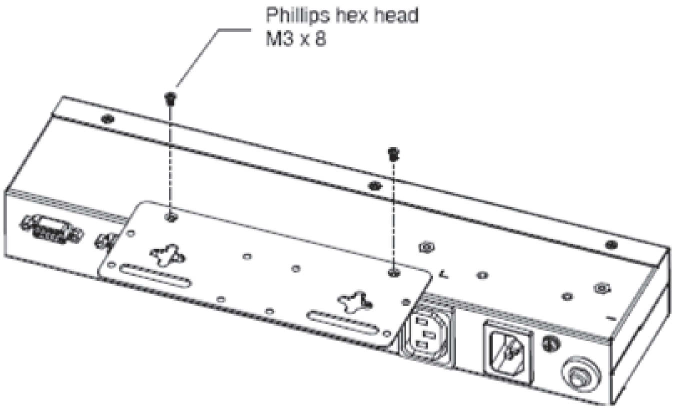
The B051-000 comes with both 0U and DIN rail mounting hardware, so that it can be conveniently mounted on a system rack.

Note: *Diagram shows B051-000-AC, but all instructions also apply to B051-000.*

To mount the unit using the 0U hardware, follow these steps:

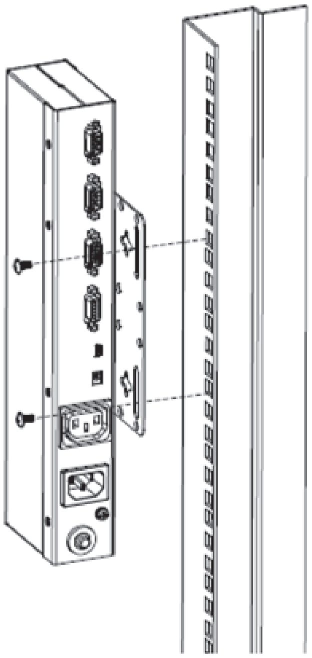
1. Remove the two screws from the top or bottom of the unit (towards the back panel).
2. Secure the bracket to the unit using the two screws you just removed.
3. Mount the unit in a standard 19-inch rack using appropriate user-supplied screws.

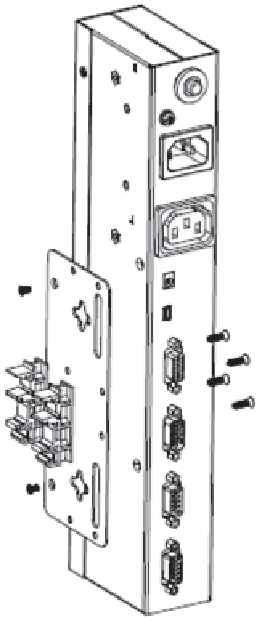
   Note: *The unit can also be wall-mounted using the included 0U mounting hardware.*



To mount the unit using the DIN rail hardware, follow these steps:

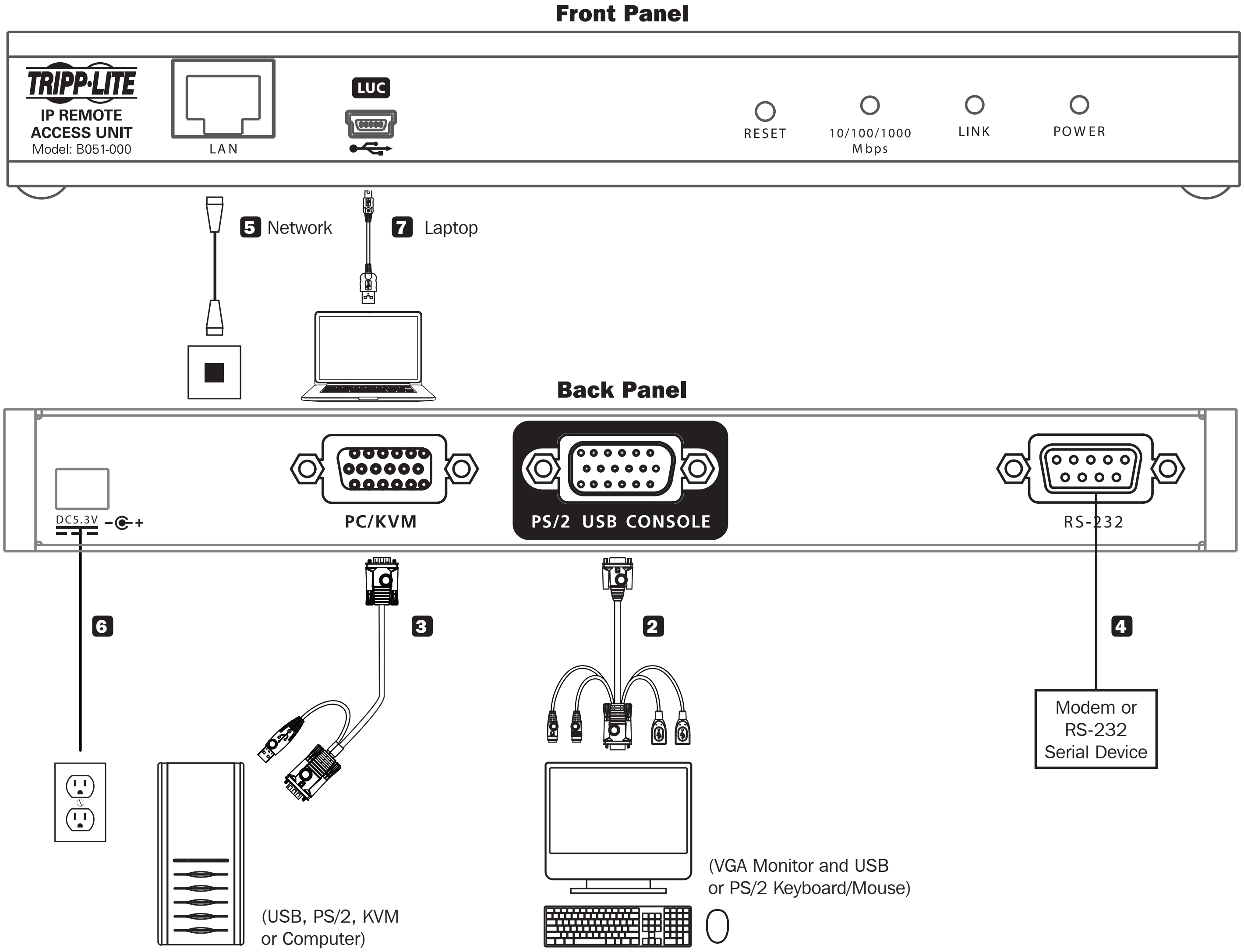
1. Secure the 0U mounting bracket to the unit by following steps 1 and 2 in the previous section.
2. Secure the DIN rail hardware to the 0U hardware using the included screws.
3. Hang the unit on the DIN rail.





Hardware Setup

Installation



1 Be sure power to all devices you are connecting is turned off.

2 Using the included USB/PS/2 combo console cable kit, connect the PS/2–USB Console port to a VGA monitor and a USB or PS/2 keyboard and mouse.

Note: You can connect any combination of keyboard/mouse: USB and PS/2, USB and USB or PS/2 and PS/2.

3 Using either of the included USB or PS/2 KVM cable kits, connect the PC/KVM port to the VGA monitor and USB or PS/2 keyboard/mouse ports on a computer or KVM switch.

***Note:** The installation diagram shows a USB KVM cable kit. The PS/2 KVM cable kit is the same, except it has two PS/2 connectors to connect to the PS/2 ports on a computer or KVM switch. Use the cable kit appropriate for your installation.*

4 **(Optional)** Connect a modem or other RS-232 serial device to the unit's RS-232 port.

5 Connect the LAN port to your network using a standard Cat5e/6 cable.

6 Connect the included external power supply to the power jack, then plug it into a Tripp Lite surge protector, UPS or PDU.

7 **(Optional)** When using the Laptop USB Console (LUC) feature, connect the LUC port to a USB port on the laptop using the included USB Mini-B cable.

Laptop USB Console (LUC)

The front panel of the B051-000 features an LUC port (see Step 7 above), which connects to the USB port on a laptop to provide console control of the unit. To use this feature, connect your laptop to the LUC port on the front of the B051-000 using a USB Mini-B cable. When connected, an extra drive will appear in your computer's My Computer screen. Click this drive to bring up the Windows and Java non-browser clients. Run the desired client to access the B051-000. The client's login screen will appear, with the B051-000 showing up as a USB Mass Storage device in the login screen's server list. Highlight the B051-000 and then connect per the instructions in the AP Windows Client Login and/or AP Java Client Login sections of this manual.

Administrator Setup

First-Time Setup

Once the B051-000 has been installed, the Administrator must prepare the unit for user operation by setting the network parameters and adding users.

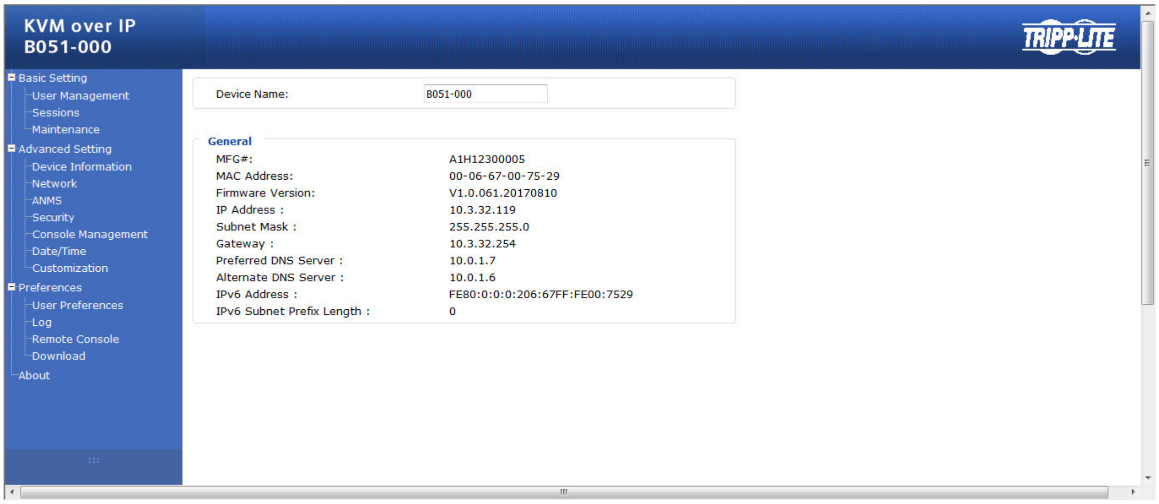
Network Setup - IP Address Determination

If you are an administrator logging in for the first time, you must access the B051-000 in order to give it an IP address to which users can connect. You can do this via *Web Browser*, the *IP Installer* utility, or the non-browser *Windows* or *Java Client* applications.

Web Browser

By default, the B051-000 is set to have its IP address assigned automatically via DHCP server. If it is 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. If it is on an IPv6 network, the default IP address is determined by the B051-000's MAC address. For example, if the MAC address is 00-10-74-13-81-01, the IPv6 address is **FE80:0:0:0:**0010:74**FF:FE**13:8101. The parts of the IP address that are in bold and underlined are fixed.

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 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 User Name (*administrator*) and the default Password (*password*). The Admin Utility Main Page will open upon entering the User Name and Password.

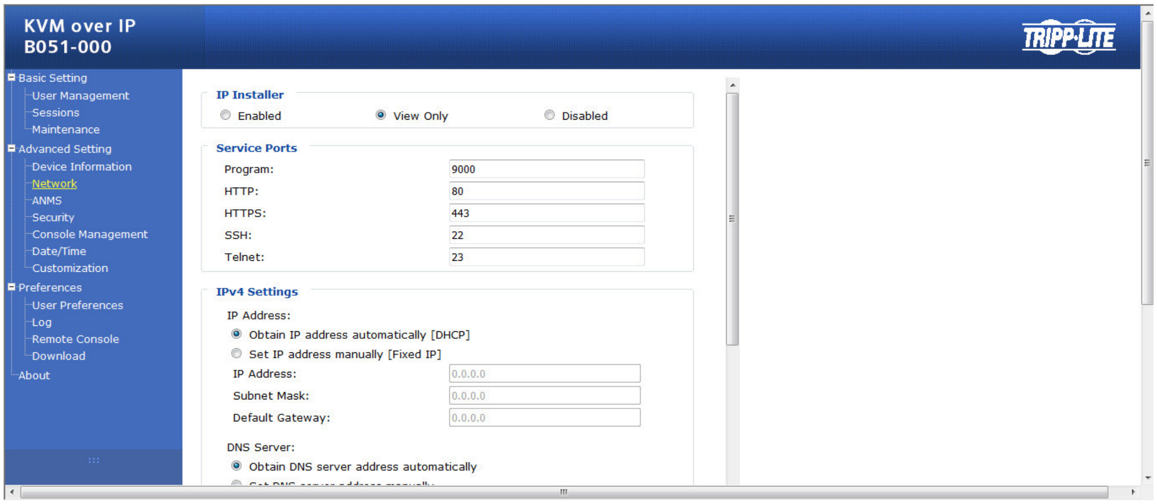


Device Name: B051-000

General

MFG#:	A1H12300005
MAC Address:	00-06-67-00-75-29
Firmware Version:	V1.0.061.20170810
IP Address :	10.3.32.119
Subnet Mask :	255.255.255.0
Gateway :	10.3.32.254
Preferred DNS Server :	10.0.1.7
Alternate DNS Server :	10.0.1.6
IPv6 Address :	FE80:0:0:0:206:67FF:FE00:7529
IPv6 Subnet Prefix Length :	0

4. Click on the *Network* icon at the top of the page to bring up the *Network Settings* page.



IP Installer

○ Enabled ● View Only ○ Disabled

Service Ports

Program:	9000
HTTP:	80
HTTPS:	443
SSH:	22
Telnet:	23

IPv4 Settings

IP Address:

● Obtain IP address automatically [DHCP]

○ Set IP address manually [Fixed IP]

IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0

DNS Server:

● Obtain DNS server address automatically

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.*

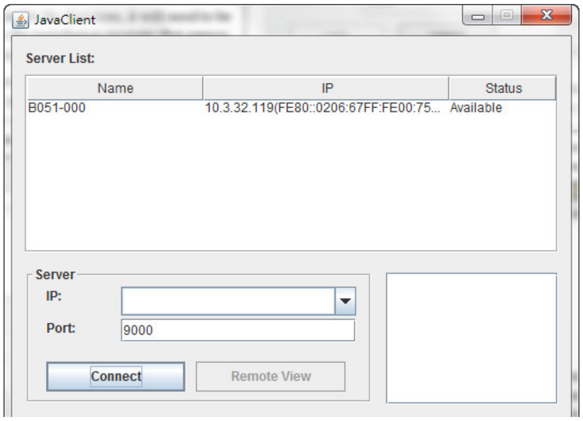
8. When you have entered the *IP Address* and *DNS Server* settings, click the *Apply* button. Clicking the *Apply* button will automatically check the *Reset on exit* checkbox located in the *Customization* page of the Admin Utility. When you log out, the unit will be reset and your network changes will be applied.

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

Non-Browser Client

The CD that comes with the product includes Windows and Java Client applications that allow you to remotely access the B051-000 and its Admin Utility 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 IP remote access unit, 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 IP remote access unit, you must obtain the IP address from your network administrator and manually enter it into the client. (See *Web 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.

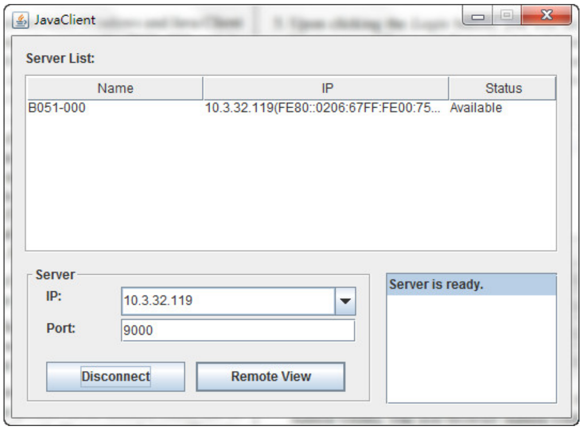


Name	IP	Status
B051-000	10.3.32.119(FE80::0206:67FF:FE00:75...	Available

IP:

Port: 9000

4. If you are on the same network as the B051-000, 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 *Connect* 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 *Connect* button.
5. Upon clicking the *Connect* button, you will be prompted to enter in a User Name and Password. Enter the default User Name (*administrator*), and the default Password (*password*).



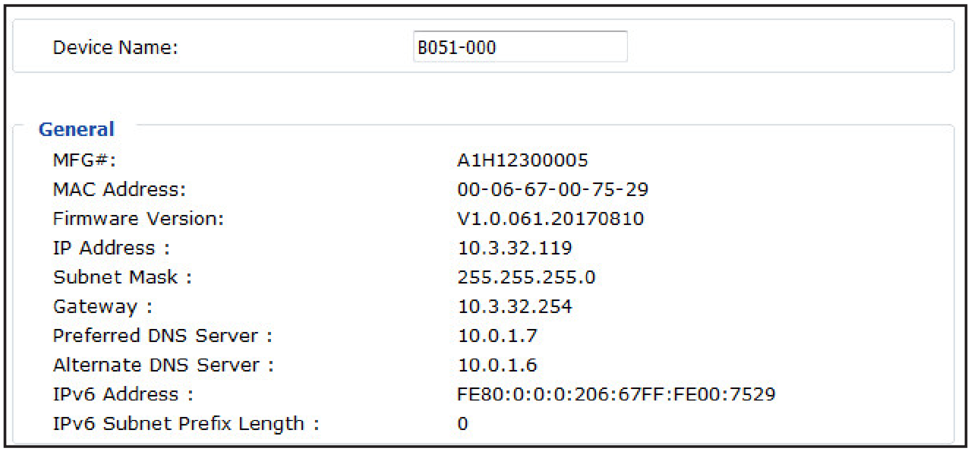
Name	IP	Status
B051-000	10.3.32.119(FE80::0206:67FF:FE00:75...	Available

IP: 10.3.32.119

Port: 9000

Server is ready.

6. Click the Remote View Button to initiate a remote session. Then, using the remote toolbar at the top of the screen, click the Open GUI icon to open the administrative interface. The non-browser *Admin Utility* contains most of the features in the browser version, but presented in a different format. See the *Admin Utility* section for details on the differences between the two versions.



Device Name: B051-000

General

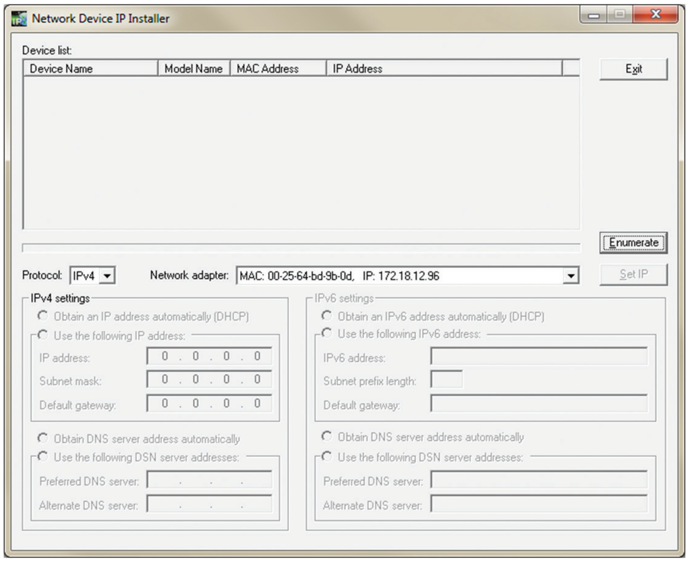
MFG#:	A1H12300005
MAC Address:	00-06-67-00-75-29
Firmware Version:	V1.0.061.20170810
IP Address :	10.3.32.119
Subnet Mask :	255.255.255.0
Gateway :	10.3.32.254
Preferred DNS Server :	10.0.1.7
Alternate DNS Server :	10.0.1.6
IPv6 Address :	FE80:0:0:0:206:67FF:FE00:7529
IPv6 Subnet Prefix Length :	0

7. Click on the Network tab at the top of the screen. From here, a fixed IP address can be assigned in the same way as when using a web browser. (See steps 4 through 8 in the *Web Browser* section)

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. 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 IP remote access unit. Also, the IP Installer setting in the Admin Utility must be set to Enabled, which it is by default. (See the ANMS section for details)

1. Save the *IP Installer* utility file to a desired location on your computer. Double-click on the file to open the *IP Installer* utility.



Protocol: IPv4

Network adapter: MAC: 00-25-64-bd-9b-0d, IP: 172.18.12.96

IPv4 settings

- ○ Obtain an IP address automatically (DHCP)
- ○ Use the following IP address:
  - IP address: 0 . 0 . 0 . 0
  - Subnet mask: 0 . 0 . 0 . 0
  - Default gateway: 0 . 0 . 0 . 0
- ○ Obtain DNS server address automatically
- ○ Use the following DSN server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .

IPv6 settings

- ○ Obtain an IPv6 address automatically (DHCP)
- ○ Use the following IPv6 address:
  - IPv6 address:
  - Subnet prefix length:
  - Default gateway:
- ○ Obtain DNS server address automatically
- ○ Use the following DSN server addresses:
  - Preferred DNS server:
  - Alternate DNS server:

2. Select the B051-000 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.*

3. To assign a fixed IP address, check the *Specify an IP address* checkbox and fill in the *IP Address, Subnet Mask* and *Default Gateway* fields with information appropriate for your network.

4. Click the *Set IP* button to apply the changes to the unit. The new IP address will appear in the *Device List*.

5. Click the *Exit* button to exit the *IP Installer* utility.

Logging Into the B051-000

The B051-000 IP remote access unit can be accessed in several ways; local console, web browser, non-browser Windows or Java client. This section describes the login procedures for each of these methods.

Local Console Login

When accessing the unit via the local console, there is no login required except for what is required to access the connected computer or KVM switch. The local keyboard, monitor and mouse function the same as if they were connected directly to the computer or KVM.

Web Browser Login

To log into the IP remote access unit via web browser, follow the steps below.

***Note**: Windows Vista and later users who intend to use the unit's Virtual Media feature must run Internet Explorer as an administrator. (See Virtual Media section for details)*

1. Open your browser and enter the IP address of the B051-000 as given to you by your system administrator.

   ***Note**: For security purposes, a login string may have been set by the administrator. If so, you must include a forward slash and the login string following the IP address. For example, to access a B051-000 with an IP address of 192.168.0.60 and a login string of B051000, you would enter the URL as 192.168.0.60/B051000.*

2. When logging in for the first time, a security alert appears to inform you that the device's certificate is not trusted, and asks if you want to proceed. The certificate can be trusted, but the alert is triggered because the certificate's name is not found in the browser's list of trusted certificates.

You have two options:

a. If you are working on a computer other than your own, choose to proceed with your session even though the certificate is not trusted.

b. If you are working on your own computer, install the certificate by following the steps below. ***Note**: You may need to run Internet Explorer as an administrator to install the certificate.*

   a. In the Security Alert dialog box, click *View Certificate*. The certificate information dialog box appears.

   b. Click *Install Certificate*.

   c. Follow the installation wizard to complete the certificate installation. Unless you have a specific reason to choose otherwise, accept the default options.

   d. When presented with a caution screen asking you to confirm that you want to install the certificate, click *Yes*.

   e. Click *Finish* to complete the installation and click OK to close the dialog box. The certificate is now trusted.

c. You may continue to get a security alert stating that the name on the security certificate does not match the name attached to the website. Follow the steps below to correct this issue.

   a. In Internet Explorer, go to the *Tools > Internet Options* menu and click the *Advanced* tab.

   b. In the *Settings* list, scroll down to and uncheck the *Warn about certificate address mismatch* setting.

   ***Note:** In order for this setting to take effect, you must close out of and restart Internet Explorer.*

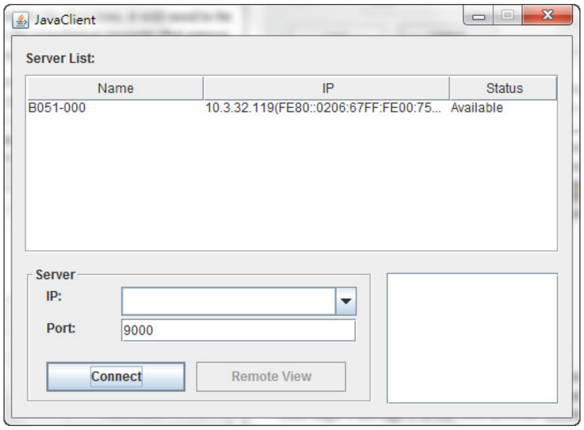
3. Upon installing the certificate or choosing to continue even though the certificate is not trusted, a login page appears asking you to enter a user name and password. Enter in your user name and password as given to you by your system administrator. If you are an administrator logging in for the first time, the default user name is *administrator*, and the default password is *password*.

Logging Into the B051-000

Non-Browser Login

The CD that comes with the product includes Windows and Java Client applications that allow you to remotely access the B051-000 and its Admin Utility 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. If you do not have access to the CD, you will need to obtain a copy of the Windows and/or Java Client from your system administrator.

1. Save the Windows or Java client to a desired location on your computer. Double-click on 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. If you do not have access to the CD, you will need to obtain the serial number from your system administrator. Once entered, you will not be prompted for it again. The non-browser client connection screen appears.
4. If you are on the same network as the B051-000, 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 *Connect* 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, as given to you by your system administrator, in the IP Address field, and then click the *Connect* button.



Server List:

Name	IP	Status
B051-000	10.3.32.119(FE80::0206:67FF:FE00:75...	Available

Server

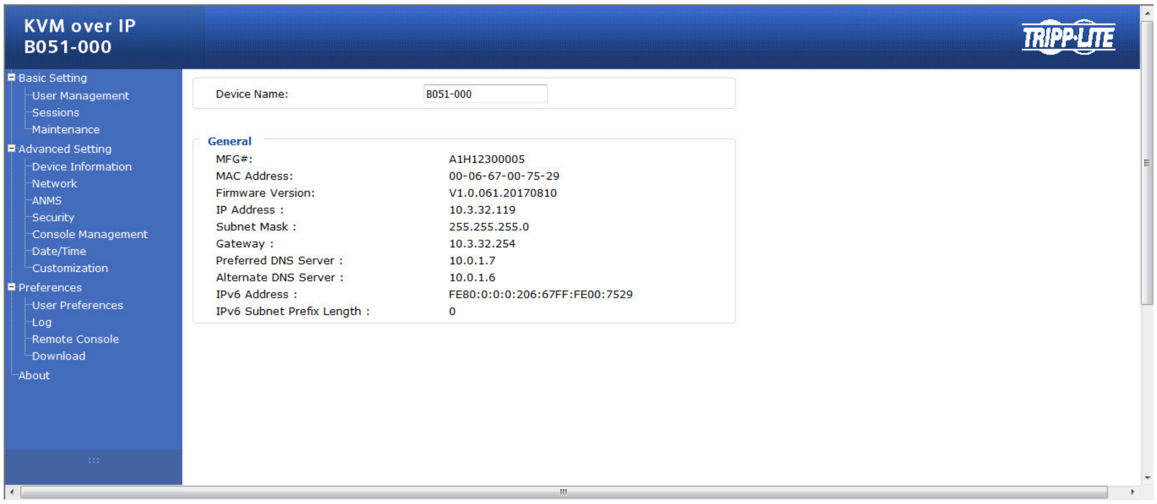
IP:

Port: 9000

5. Upon clicking the *Connect* button, you will be prompted to enter a User Name and Password, which were given to you by your system administrator. If you are an administrator logging in for the first time, your default User Name is *administrator* and the default Password is *password*.

Admin Utility

Device Information is the page that displays by default when the Admin Utility is accessed. The features found in the *Device Information* page and the corresponding pages of the Admin Utility are discussed in this section.



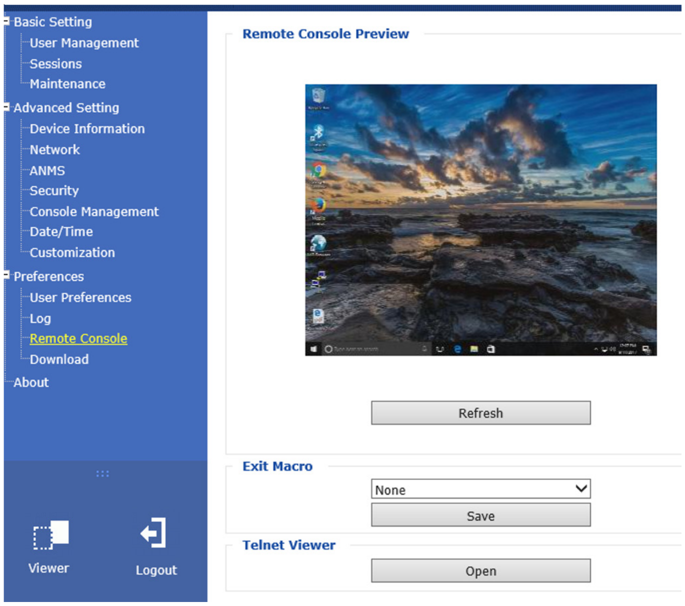
Device Name:	B051-000

General

MFG#:	A1H12300005
MAC Address:	00-06-67-00-75-29
Firmware Version:	V1.0.061.20170810
IP Address :	10.3.32.119
Subnet Mask :	255.255.255.0
Gateway :	10.3.32.254
Preferred DNS Server :	10.0.1.7
Alternate DNS Server :	10.0.1.6
IPv6 Address :	FE80:0:0:0:206:67FF:FE00:7529
IPv6 Subnet Prefix Length :	0

Remote Console Preview

The *Remote Console Preview* is available via web browser only. It displays a snapshot of the screen of the connected computer/KVM. Clicking the *Refresh* button below the preview screen will refresh it to display the current screen image.



Java Applet and Windows Client

On the left side of the *Remote Console Preview* screen is a viewer link that allows you to initiate a remote session. By default, the Admin Utility is set to auto-detect which browser you are using and to display the appropriate link. If you are using Internet Explorer, the default link will be *Windows Client*. If you are using any browser other than IE, the default link will be *Java Applet*.

Java Applet can be used in both IE and non-IE browsers, but *Windows Client* can only be used in IE. To use *Java Applet* in IE, you must select it from the *User Preferences* page (see the *User Preferences* section for details). Clicking one of these links will initiate a remote session (see *Remote Session Operation* for details).

Exit Macro

Under the *Remote Console Preview screen* links is the *Exit Macro* drop-down list. This drop-down list will contain all of the user-created macros. (See *Macros* section for details) Selecting a macro from this list and clicking the *Save* button will cause that macro to be performed upon exiting a remote session.

Telnet/SSH Viewer

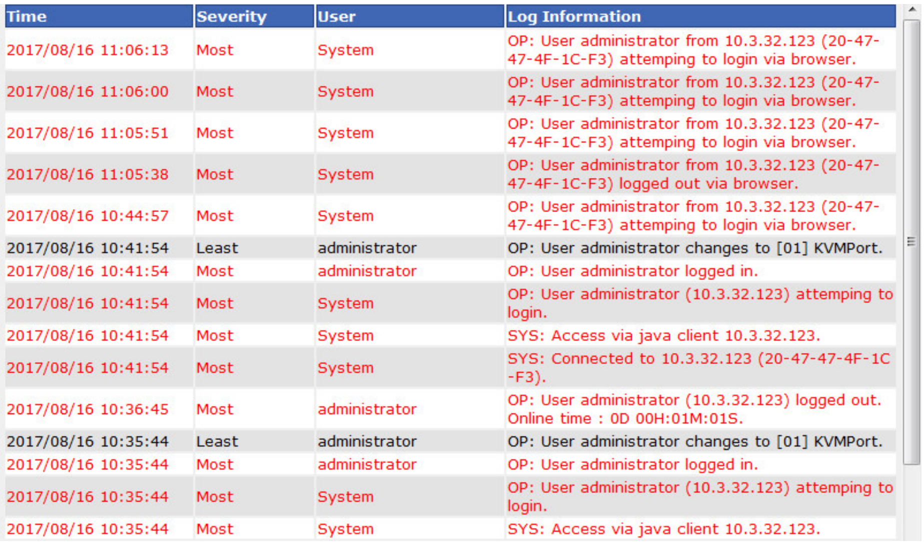
Under the *Exit Macro* section is the *Telnet/SSH Viewer* section, which provides access to the serial device connected to the B051-000. Depending on the permission given to the user accessing the Admin Utility, either the *Telnet Viewer*, the *SSH Viewer*, both viewers or neither will appear. Click on the *Telnet Viewer* to initiate a Telnet session or the *SSH Viewer* to initiate a SSH session.

Log (Browser Only)

The B051-000 logs all events that take place on it (e.g. login, logout, system reboot, etc.) and writes them to a log file. The web browser Admin Utility contains a *Log* section, which provides a list of the 512 most current events that took place on the unit. After the 512 record limit is reached, the oldest records will be deleted and replaced with the newest ones.

To clear the log file, click the *Clear Log* button in the lower-right corner.

For a more extensive solution, a Windows-based Log Server is provided with the CD that comes with the unit. (See *Log Server* section for details) The Log Server provides a searchable database of all the events on the installation, not just the 512 most recent ones.



Time	Severity	User	Log Information
2017/08/16 11:06:13	Most	System	OP: User administrator from 10.3.32.123 (20-47-47-4F-1C-F3) attemping to login via browser.
2017/08/16 11:06:00	Most	System	OP: User administrator from 10.3.32.123 (20-47-47-4F-1C-F3) attemping to login via browser.
2017/08/16 11:05:51	Most	System	OP: User administrator from 10.3.32.123 (20-47-47-4F-1C-F3) attemping to login via browser.
2017/08/16 11:05:38	Most	System	OP: User administrator from 10.3.32.123 (20-47-47-4F-1C-F3) logged out via browser.
2017/08/16 10:44:57	Most	System	OP: User administrator from 10.3.32.123 (20-47-47-4F-1C-F3) attemping to login via browser.
2017/08/16 10:41:54	Least	administrator	OP: User administrator changes to [01] KVMPort.
2017/08/16 10:41:54	Most	administrator	OP: User administrator logged in.
2017/08/16 10:41:54	Most	System	OP: User administrator (10.3.32.123) attemping to login.
2017/08/16 10:41:54	Most	System	SYS: Access via java client 10.3.32.123.
2017/08/16 10:41:54	Most	System	SYS: Connected to 10.3.32.123 (20-47-47-4F-1C-F3).
2017/08/16 10:36:45	Most	administrator	OP: User administrator (10.3.32.123) logged out. Online time : 0D 00H:01M:01S.
2017/08/16 10:35:44	Least	administrator	OP: User administrator changes to [01] KVMPort.
2017/08/16 10:35:44	Most	administrator	OP: User administrator logged in.
2017/08/16 10:35:44	Most	System	OP: User administrator (10.3.32.123) attemping to login.
2017/08/16 10:35:44	Most	System	SYS: Access via java client 10.3.32.123.

User Preferences

The *User Preferences* page allows you to determine which viewer is used to initiate a remote session and which language the Admin Utility is displayed in. It is also a convenient place in which to change your password. The non-browser clients provide a method for changing your password and setting the Admin Utility language, but do not allow you to determine the viewer used to initiate a remote session. These settings are described in the following section.

Viewer (Browser only)

The *Viewer* section provides three options for choosing what is used (Windows Client or Java Applet) to initiate a remote session: *Auto Detect, Java* and *User Select*. When using the non-browser Windows Client, the Windows Client viewer is automatically used. When using the non-browser Java Client, the Java Applet viewer is automatically used.

- *Auto Detect* automatically chooses based on your browser. If you are using Internet Explorer, the Windows Client is used. If using a browser other than Internet Explorer, the Java Applet is used.
- *Java* uses the Java Applet to initiate a remote session.
- *User Select* places both the Windows Client and Java Applet viewer links in the *Remote Console Preview* section, allowing the user to click on whichever one they want to use.

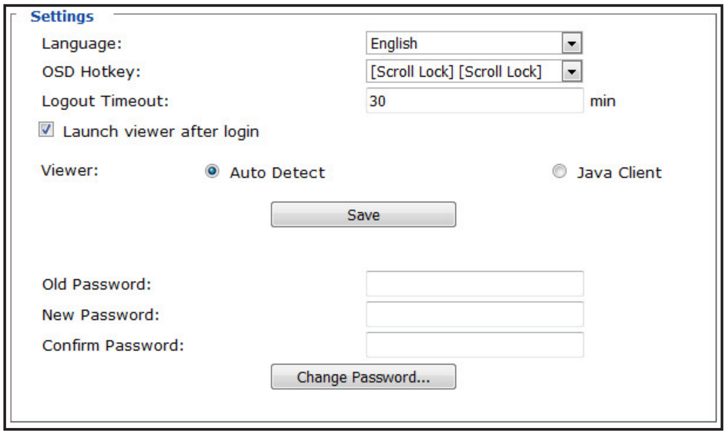
  Note*: As the Windows Client viewer cannot be used in browsers other than Internet Explorer, this setting is only functional in Internet Explorer. When using a browser other than Internet Explorer, you will be able to select this setting; however, only the Java Applet viewer link will appear in the Remote Console Preview section.*

After marking the checkbox of the viewer setting you desire, click the *Apply* button to save the change.

Admin Utility

Set Language

The drop-down list in this section allows you to choose among the following languages for displaying the Admin Utility: English, German, Russian, Japanese, Korean, Traditional Chinese, Simplified Chinese, French, Italian and Spanish. Select the desired language from the drop-down list, and click the *Apply* button to save the change.



Settings

Language: English

OSD Hotkey: [Scroll Lock] [Scroll Lock]

Logout Timeout: 30 min

☑ Launch viewer after login

Viewer: ● Auto Detect ○ Java Client

Old Password:

New Password:

Confirm Password:

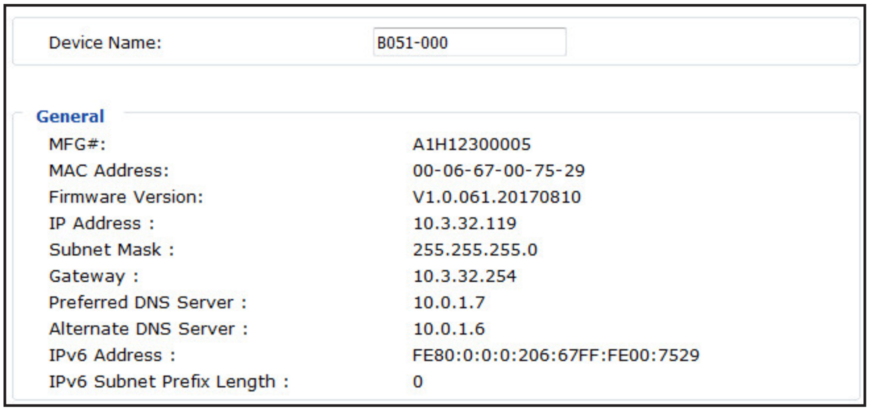
Change Password

To change your password, enter your current password in the *Old Password* field, and then enter your new password twice; in the *New Password* and *Confirm New Password* fields. Click the *Change Password* button to save the change.

Device Information

The *Device Information* page provides information about your B051-000, including firmware version number and IP address. It is the first page to be displayed. If you have switched to a new page, you can navigate back to it by clicking the corresponding tab.

***Note**: An IPv6 address is included in the* Device Information *page. This is a default address that is given to the unit, and can be used to access the B051-000 via browser and/or the non-browser clients. It cannot be used to communicate with LDAP, RADIUS and other management devices. An IPv6 address cannot be assigned to the unit via DHCP server, nor can one be manually set by the administrator.*



Device Name: B051-000

General

MFG#:	A1H12300005
MAC Address:	00-06-67-00-75-29
Firmware Version:	V1.0.061.20170810
IP Address :	10.3.32.119
Subnet Mask :	255.255.255.0
Gateway :	10.3.32.254
Preferred DNS Server :	10.0.1.7
Alternate DNS Server :	10.0.1.6
IPv6 Address :	FE80:0:0:0:206:67FF:FE00:7529
IPv6 Subnet Prefix Length :	0

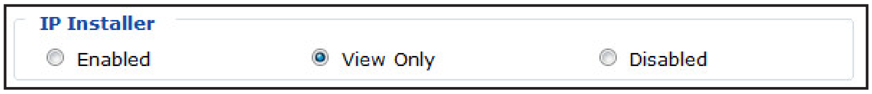
Network

The *Network* page is where the unit's network parameters are set.

The *Network* page is split into several sections, each of which is described in the following section.

IP Installer

The B051-000 comes with an *IP Installer* application that allows Windows computers to easily view and edit the KVM's network settings. This section determines what access the IP Installer has to the unit.



IP Installer

○ Enabled ● View Only ○ Disabled

- **Enabled** – When selected, the IP Installer can locate the KVM switch on the network and display its current IP address. It also allows the IP Installer to be used to change the IP address of the KVM switch. This option is checked by default.
- **View Only** – When selected, the IP Installer can locate the KVM switch on the network and display its current IP address, but it cannot be used to change the IP address of the KVM switch.
- **Disabled** – When selected, the IP Installer cannot locate the KVM switch on the network, nor can it be used to change the IP address of the KVM switch.

Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

Service Ports

This section allows you to set up port numbers that will be allowed by a firewall. If the port numbers on this page are not allowed access by the firewall, you will not be able to access the corresponding features. Valid entries for all of the service ports are from 1 to 65535. ***Note:*** *You must enter a different port number for each field. If the unit is connected to a network without a firewall, it doesn't matter what these ports are set to, as they will have no effect.*

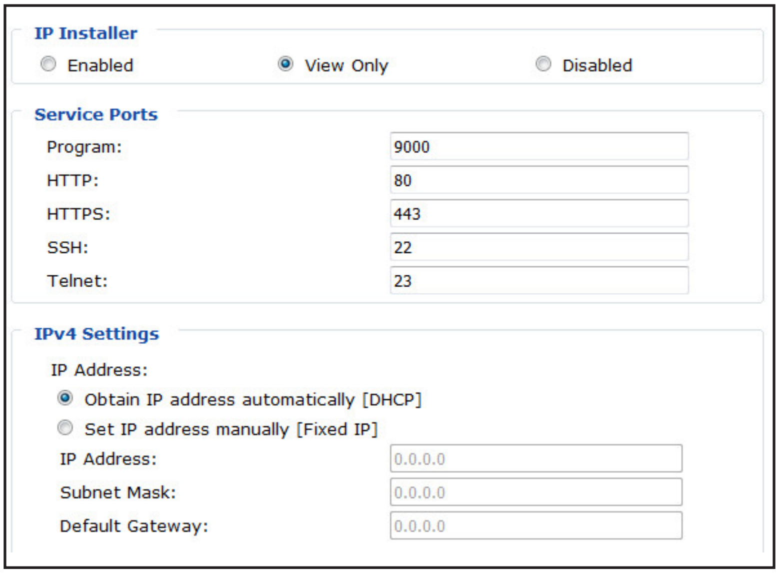
- **HTTP** – The port number used for a browser login. The default value is 80.
- **HTTPS** – The port number used for a secure browser login. The default value is 443.
- **Telnet Port** – The port number used when accessing a connected serial device via telnet. The default value is 23.
- **Program** – The port number used when accessing connected computers via the browser and non-browser Windows and Java clients. The default value is 9000.

  Note: *This port number must match the port number in the non-browser Windows and Java clients when using them to connect to the KVM switch.*
- **SSH Port** – The port number used when accessing a connected serial device via SSH. The default value is 22.

IP Address

This section allows you to obtain an IP address automatically via DHCP server or to manually assign one yourself. By default, the B051-000 is set to have its IP address assigned automatically via DHCP server. If it is 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. If it is on an IPv6 network, the default IP address is determined by the B051-000's MAC address. For example, if the MAC address is 00-10-74-13-81-01, the IPv6 address is **FE80:0:0:0:**0010:74**FF:FE**13:8101. The parts of the IP address that are in bold and underlined are fixed. The *Network* page contains fields for setting both IPv4 and IPv6 settings. Simply enter the settings for the desired network type, and leave the other section unchanged.

- **Obtain an IP Address Automatically [DHCP]** – When this option is checked, the KVM switch will have its IP address assigned to it by a DHCP server upon booting up, and the remaining fields in this section will be grayed out. This option is checked by default.
- **Set IP Address Manually [Fixed IP]** – Check this option if you wish to assign an IP address to the KVM yourself. When checked, the settings fields below will be activated for you to edit.
- **IP Address** – Enter the desired IP address here.
- **Subnet Mask** – Enter the desired Subnet Mask here.
- **Default Gateway** – Enter the desired Default Gateway here.



IP Installer

○ Enabled ● View Only ○ Disabled

Service Ports

Program:	9000
HTTP:	80
HTTPS:	443
SSH:	22
Telnet:	23

IPv4 Settings

IP Address:

● Obtain IP address automatically [DHCP]

○ Set IP address manually [Fixed IP]

IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0

DNS Server

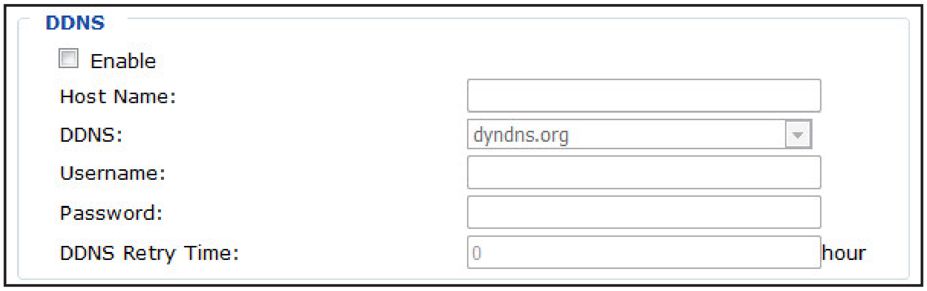
This section allows you to obtain a DNS server address automatically or to assign one yourself manually. By default, the unit is set to have its DNS server address assigned automatically.

- **Obtain DNS Server Address Automatically** – When this option is checked, the KVM switch will have its DNS Server address assigned automatically, and the remaining fields in this section will be grayed out. If you selected to set the IP address manually above, this option will be grayed out, and you will be required to enter the DNS Server address manually as well.
- **Set DNS Server Address Manually** – Check this option if you wish to assign a DNS Server address to the KVM yourself. When checked, the settings fields below will be activated for you to edit.
- **Preferred DNS Server** – Enter the preferred DNS Server address here.
- **Alternate DNS Server** – Enter the alternate DNS Server address here. This is an optional field.
- **Network Transfer Rate** – This setting allows you to set the size of the data transfer stream to match your network by setting the rate at which the unit transfers data to the remote computer/KVM. The range is from 4 to 99,999 KBps. The default is 99999.

***Note**: After making changes in the* Network *page, make sure that the* Reset on exit *checkbox in the* Customization *page (See* Customization *section for details) is checked. When changes are made, this checkbox is automatically marked, and upon logging out, the unit is reset and the changes implemented.*

DDNS

This section allows you to map an IP address assigned by a DHCP server to a host name. To provide DDNS capability for the unit, follow the steps below.



DDNS

□ Enable

Host Name:

DDNS: dyndns.org

Username:

Password:

DDNS Retry Time: 0 hour

1. Check the *Enable* checkbox. When checked, the *Host Name, DDNS, User Name, Password* and *DDNS Retry Time* fields are activated.
2. In the *Host Name* field, enter the host name that you registered with your DDNS service provider.
3. Select from the DDNS drop-down list the DDNS service you are registered with.
4. In the *User Name* and *Password* fields, key in the user name and password that authenticates you with your DDNS service.
5. When the unit's IP address changes, the DDNS server must be updated to associate the new IP address with your host name. If this process fails, it will automatically be tried again based on the time set in the *DDNS Retry Time* field. Enter a value (in hours).

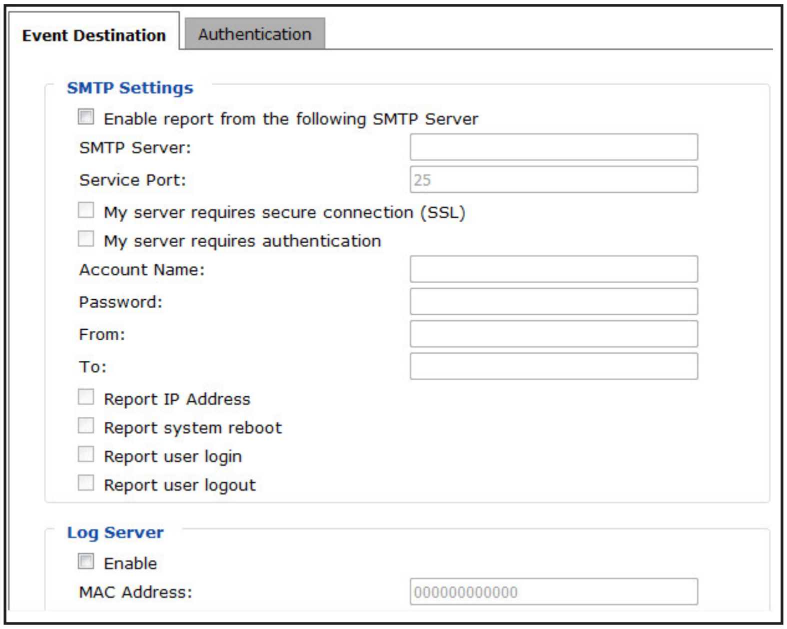
Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

ANMS

The Advanced Network Management Settings (ANMS) page allows you to set up login authentication and authorization management from external sources. The ANMS page is divided into several sections, each of which is described in the following.

SMTP Settings

The *SMTP Settings* section allows you to have notifications of system events emailed to you via SMTP server. To set up this feature, follow the steps below.



Event Destination | Authentication

SMTP Settings

□ Enable report from the following SMTP Server

SMTP Server:

Service Port: 25

□ My server requires secure connection (SSL)

□ My server requires authentication

Account Name:

Password:

From:

To:

□ Report IP Address

□ Report system reboot

□ Report user login

□ Report user logout

Log Server

□ Enable

MAC Address: 000000000000

1. Check the *Enable report from the following SMTP Server* checkbox.
2. In the *SMTP Server* field, key in the IP address or domain name of the SMTP server.
3. If your server requires a secure SSL connection, check the *Server requires authentication* checkbox.
4. If your server requires authentication, check the *Server requires authentication* checkbox. When checked, the *Account Name* and *Password* fields are activated.
5. Enter in an *Account Name* and *Password* for your SMTP server.
6. In the *From* field, key in the email address that you want the report to show as being sent from.

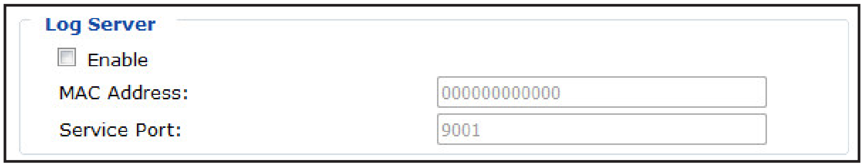
   ***Note**: Only one email address is allowed in the From field, and it cannot exceed 64 Bytes. 1 Byte is equal to 1 English alphanumeric character.*
7. In the To field, key in the email address(es) you want the report sent to.

   ***Note**: If you are entering more than one address, separate them with a semicolon. The size of all email addresses cannot combine to more than 256 Bytes. 1 Byte is equal to 1 English alphanumeric character.*
8. At the bottom of this section are the events that can be reported on: *Report IP address, Report system reboot, Report user login* and *Report user logout*. Check the checkbox next to each event for which you want reports sent.

Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

Log Server

In addition to the log that is built into the web browser Admin Utility, the B051-000 comes with an external Windows-based log server that can be installed on a computer. The *Log Server* section on the *ANMS* page is where the external log server can be enabled and set up for use. To do this, follow the steps below.



Log Server

□ Enable

MAC Address: 000000000000

Service Port: 9001

1. Check the *Enable* checkbox. When checked, the *MAC Address* and *Service Port* fields are activated.
2. In the *MAC Address* field, enter the MAC address of the computer that the log server resides on.

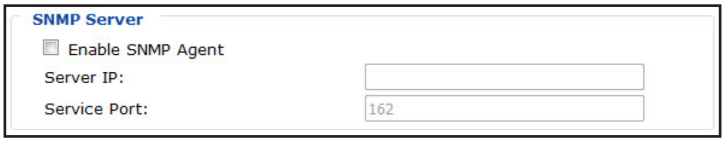
3. In the *Service Port* field, enter in a port that the firewall will allow to be used to access the log server. The valid port range is between 1 and 65535. The default port number is 9001.

   Note*: The port number entered here must not be the same as any of the ports entered into the Network page. (See the Network section in this manual for details.)*

Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

SNMP Server

This section allows you to enable SNMP traps to be sent, notifying you of events that take place on the unit. When enabled, the following SNMP traps are sent: *System Power On, Login Failure* and *System Reset*. To enable SNMP traps, follow the steps below.



SNMP Server

□ Enable SNMP Agent

Server IP:

Service Port: 162

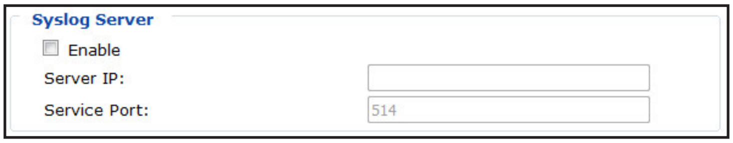
1. Check the *Enable SNMP Agent* checkbox. When checked, the *Server IP* and *Service Port* fields are activated.
2. In the *Server IP* field, enter the IP address or domain name of the computer to be notified of SNMP trap events.
3. In the *Service Port* field, enter in a port that the firewall will allow access through. The valid port range is between 1 and 65535. The default port number is 162.

   Note*: The port number entered here must not be the same as any of the ports entered into the Network page. (See the Network section in this manual for details.)*

Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

Syslog Server

To record all the events that take place on the unit and write them to a Syslog server, follow the steps below.



Syslog Server

□ Enable

Server IP:

Service Port: 514

1. Check the *Enable* checkbox. When checked, the *Server IP* and *Service Port* fields are activated.
2. In the *Server IP* field, enter the IP address or domain name of the Syslog server.
3. In the *Service Port* field, enter in a port that the firewall will allow access through. The valid port range is between 1 and 65535. The default port number is 514.

   Note*: The port number entered here must not be the same as any of the ports entered into the* Network *page (See the* Network *section in this manual for details)*.

Click the *Apply* button at the bottom of the *ANMS* page to save your changes.

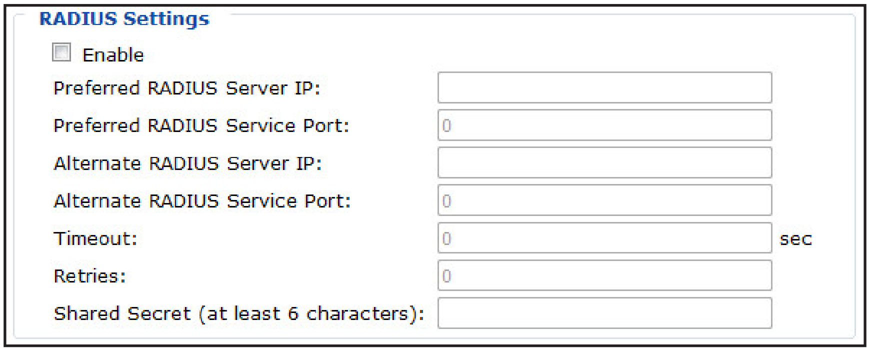
Disable Device Authentication

Clicking the Authentication tab in the ANMS section brings up the page where authentication settings are entered. When the Disable Device Authentication checkbox is checked, local authentication of the B051-000 will be disabled. This allows the unit to be accessed only by *RADIUS, LDAP, LDAPS* or *MS Active Directory* authentication. This checkbox is accessed only when the *Enabled* checkbox in the *RADIUS Settings* and/or *LDAP Settings* section is checked.

□ Disable Device Authentication

RADIUS Settings

To allow authentication and authorization for the B051-000 through a RADIUS server, follow the steps below.



RADIUS Settings

☐ Enable

Preferred RADIUS Server IP:		
Preferred RADIUS Service Port:	0	
Alternate RADIUS Server IP:		
Alternate RADIUS Service Port:	0	
Timeout:	0	sec
Retries:	0	
Shared Secret (at least 6 characters):		

1. Check the *Enable* checkbox. When checked, the fields in the *RADIUS Setting*s section are activated.
2. Fill in the IP addresses and port numbers for the Preferred and Alternate RADIUS servers.
3. In the *Timeout (seconds)* field, set the amount of time that the unit waits for a RADIUS server reply before it times out.
4. In the *Retries* field, set the number of allowed RADIUS retries.
5. In the *Shared Secret (at least 6 characters)* field, key in the character string that you want to use for authentication between the B051-000 and the RADIUS Server.
6. Click the *Apply* button at the bottom of the ANMS page to save your changes.
7. On the RADIUS server, set the access rights for each user according to the information in the table below.

   ***Note**: Characters are not case-sensitive; either capital or lower-case letters can be used. Characters are comma delimited.*

Entry	Description
c	Gives the corresponding user administrator privileges, allowing them to configure the unit.
w	Gives the corresponding user access to the B051-000 via the browser and non-browser versions of the Windows Client.
j	Gives the corresponding user access to the B051-000 via the browser and non-browser versions of the Java Client.
l	Gives the corresponding user access to the *Log* in the web browser Admin Utility.
v	Gives the corresponding user *View Only* access to the computer/KVM connected to the B051-000.
s	Gives the corresponding user access to the *Virtual Media* function in *Read Only* mode.
m	Gives the corresponding user access to the *Virtual Media* function in *Read/Write* mode.
t	Gives the user access to connected serial devices via *Telnet Session.*
h	Gives the user access to connected serial devices via *SSH Session.*
a	Gives the user access to connected serial devices via both *Telnet* and *SSH Session.*
su/user	Where user represents the user name of a B051-000 user whose permissions match the permissions you want the RADIUS authorized user to have.

The table below gives examples of RADIUS server access rights.

Entry	Description
c, w	Gives the corresponding user administrator privileges, and allows them to access the B051-000 via the browser and non-browser versions of the Windows Client.
w, j, l	Gives the corresponding user access to the B051-000 via the browser and non-browser versions of both the Windows and Java Clients, as well as access to the *Log* in the web browser Admin Utility.

LDAP Settings

To allow authentication and authorization for the B051-000 via LDAP / LDAPS, refer to the information in the table below.

Entry	Description
Enable	Check this checkbox to allow LDAP or LDAPS authentication and authorization.
LDAP / LDAPS	Click to specify whether to use LDAP or LDAPS.
LDAP Server IP and Port	Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Timeout (seconds)	Set the time in seconds that the unit waits for an LDAP or LDAPS server reply before it times out.
LDAP Administrator DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=B051-000,dc=tripplite,dc=com
LDAP Administrator Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. ***Note:*** *If the Enable Authorization checkbox is not checked, this field must include the entry where the B051-000 Admin Group is created. See the LDAP / LDAPS administrator to obtain this information.*

LDAP Configuration — Active Directory

To allow authentication and authorization for the B051-000 via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the B051-000 – ***permission*** – is added as an optional attribute to the *person* class.

- *Authentication* refers to determining the authenticity of the person logging in.
- *Authorization* refers to assigning permission to use the device's various features.

In order to configure the LDAP server, you will have to complete the following procedures: 1) Install the Windows 2003 Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema.

Install the Windows 2003 Support Tools

1. On your Windows Server CD, 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. On the *File* menu of the screen that appears, click *Add/Remove Snap-in*, then click *Add*.
5. Under *Available Standalone Snap-ins*, double click *Active Directory Schema*, click *Close* and click *OK*.
6. On the screen you are in, open the *File* menu and click *Save*.
7. For *Save in*, specify the *C:\Windows\system32* directory.
8. For *File name*, key in schmmgmt.msc.
9. Click *Save* to complete the procedure.

Creating a Start Menu Shortcut Entry

To create a shortcut entry on the Start Menu for the Active Directory Schema, do the following:

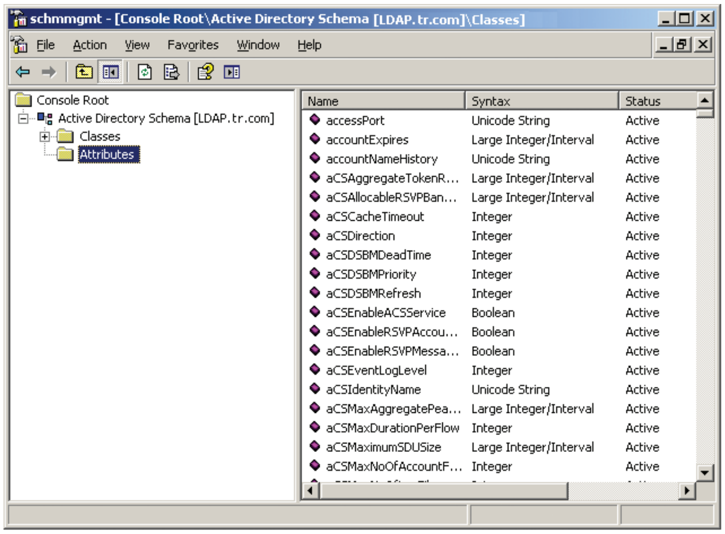
1. Right click *Start*; select: **Open all Users** → **Programs** → **Administrative Tools**.
2. On the *File* menu, select **New** → **Shortcut**
3. In the dialog box that comes up, browse to or key in the path to schmmgmt.msc (C:\Windows\system32\schmmgmt.msc) and click *Next***.**
4. In the dialog box that comes up, key in *Active Directory Schema* as the name for the shortcut, then click *Finish***.**

Extend and Update the Active Directory Schema

Step 1 - Create a New Attribute:

a) Open **Control Panel** ⟶ **Administrative Tools** ⟶ **Active Directory Schema**.

b) In the left panel of the screen that comes up, right-click *Attributes*:


schmmgmt - [Console Root\Active Directory Schema [LDAP.tr.com]\Classes]
File
Action
View
Favorites
Window
Help

Console Root
Active Directory Schema [LDAP.tr.com]
Classes
Attributes

Name	Syntax	Status
accessPort	Unicode String	Active
accountExpires	Large Integer/Interval	Active
accountNameHistory	Unicode String	Active
aCSAggregateTokenR...	Large Integer/Interval	Active
aCSAllocableRSVPBan...	Large Integer/Interval	Active
aCSCacheTimeout	Integer	Active
aCSDirection	Integer	Active
aCSDSBMDeadTime	Integer	Active
aCSDSBMPriority	Integer	Active
aCSDSBMRefresh	Integer	Active
aCSEnableACSService	Boolean	Active
aCSEnableRSVPAccou...	Boolean	Active
aCSEnableRSVPMessa...	Boolean	Active
aCSEventLogLevel	Integer	Active
aCSIdentityName	Unicode String	Active
aCSMaxAggregatePea...	Large Integer/Interval	Active
aCSMaxDurationPerFlow	Integer	Active
aCSMaximumSDUSize	Large Integer/Interval	Active
aCSMaxNoOfAccountF...	Integer	Active

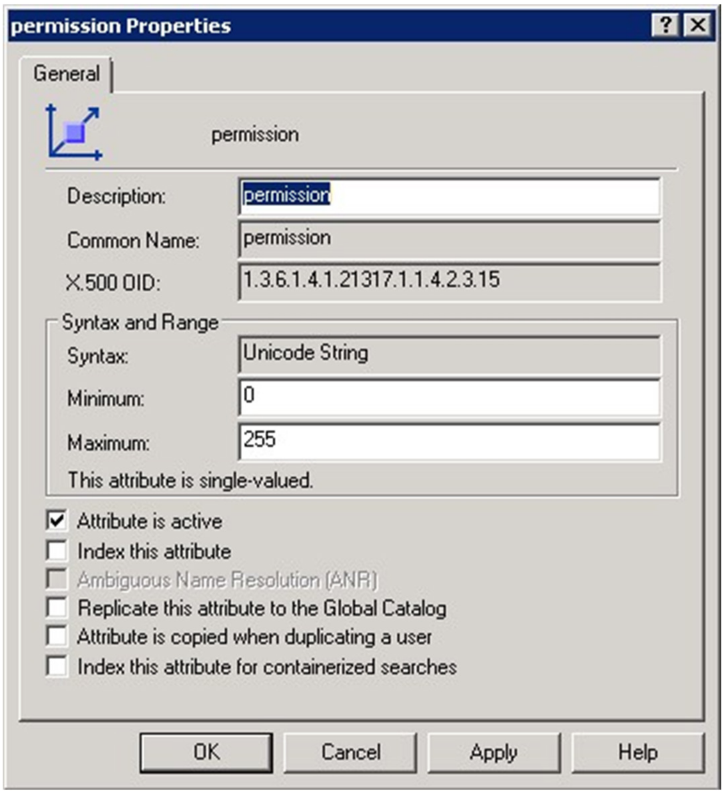
c) Select **New** ⟶ **Attribute**.

d) In the warning message that appears, click *Continue* to bring up the *Create New Attribute* dialog box.

e) Fill in the dialog box according to the example below and click *OK* to complete step 1 of the procedure.

- **Common Name –** ***permission***
- **LDAP Display Name –** ***permission***
- **Syntax –** Unicode String
- **Minimum –** 1
- **Maximum –** 255

Note: *The Unique X500 Object ID uses periods, not commas.*



permission

Description: permission

Common Name: permission

X.500 OID: 1.3.6.1.4.1.21317.1.1.4.2.3.15

Syntax and Range

Syntax: Unicode String

Minimum: 0

Maximum: 255

This attribute is single-valued.

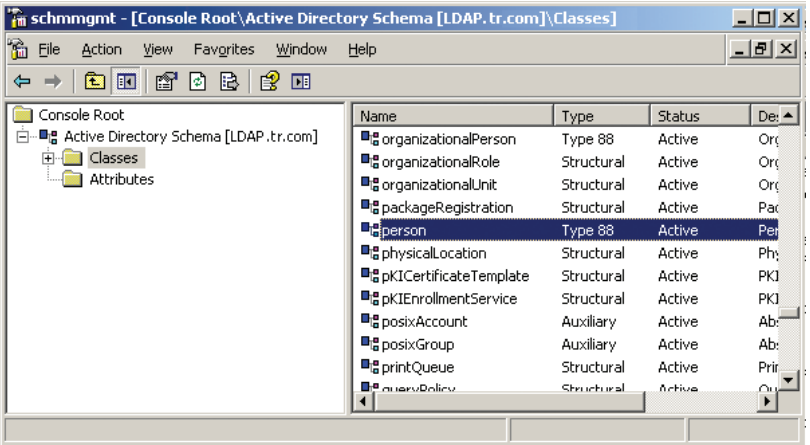
☑ Attribute is active
☐ Index this attribute
☐ Ambiguous Name Resolution (ANR)
☐ Replicate this attribute to the Global Catalog
☐ Attribute is copied when duplicating a user
☐ Index this attribute for containerized searches

Step 2 - Extend the Object Class With the New Attribute:

a) **Open Control Panel** ⟶ **Administrative Tools** ⟶ **Active Directory Schema**.

b) In the left panel of the screen that comes up, select *Classes*.

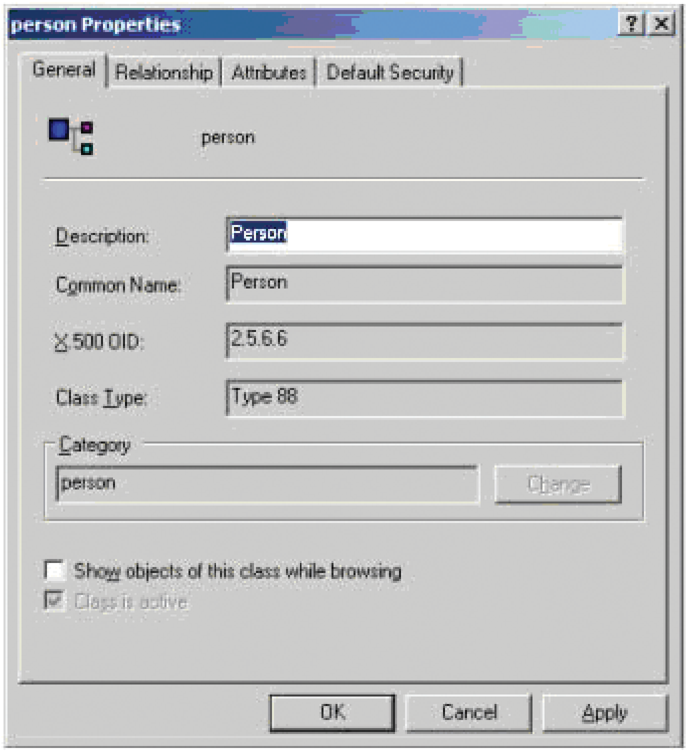
c) In the right panel, right-click *person*:


schmmgmt - [Console Root\Active Directory Schema [LDAP.tr.com]\Classes]
File
Action
View
Favorites
Window
Help

Console Root
- Active Directory Schema [LDAP.tr.com]
  - Classes
  - Attributes

Name	Type	Status	Des
organizationalPerson	Type 88	Active	Or
organizationalRole	Structural	Active	Or
organizationalUnit	Structural	Active	Or
packageRegistration	Structural	Active	Pac
person	Type 88	Active	Per
physicalLocation	Structural	Active	Phy
pKICertificateTemplate	Structural	Active	PKI
pKIEnrollmentService	Structural	Active	PKI
posixAccount	Auxiliary	Active	Ab:
posixGroup	Auxiliary	Active	Ab:
printQueue	Structural	Active	Prir
queryPolicy	Structural	Active	Qu

d) Select *Properties*. The person's *Properties* page comes up with the *General* tab displayed. Click the *Attributes* tab.



person

Description: Person

Common Name: Person

X.500 OID: 2.5.6.6

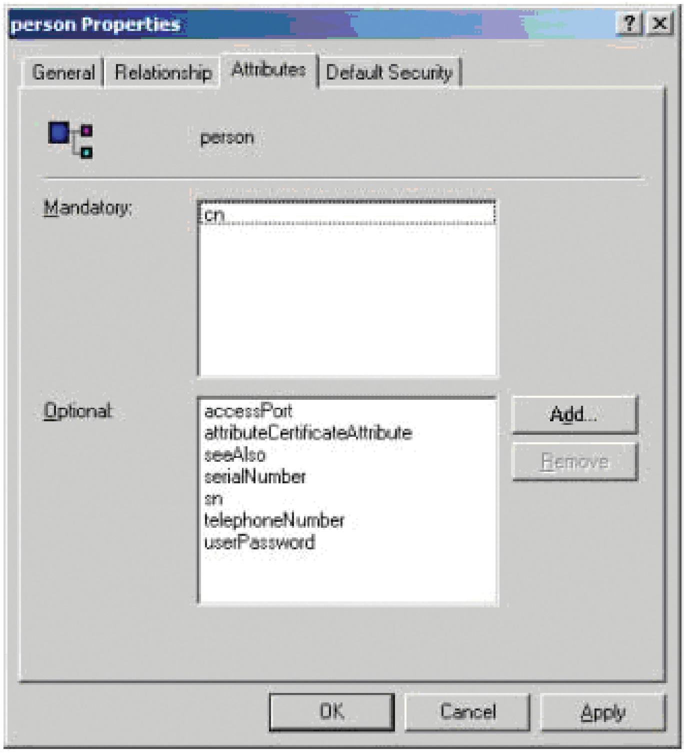
Class Type: Type 88

Category: person

☐ Show objects of this class while browsing

☑ Class is active

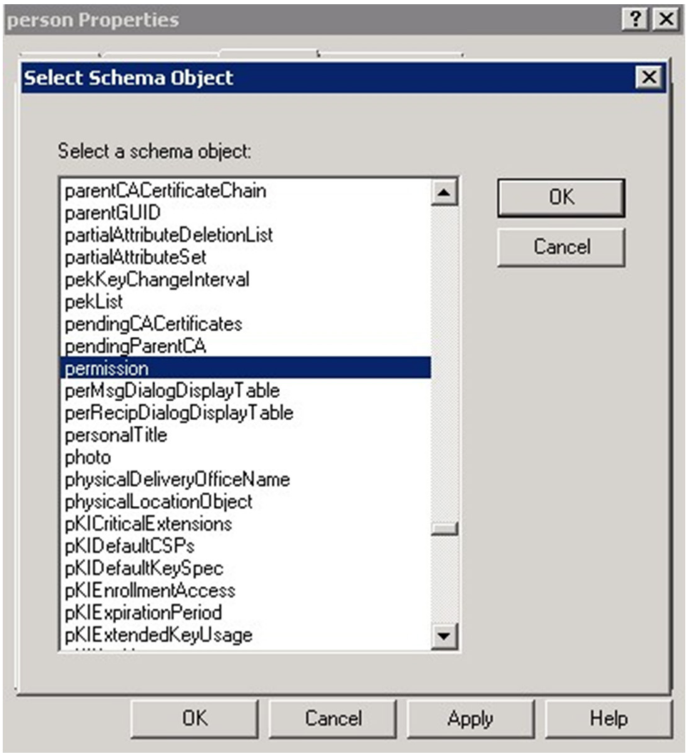
e) Select the *Attributes* tab and click the *Add* button:



Mandatory: cn

Optional:
accessPort
attributeCertificateAttribute
seeAlso
serialNumber
sn
telephoneNumber
userPassword

f) In the list that comes up, select ***permission***, then click *OK* to complete step 2 of the procedure.



Select a schema object:

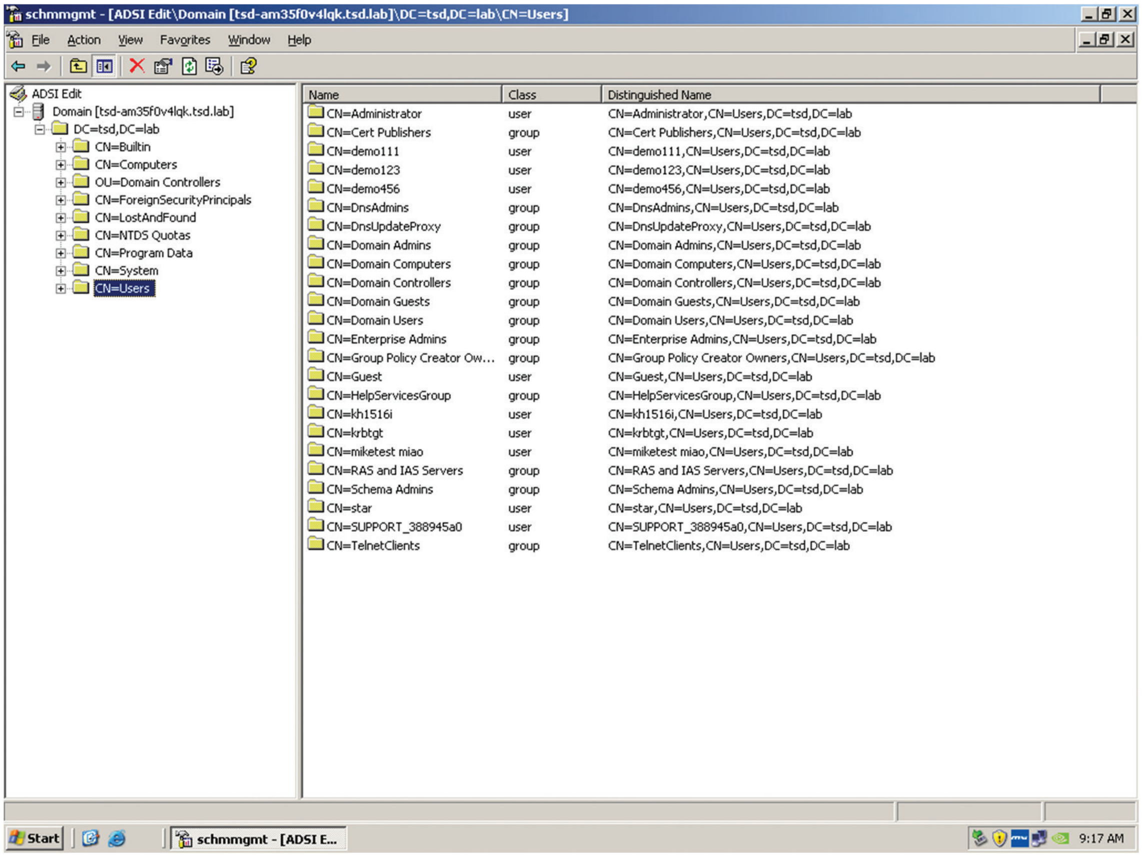
parentCACertificateChain
parentGUID
partialAttributeDeletionList
partialAttributeSet
pekKeyChangeInterval
pekList
pendingCACertificates
pendingParentCA
permission
perMsgDialogDisplayTable
perRecipDialogDisplayTable
personalTitle
photo
physicalDeliveryOfficeName
physicalLocationObject
pKICriticalExtensions
pKIDefaultCSPs
pKIDefaultKeySpec
pKIEnrollmentAccess
pKIExpirationPeriod
pKIExtendedKeyUsage

Step 3 - Edit Active Directory Users With the Extended Schema:

a) Run **ADSI Edit**. (Installed as part of the *Support Tools*.)

b) Open *Domain*, and navigate to the *cn=users dc=tripplite dc=com* node.

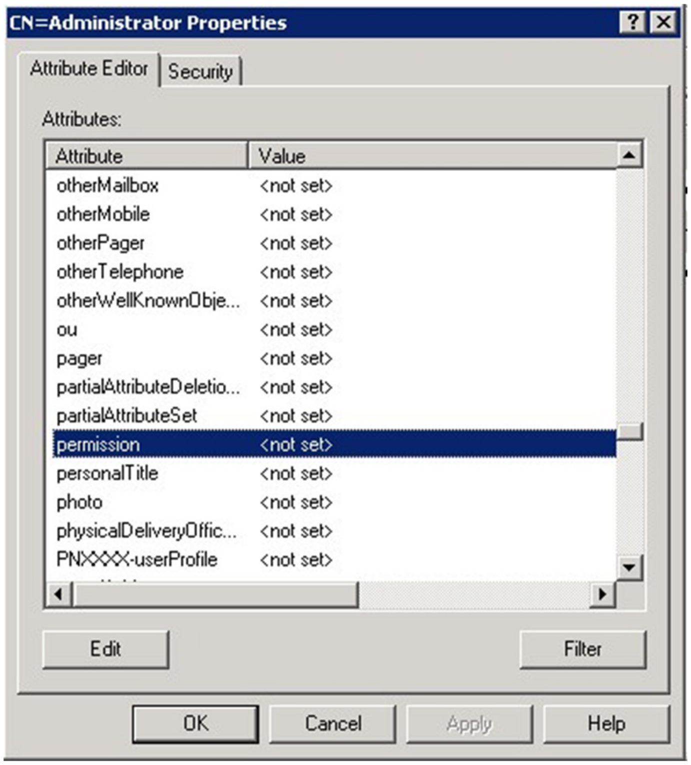
c) Locate the user you wish to edit.



Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=tsd,DC=lab
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=tsd,DC=lab
CN=demo111	user	CN=demo111,CN=Users,DC=tsd,DC=lab
CN=demo123	user	CN=demo123,CN=Users,DC=tsd,DC=lab
CN=demo456	user	CN=demo456,CN=Users,DC=tsd,DC=lab
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=tsd,DC=lab
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=tsd,DC=lab
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=tsd,DC=lab
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=tsd,DC=lab
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=tsd,DC=lab
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=tsd,DC=lab
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=tsd,DC=lab
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=tsd,DC=lab
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=tsd,DC=lab
CN=Guest	user	CN=Guest,CN=Users,DC=tsd,DC=lab
CN=HelpServicesGroup	group	CN=HelpServicesGroup,CN=Users,DC=tsd,DC=lab
CN=kh1516i	user	CN=kh1516i,CN=Users,DC=tsd,DC=lab
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=tsd,DC=lab
CN=miketest miao	user	CN=miketest miao,CN=Users,DC=tsd,DC=lab
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=tsd,DC=lab
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=tsd,DC=lab
CN=star	user	CN=star,CN=Users,DC=tsd,DC=lab
CN=SUPPORT_388945a0	user	CN=SUPPORT_388945a0,CN=Users,DC=tsd,DC=lab
CN=TelnetClients	group	CN=TelnetClients,CN=Users,DC=tsd,DC=lab

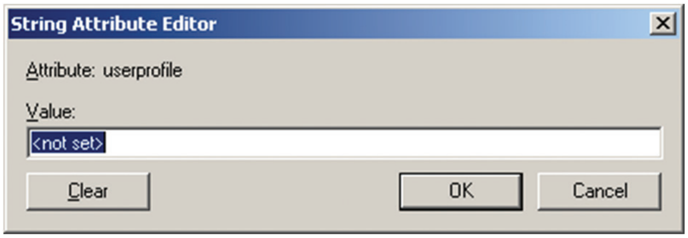
d) Right-click on the user's name and select *Properties***.**

e) On the *Attribute Editor* page of the dialog box that appears, select ***permission*** from the list.



Attribute	Value
otherMailbox	<not set>
otherMobile	<not set>
otherPager	<not set>
otherTelephone	<not set>
otherWellKnownObje...	<not set>
ou	<not set>
pager	<not set>
partialAttributeDeletio...	<not set>
partialAttributeSet	<not set>
permission	<not set>
personalTitle	<not set>
photo	<not set>
physicalDeliveryOffic...	<not set>
PNXXXX-userProfile	<not set>

f) Click *Edit* to bring up the *String Attribute Editor*:

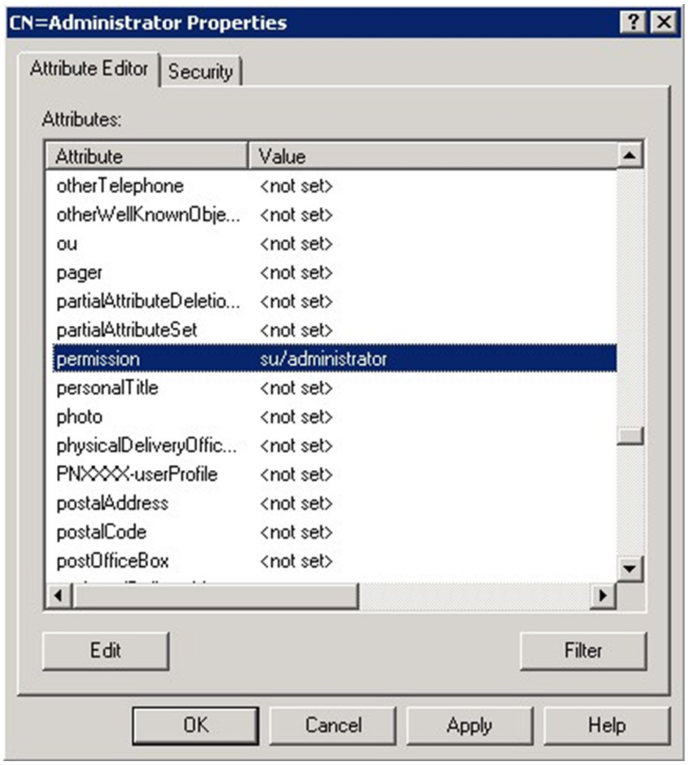


Attribute: userprofile

Value: <not set>

g) In this field, replace the value shown with the desired access rights (e.g. c, w, j, l). (See the access rights table in the RADIUS Settings section for details) You can also replace the value shown with su/xxxx, where xxxx represents the username assigned to the user in the B051-000. In this case, user access rights will be the same as those that were assigned to them in the B051-000. (See the User Management section for details)

h) Click *OK*. When you return to the *Attribute Editor* page, the ***permission*** entry now reflects the new permissions:



Attributes:

Attribute	Value
otherTelephone	<not set>
otherWellKnownObje...	<not set>
ou	<not set>
pager	<not set>
partialAttributeDeletio...	<not set>
partialAttributeSet	<not set>
permission	su/administrator
personalTitle	<not set>
photo	<not set>
physicalDeliveryOffic...	<not set>
PNXXXX-userProfile	<not set>
postalAddress	<not set>
postalCode	<not set>
postOfficeBox	<not set>

i) Click *Apply* to save the change and complete the procedure.

j) Repeat Step 3 (*Edit Active Directory Users With the Extended Schema*) for any other users you wish to add.

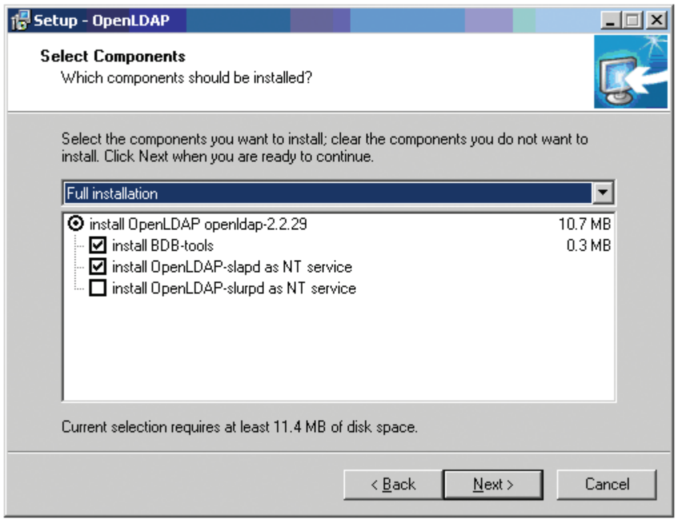
OpenLDAP Server

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-0.9.8awin32 _ 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*, as shown in the diagram below:



Setup - OpenLDAP

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

○ install OpenLDAP openldap-2.2.29	10.7 MB
☑ install BDB-tools	0.3 MB
☑ install OpenLDAP-slapd as NT service	
□ install OpenLDAP-slurpd as NT service	

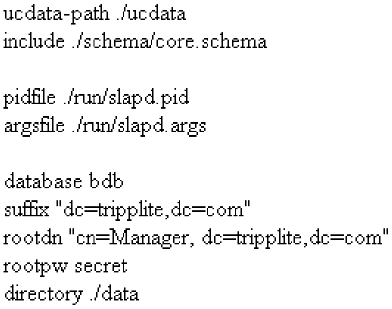
Current selection requires at least 11.4 MB of disk space.

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* startup 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 in the figure below:

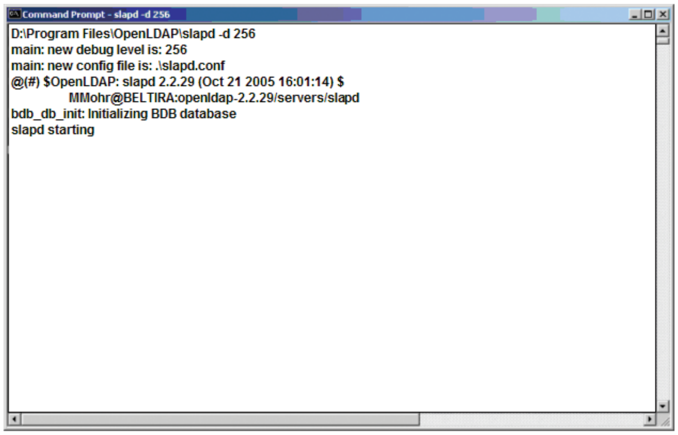


```
ucdata-path ./ucdata
include ./schema/core.schema

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:

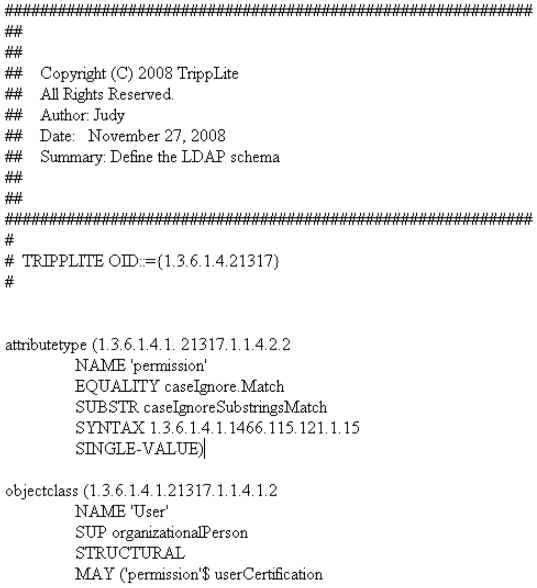
Note: For details about **slapd** *options and their meanings, refer to the OpenLDAP documentation.*



```
D:\Program Files\OpenLDAP\slapd -d 256
main: new debug level is: 256
main: new config file is: .\slapd.conf
@(#) $OpenLDAP: slapd 2.2.29 (Oct 21 2005 16:01:14) $
            MMohr@BELTIRA:openldap-2.2.29/servers/slapd
bdb_db_init: Initializing BDB database
slapd starting
```

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 B051-000, the B051-000 *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 B051-000 is shown in the figure below:

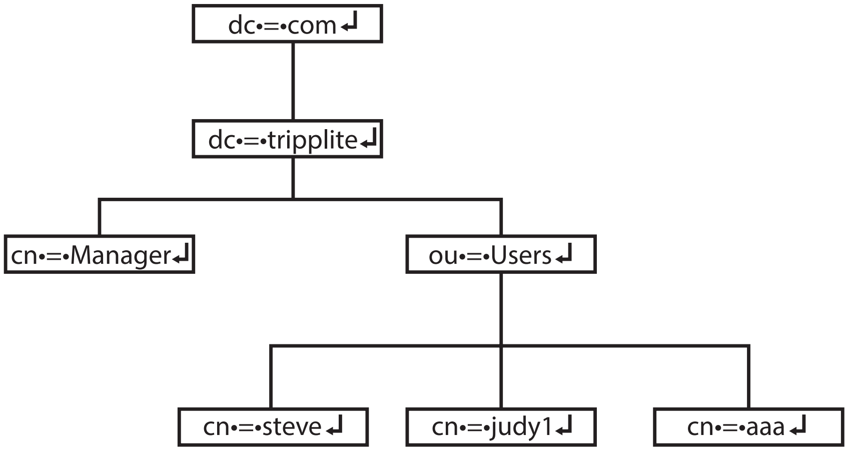


```
############################################################
##
##
##    Copyright (C) 2008 TrippLite
##    All Rights Reserved.
##    Author: Judy
##    Date:   November 27, 2008
##    Summary: Define the LDAP schema
##
##
############################################################
#
#  TRIPPLITE OID::={1.3.6.1.4.21317}
#


attributetype (1.3.6.1.4.1. 21317.1.1.4.2.2
              NAME 'permission'
              EQUALITY caseIgnore.Match
              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'$ userCertification
```

LDAP DIT Design and LDIF File

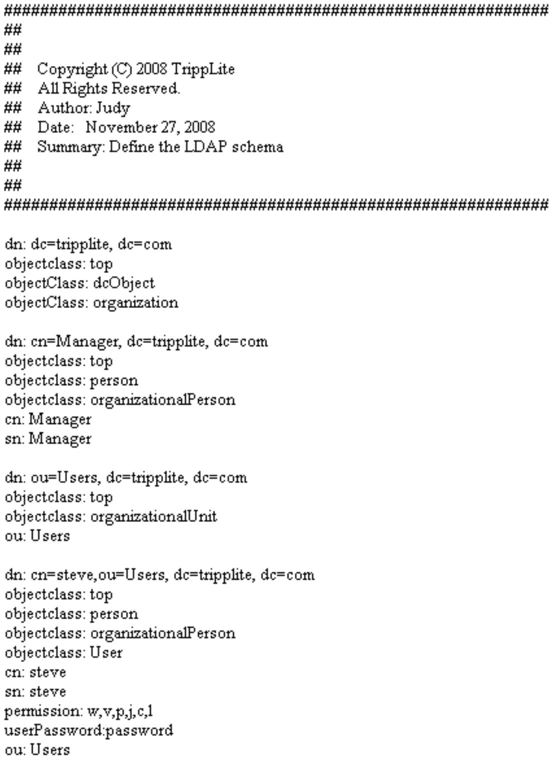
LDAP Data Structure

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 for the B051-000 is shown in the figure below:



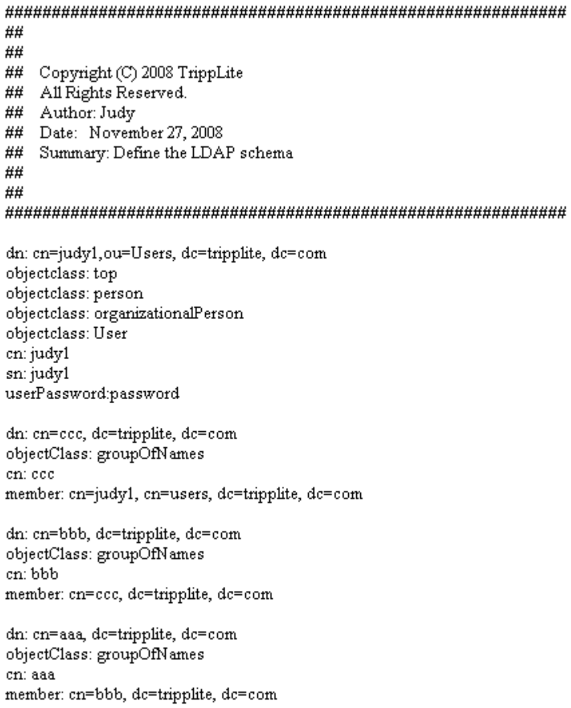
DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the B051-000 directory tree (shown in the figure in the previous section).



```
##################################################################
##
##
##    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,j,c,l
userPassword:password
ou: Users
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the B051-000.

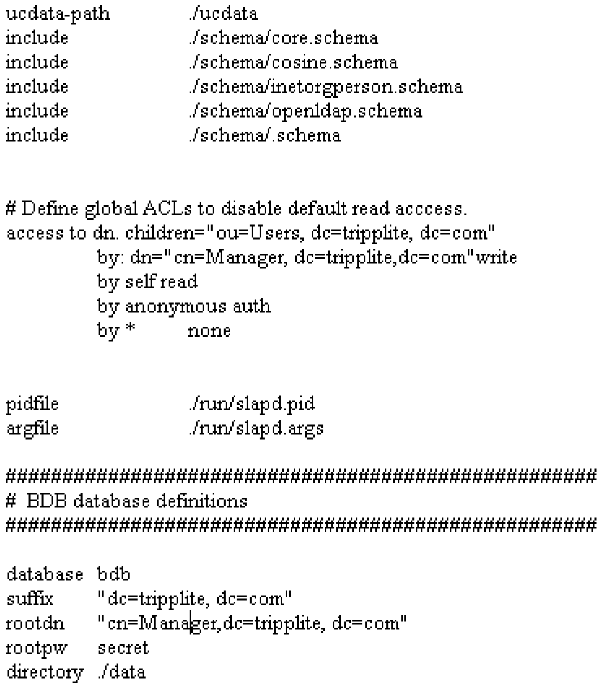


```
##################################################################
##
##
##    Copyright (C) 2008 TrippLite
##    All Rights Reserved.
##    Author: Judy
##    Date:   November 27, 2008
##    Summary: Define the LDAP schema
##
##
##################################################################

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
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., B051-000.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 acccess.
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

Security

The following pages describe the sections found in the *Security* page.

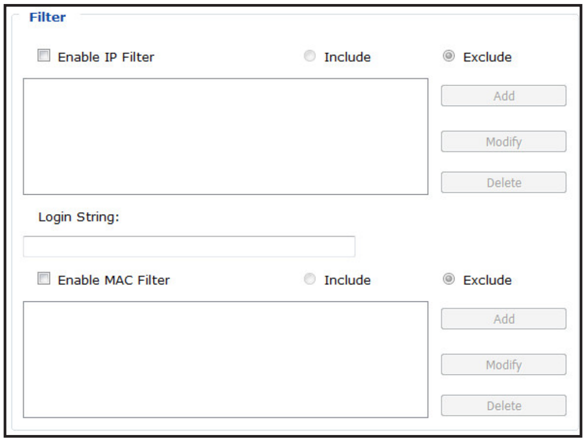
User Station Filters

IP and MAC filters provide a way for you to control access to the B051-000 based on the IP address and/or MAC address of the computer being used to access it. To enable IP and/or MAC filtering, click the *IP Filter Enable* and/or *MAC Filter Enable* checkbox. There are a maximum of 100 filters allowed for each. ***Note**: You can only filter by IPv4 address.*

- If the *Include* checkbox is checked, all the addresses within the filter range are allowed access to the unit; all other addresses are denied access.
- If the *Exclude* checkbox is checked, all the addresses within the filter range are denied access to the unit; all other addresses are allowed access.

To add an IP filter:

1. Check the *IP Filter Enable* checkbox.
2. Click *Add*. A dialog box similar to the one below appears.



3. To filter a single IP address, enter the same address into the *From* and *To* fields. To filter a range of IP addresses, enter the starting IP address in the *From* field, and the ending IP address in the *To* field.
4. After entering the addresses, click *OK*. The IP filter will appear in the IP filter list.
5. Click the *Apply* button at the bottom of the page to save your changes.
6. Repeat these steps for any additional IP addresses you want to filter.

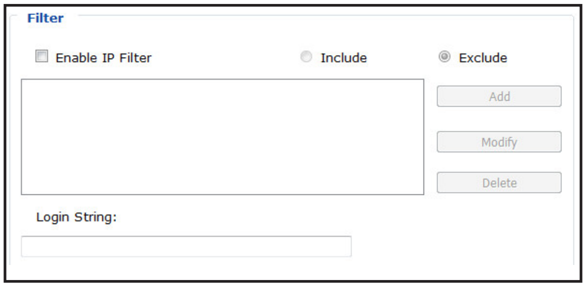
To delete an IP filter:

1. Select the desired IP filter from the IP filter list and click *Remove*.
2. Click the *Apply* button at the bottom of the page to save your changes.

To modify an IP filter:

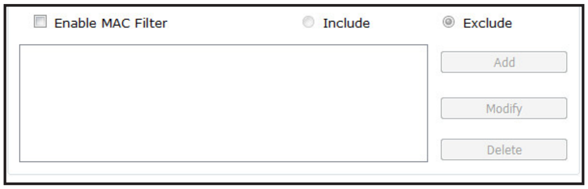
1. Select the desired IP filter from the list and click *Edit*. An *Edit* dialog box similar to the *Add* dialog box will appear.
2. Delete the IP address in the *From* field and replace it with the new one.
3. Delete the IP address in the *To* field and replace it with the new one. Click *OK*.
4. Click the *Apply* button at the bottom of the page to save your changes.

***Note**: To block a computer from accessing the unit, you do not need to filter both its IP address and MAC address. A computer that is blocked by one filter will be denied access to the unit even if it is allowed under the other.*



To add a MAC filter:

1. Click *Add*. A dialog box similar to the one below appears.



2. Type in the desired MAC address and click *OK*.
3. Click the *Apply* button at the bottom of the page to save your changes.
4. Repeat these steps for any additional MAC addresses you want to filter.

To delete a MAC filter:

1. Select the desired MAC filter from the list and click *Remove*.
2. Click the *Apply* button at the bottom of the page to save your changes.

To modify a MAC filter:

1. Select the desired MAC filter from the list and click *Edit*. An *Edit* dialog box similar to the *Add* dialog box will appear.
2. Delete the old address and replace it with the new one. Click *OK*.
3. Click the *Apply* button at the bottom of the page to save your changes.

***Note**: To block a computer from accessing the unit, you do not need to filter both its IP address and MAC address. A computer that is blocked by one filter will be denied access to the unit even if it is allowed under the other.*

Login String

The *Login String* allows the IP address assigned to the B051-000 to be more secure by adding extra text to the end of it. When text is entered into the *Login String* field, users will need to include a forward slash (/) and the Login String at the end of the URL to access the unit. For example, if a Login String of abcdefg is entered, the user must enter a URL such as 192.168.0.126/abcdefg. Upon entering the desired login string, click the *Apply* button at the bottom of the page to save your changes.

The following characters are allowed in the login string:

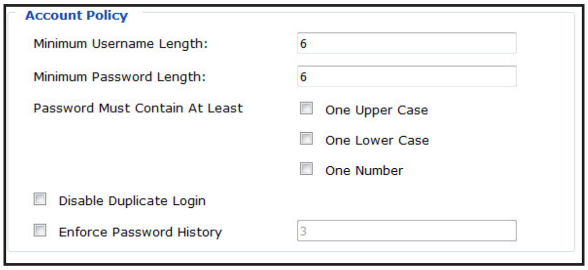
- 0–9, a–z, A–Z, ~ ! @ $ ^ & * ( ) _ + - = [ ] { } ; ’ < > , . |

The following characters are not allowed:

- % ” : / ? # \ [Space]
- Compound characters (Ẻ, Ç etc.)

***Note**: If a Login String is not entered, anyone can access the* B051-000 *using the IP Address alone, which makes the installation less secure.*

Account Policy



Account Policy

Minimum Username Length: 6

Minimum Password Length: 6

Password Must Contain At Least

□ One Upper Case

□ One Lower Case

□ One Number

□ Disable Duplicate Login

□ Enforce Password History 3

The *Account Policy* section allows rules for usernames and passwords to be regulated. The settings in this section are described in the table below.

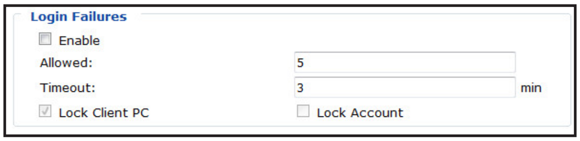
Field	Description
Minimum Username Length	Sets the minimum number of characters required for each username. Values from 1 to 16 can be entered. The default value is 6.
Minimum Password Length	Sets the minimum number of characters required for each password. Values can be from 0 to 16. A setting of 0 means that a password is not required, and users can login with only their username. The default value is 6.
Password Must Contain at Least	**One Upper Case** – Checking this box will require that each password contain one upper case letter **One Lower Case** – Checking this box will require that each password contain one lower case letter **One Number** – Checking this box will require that each password contain one number ***Note:*** *Current usernames and passwords are not affected when these settings are changed. Only usernames and passwords that are created after these settings have been changed must follow the rules.*
Disable Duplicate Login	Checking this box will prevent users from logging in with the same username and password to open more than one session at the same time.
Enforce Password History	Check this box, and enter the number of times a unique password must be created before an old password can be reused. The number represents the number of passwords the system will remember to enforce password history.

When you have finished editing the *Account Policy* settings, click the *Apply* button at the bottom of the page to save your changes.

Login Failures

The *Login Failures* section allows you to set up the parameters for what occurs when an account fails to log in successfully. To enable the settings entered here, check the *Enable* checkbox. The table below describes the settings found in this section.

Note*: When the Login Failures settings are disabled, there is no restriction on the number of login failures. It is strongly recommended that you enable these features, and that both the* Lock Client PC *and* Lock Account *settings are enabled.*



Login Failures

□ Enable

Allowed: 5

Timeout: 3 min

☑ Lock Client PC

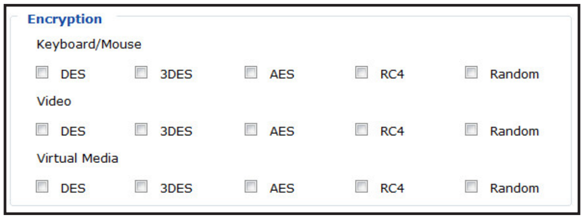
□ Lock Account

Field	Description
Allowed	Determines the number of failed login attempts an account gets before they are prevented from accessing the unit. The default value is 5.
Timeout	Determines the amount of time that the user is prevented from accessing the unit after exceeding the maximum number of failed login attempts. The default value is 3 minutes.
Lock Client PC	When this checkbox is checked, the computer used to unsuccessfully access the unit will be locked out after exceeding the maximum number of failed login attempts. This setting is enabled by default. ***Note:*** *This feature blocks the computer using its IP address. If the computer IP address is changed, it will be able to access the KVM in spite of this setting.*
Lock Account	When this checkbox is checked, the account used to unsuccessfully access the KVM will be locked out after exceeding the maximum number of failed login attempts. This setting is enabled by default.

When you have finished editing the *Login Failures* settings, click the *Apply* button at the bottom of the page to save your changes.

Encryption

This section allows you to set different encryption settings for the *Keyboard/Mouse, Video* and *Virtual Media* functions of the B051-000. You can choose any combination of encryption methods (DES, 3DES, AES and/or RC4), you can choose to randomly switch between them or you can choose no encryption at all. Although enabling encryption will add more security to your installation, it can also slow down system performance (mouse, keyboard, video), with the following having the most impact:



Encryption

Keyboard/Mouse

□ DES □ 3DES □ AES □ RC4 □ Random

Video

□ DES □ 3DES □ AES □ RC4 □ Random

Virtual Media

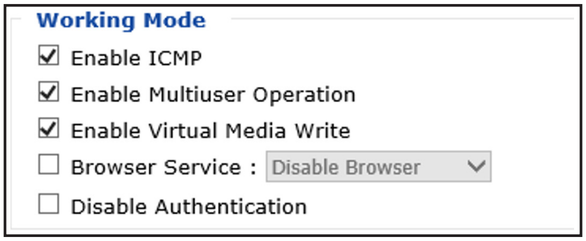
□ DES □ 3DES □ AES □ RC4 □ Random

- RC4 impacts performance the least out of the four encryption methods. DES is second to least in impact, followed by 3DES and AES.
- Of all the possible combinations, a combination of RC4 and DES impacts performance the least.

When you have finished editing the *Encryption* settings, click the *Apply* button at the bottom of the page to save your changes.

Working Mode

Use this section to set the working mode parameters.



Working Mode

☑ Enable ICMP

☑ Enable Multiuser Operation

☑ Enable Virtual Media Write

□ Browser Service : Disable Browser

□ Disable Authentication

- **Enable ICMP**—Enables the B051-000 to be pinged. If this checkbox is not checked, the unit cannot be pinged. The default is Enabled.
- **Enable Multiuser Operation**—Permits more than one user to log into the B051-000 at the same time. The default is Enabled.
- **Enable Virtual Media Write**—Allows redirected virtual media devices on a user's system to send data to a remote server, as well as being able to have data from the remote server written to them. The default is Enabled.
- **Browser Service**—Allows the administrator to limit the scope of browser access to the B051-000. Check the checkbox to enable this function, then select the browser limitation in the drop-down box. Choices are explained in the following table:

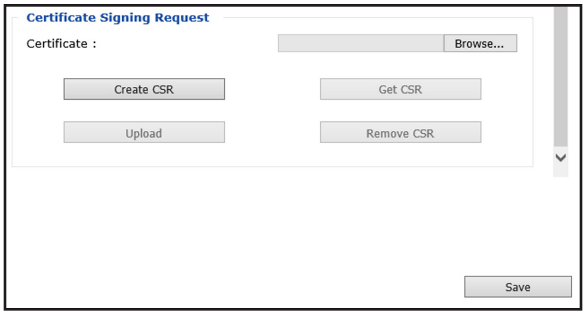
Item	Explanation
Disable Browser	The B051-000 cannot be accessed via browser, but only from non-browser clients.
Disable HTTP	The B051-000 can be accessed via browser, but not an ordinary HTTP login connection—only over a secure HTTPS (SSL) connection.
Disable HTTPS (SSL)	The B051-000 can be accessed via browser over an ordinary HTTP login connection, but not via a secure HTTPS (SSL) connection.

- **Disable Authentication**—No authentication procedures are used to check users attempting to log in. Users gain Administrator access simply by entering a user name and password.

  Note: *Enabling this setting creates a dangerous security breach and should only be used under very special circumstances.*

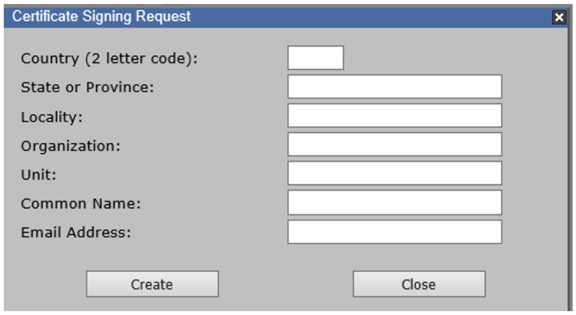
Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.



To perform this operation, do the following:

1. Click *Create CSR*. The following dialog box appears:



2. Fill in the form using entries valid for your site. All fields are required. See the examples in the table below:

Information	Example
Country (2-Letter Code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	www.mycompany.com (This must be the exact domain name of the site for which you want the certificate to be valid. If the site's domain name is www.mycompany.com and you specify only mycompany.com, the certificate will not be valid.)
Email Address	administrator@mycompany.com

3) Click *Create*. A self-signed certificate based on the information you provided is now stored on the B051-000.

4) Click *Get CSR*. Save the certificate file (*csr.cer*) to your computer. This is the file you give to the third-party CA to apply for their signed SSL certificate.

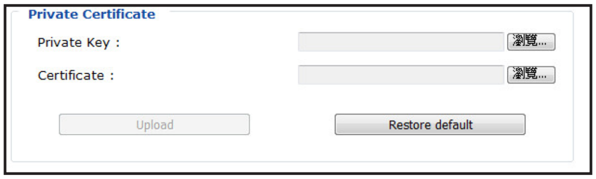
5) After the CA sends you the certificate, save it to your computer. Click *Browse* to locate the file, and click *Upload* to store it on the B051-000.

   Note: *When you upload the file, the B051-000 checks it to make sure the specified information matches. If it does, the file is accepted. If it does not, the file is rejected.*

6) To remove the certificate or replace it with a new one (because of a domain name change, for instance), click *Remove CSR*.

Private Certificate

When logging into the KVM switch over a secure (SSL) connection, a certificate is required to ensure you are logging into a secure site. If a certificate is not recognized as secure, you will be prompted each time you log in to verify you want to continue to the website. This section allows you to import an Encryption Key and Certificate. To import an *Encryption Key* and *Certificate*, follow the steps below.



Private Certificate

Private Key :

Certificate :

1. Click the *Browse* button to the right of the *Private Key* field, browse to where your private encryption key file is located, and then select it.
2. Click the *Browse* button to the right of the *Certificate* field, browse to where your certificate file is located, and then select it.
3. Click the *Upload* button to complete the procedure.

   Note*: Both the Private Key and Certificate must be imported at the same time. Clicking the Restore Default button returns the KVM to the default certificate that came installed on it.*

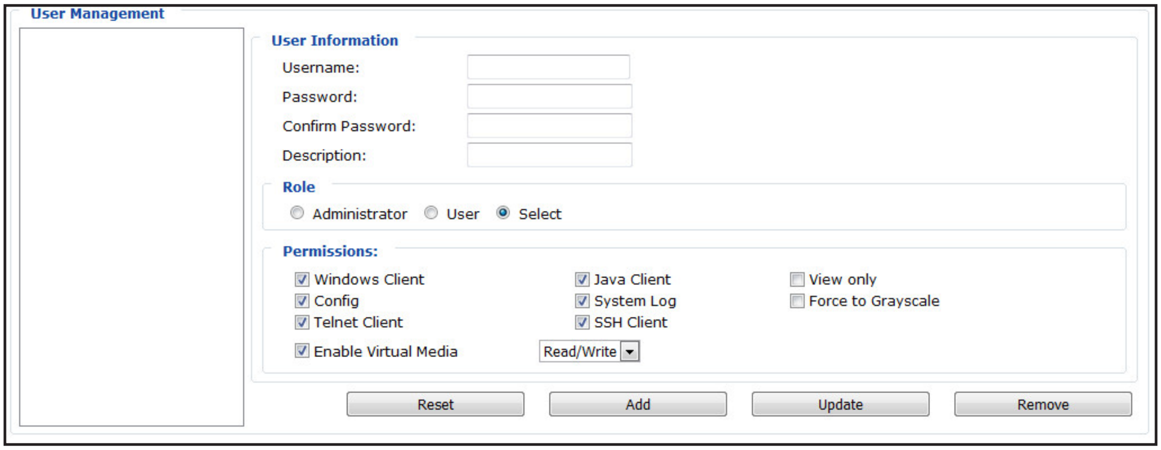
4. Click the *Apply* button at the bottom of the page to save your changes.

User Management

The *User Management* page allows Administrators and Select accounts who have been given *Configure* permission (see the following section for details) to add/edit accounts on the B051-000. If an account has not been given *Configure* permission, they will not be able to access it when they log in.

Adding an Account

There is a default Administrator account on the B051-000 that can be used for setting up the unit. The default Administrator username is *administrator*, and the default password is *password*. It is strongly recommended that you update the default account's username and password to something unique. To add a new account, follow the steps below.



User Management

User Information

Username:

Password:

Confirm Password:

Description:

Role

○ Administrator ○ User ● Select

Permissions:

☑ Windows Client ☑ Java Client □ View only
☑ Config ☑ System Log □ Force to Grayscale
☑ Telnet Client ☑ SSH Client

☑ Enable Virtual Media Read/Write

1. Upon entering the *User Management* page, the fields on the right will be blank. Enter the appropriate information for the account you are creating. Clicking the *Reset* button will clear all of the settings on the right side of the page. (The contents of the user information screen and their meanings are described in the table below.)

Setting	Description
Username	Enter a username for the account here. The username can contain up to 16 characters, and must meet the *Account Policy* requirements set in the *Security* page. (See *Account Policy* section for details.)
Password	Enter a password for the account here. The password can contain up to 16 characters, and must meet the *Account Policy* requirements set in the *Security* page. (See *Account Policy* section for details.)
Confirm Password	For security purposes you must re-enter the password. If the password does not match the password you just entered in the previous field, you will not be allowed to save the account information.
Description	Enter any additional information that you want to describe the account. This is an optional field.
Admin / User / Select	Select the type of account that you will be creating; *Administrator, User* or *Select*. There is no limitation on the number of each type of account that can be created, only a limit on the number of total accounts. You can create up to 64 accounts on the B051-000. • **Administrator** – This account type has full access to the unit. They can fully access the computer/KVM and serial devices connected to the B051-000, change any and all settings, and add/edit any account type. • **User** – This account type has limited permissions, which consist of access to the unit via either the Windows or Java clients and access to the unit's power management functionality. • **Select** – This account type gives *Administrators* the ability to customize the permissions granted to the account. Any combination of permissions can be granted by checking the checkbox of the corresponding permission.
Permissions	The permission settings in this section of the user information page determine what functionality the account is able to use. Check the checkbox next to the permission to enable it for the account. Leave it unchecked to deny the account access to that functionality. • **Windows Client** – Gives the account access to the browser and non-browser versions of the Windows client. • **Java Client** – Gives the account access to the browser and non-browser versions of the Java client. • **View Only** – Limits the account to viewing the video of the connected computer/KVM only. They will not be able to perform keyboard and mouse functions. • **Configure** – Gives the account access to all of the settings in the Admin utility, allowing them to set up and modify the unit's operating environment and create/edit user accounts. • **Log** – Gives the account access to the *Log* page in the web browser Admin Utility, where they can view events that have taken place on the installation. (See the *Log* section in this manual for details.) If this checkbox is not checked, the *Log* icon will not appear when the account logs into the unit. • **Enable Telnet/SSH** – Allows the account access to the connected serial device(s) via a telnet/SSH client. When checked, choose from the drop-down list whether to give the account telnet access, SSH access, or both. ***Note**: The telnet and SSH links will not appear on the web browser* Remote Console *page unless* Serial Console *or* 2-Wire RS-232 Serial Console *management is enabled in the* Console Management *page. (See the* Console Management *section in this manual for details)* • **Enable Virtual Media** – Allows the account to access the unit's virtual media functionality. When checked, choose from the drop-down list whether the account will have *Read Only* or *Read/Write* access to virtual media.

2. When you are finished with your changes, click the *Add* button to add the new account to the list on the left side of the page. Click the *Apply* button at the bottom of the page to save the new account.

Modifying an Account

To modify an existing account, do the following:

1. Select the desired account from the list on the left side of the *User Management* page. Upon selection, the account information will be displayed on the right side of the page.
2. As when creating an account, make any necessary changes.
3. When you are finished with your changes, click the *Update* button to update the selected account. Click the *Apply* button at the bottom of the page to save the modified account information.

Deleting an Account

To delete an existing account, do the following:

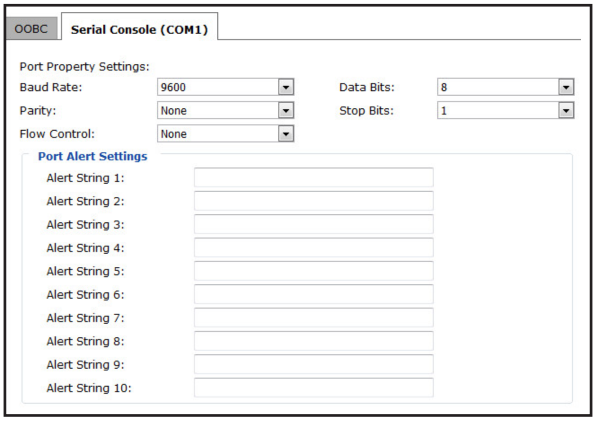
1. Select the desired account from the list on the left side of the *User Management* page. Upon selection, the account information will be displayed on the right side of the page.
2. Click the *Remove* button to remove the account from the list. Click the *Apply* button to save the changes and delete the account.

Console Management

The *Console Management* page allows *Administrators* and *Select* accounts that have been given permission to set the RS-232 Serial Port to be used as a *Serial Console* or *OOBC (Out of Band Connection)*, and to customize its settings accordingly.

Serial Console

To set the RS-232 Serial port for use with a serial device, check the *Serial Console* tab at the top of the page. When checked, the following page is displayed.



Port Property Settings:

Baud Rate: 9600
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None

Port Alert Settings

Alert String 1:
Alert String 2:
Alert String 3:
Alert String 4:
Alert String 5:
Alert String 6:
Alert String 7:
Alert String 8:
Alert String 9:
Alert String 10:

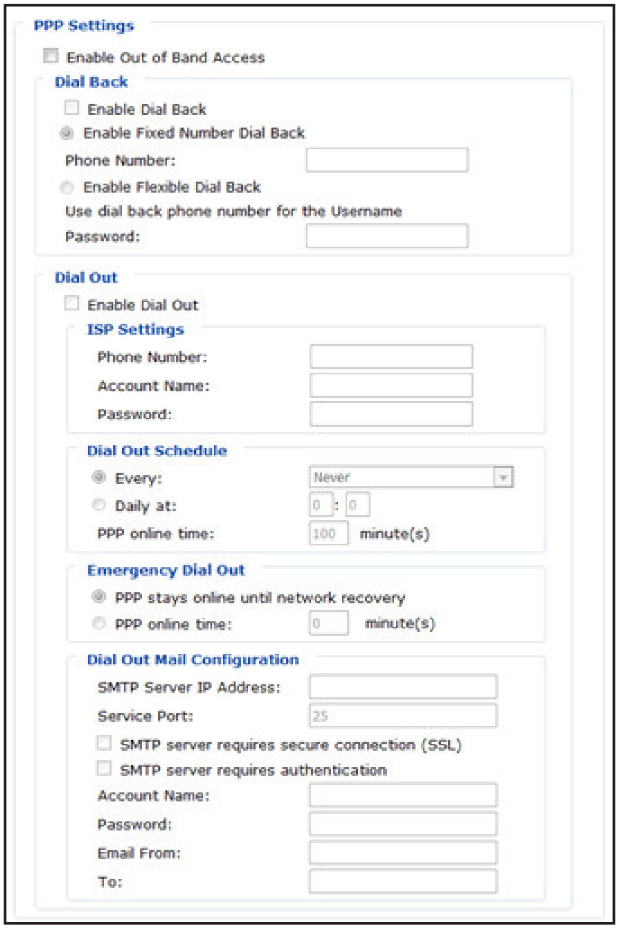
Setting	Description
Baud Rate	Sets the port's data transfer speed to match that of the connected device. The drop-down list provides settings from 300 to 115200, with the default being 9600. Select the baud rate that matches your device.
Data Bits	Sets the number of bits used to transmit one character of information. The drop-down list provides bit settings of 5, 6, 7 and 8, with the default being 8. Select the data bits setting that matches your device.
Parity	This bit checks the integrity of the transmitted data. The drop-down list provides the following options: *None, Odd, Even, Mark* and *Space*, with the default being *None*. Select the option that matches your device.
Stop Bits	Indicates a character has been transmitted. The drop-down list provides settings of 1 and 2, with the default being 1. Select the setting that matches your device.
Flow Control	Allows you to choose how the data flow will be controlled. The drop-down list provides the following options: *None, Hardware (RTS/CTS)*, and *XON/XOFF*, with the default being *None*. Select the flow control setting that matches that of your device.
Alert String	The *Alert String* fields allow you to enter events that you will be informed about as they occur on the connected device. (e.g. Power On, Power Off, etc.)

When you have finished editing the *Serial Console* settings, click the *Save* button at the bottom of the page to save your changes.

OOBC

In case the B051-000 cannot be accessed via the LAN, it can be accessed with an external modem via the switch's RS-232 serial port. To enable support for PPP (modem) operation, check the *Enable Out of Band Access* checkbox. When checked, the settings fields become active for you to customize.

***Note**: Enabling out of band access automatically enables* Dial In *operation. For the modem session, the B051-000 has an IP address of 192.168.192.1, and the user side has an IP address of 192.168.192.101.*



PPP Settings

□ Enable Out of Band Access

Dial Back

□ Enable Dial Back

● Enable Fixed Number Dial Back

Phone Number:

○ Enable Flexible Dial Back

Use dial back phone number for the Username

Password:

Dial Out

□ Enable Dial Out

ISP Settings

Phone Number:

Account Name:

Password:

Dial Out Schedule

● Every: Never

○ Daily at: 0 : 0

PPP online time: 100 minute(s)

Emergency Dial Out

● PPP stays online until network recovery

○ PPP online time: 0 minute(s)

Dial Out Mail Configuration

SMTP Server IP Address:

Service Port: 25

□ SMTP server requires secure connection (SSL)

□ SMTP server requires authentication

Account Name:

Password:

Email From:

To:

Enable Dial Back

If the *Enable Dial Back* checkbox is checked, the switch will disconnect calls that dial into it, and dial back to one of the entries specified in the table below.

- **Enable Fixed Number Dial Back** – When the *Enable Fixed Number Dial Back* checkbox is checked, the B051-000 will hang up on the modem when there is an incoming call, and dial back to the modem represented by the phone number in the *Phone Number* field.
- **Enable Flexible Dial Back** – When the *Enable Flexible Dial Back* checkbox is checked, the B051-000 can dial back to any modem specified by the user. Simply enter a password into the *Password* field, and when a user connects to the B051-000's modem, they will be prompted to enter a username and password. They should enter the phone number of the modem that they want to dial back to as the username, and use the password that is set in the *Password* field as the password.

Enable Dial Out

To use the dial-out feature, you must establish an account with an Internet Service Provider (ISP), and use a modem to dial out to your ISP account. Check the *Enable Dial Out* checkbox to enable this feature. The settings found in this section are described in the table below.

Setting	Description
ISP Settings	Enter the *Phone Number, Account Name* and *Password* that you use to connect to your ISP here.
Dial Out Schedule	This section allows you to determine what times the B051-000 will dial out over your ISP connection. • **Every** – Check this option to choose between the 5 options in the drop-down menu: *Never, Every Hour, Every 2 Hours, Every 3 Hours* or *Every 4 Hours*. • **Daily at** – Check this option to enter a time that the B051-000 will dial out over your ISP every day. Use the hh:mm format to specify the desired time. • **PPP Online Time** – Enter the amount of time you want an ISP connection to last before it is terminated. A setting of 0 means that the ISP connection will not automatically disconnect itself.
Emergency Dial Out	In the event that the B051-000 gets disconnected from the network, or the network goes down, this feature will automatically connect via the ISP dial up connection. • **PPP Stays Online Until Network Recovery** – When this option is checked, the ISP connection will remain active until the network connection is reestablished. • **PPP Online Time** – When this option is checked, the ISP connection will remain active for the amount of time you set here. A setting of 0 means that the ISP connection will not automatically disconnect itself.
Dial Out Mail Configuration	This section allows you to set up email notifications of system events via an SMTP server. These notifications will be sent over the ISP network connection, as opposed to the notifications that are set up in the *ANMS* page (see the *SMTP Setting*s section of this manual for details), which go out over the standard network. • **SMTP Server IP Address** – Enter the IP address or domain name of your SMTP server here. • In the **Email From** field, key in the email address that you want the report to show up as being sent from. • In the **To** field, key in the email address(es) you want the report to be sent to. ***Note:*** *If you are entering more than one address, separate them with a semicolon.* • **SMTP server requires secure connection (SSL)** – Check this checkbox if your server requires a secure connection. • **SMTP Server Requires Authentication** – Check this checkbox if your server requires authentication. When checked, the *Account Name* and *Password* fields are activated. Enter in the *Account Name* and *Password* for your SMTP server.

When you have finished editing the *OOBC* settings, click the *Apply* button at the bottom of the page to save your changes.

PPP Modem Access

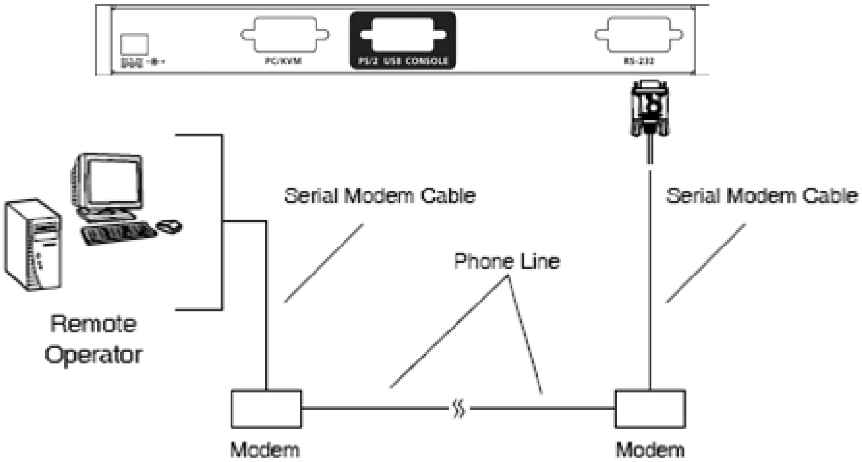
Follow the steps below to setup and access the B051-000 via dial-in modem.

Note*: For the modem session, the B051-000 has an IP address of 192.168.192.1, and the user side has an IP address of 192.168.192.101.*

1. Set up your hardware configuration to match the diagram below.
2. From your computer, use your modem terminal program to dial into the B051-000's modem.

   Note*: If you don't know the modem's serial parameters, get them from the system administrator. An example of setting up a modem terminal program under Windows XP is provided on the next page.*

3. Once the connection is established, open your browser, and specify 192.168.192.1 in the URL box. From here, operation is the same as if you had logged in from a browser or with the AP programs.



Connection Setup Example (Windows XP)

To set up a dial-in connection to the B051-000 under Windows XP, follow the steps below.

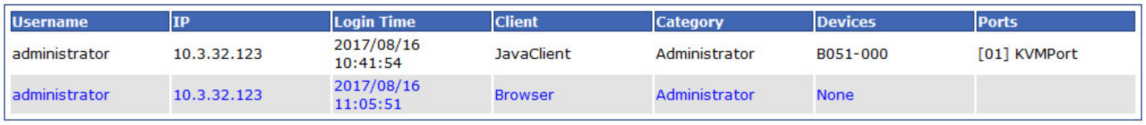
1. From the *Start* menu, select *Control Panel* → *Network Connections* → *Create a New Connection*.

2. When the *Welcome* to the *New Connection Wizard* dialog box appears, click *Next* to move on.
3. In the *Network Connection Type* dialog box, select *Connect to the network at my workplace* and click *Next*.
4. In the *Network Connection* dialog box, select *Dial-up* connection and click *Next*.
5. In the *Connection Name* dialog box, key in a name for the connection and click *Next*.
6. In the *Connection Availability* dialog box, you can select either *Anyone's use* or *My use* only, depending on your preferences, then click *Next*.

   ***Note**: If you are the only user on this computer, this dialog box won't appear.*
7. In the *Phone Number to dial* dialog box, key in the phone number of the modem connected to the B051-000 (be sure to include country and area codes, if necessary), then click *Next*.
8. In the *Completing the New Connection Wizard* dialog box, check *Add a shortcut to this connection on my desktop* and click *Finish*.
9. This completes the connection setup. Double-click the desktop shortcut icon to make a dial-in connection to the B051-000.

Sessions (Browser only)

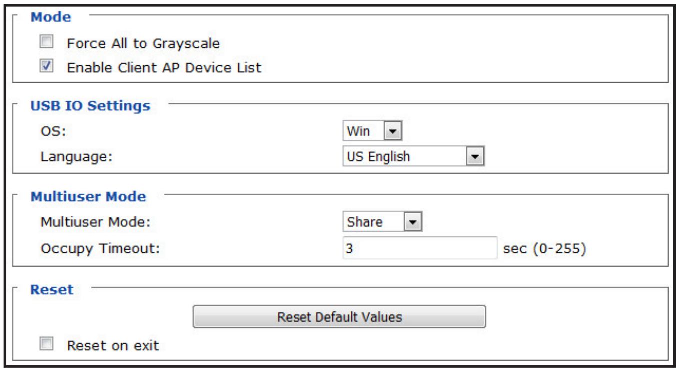
The *Sessions* page allows *Administrators*, and *Select* accounts who are given *Configure* permission (See the *User Management* section in this manual for details) to see who is logged into the B051-000, and provides information about each of their sessions. It also provides the option of ending a session by selecting the account from the Sessions list and clicking the *End Session* icon.



Username	IP	Login Time	Client	Category	Devices	Ports
administrator	10.3.32.123	2017/08/16 10:41:54	JavaClient	Administrator	B051-000	[01] KVMPort
administrator	10.3.32.123	2017/08/16 11:05:51	Browser	Administrator	None	

Customization

Use this section to edit device settings.



Mode
□ Force All to Grayscale
☑ Enable Client AP Device List

USB IO Settings
OS: Win
Language: US English

Multiuser Mode
Multiuser Mode: Share
Occupy Timeout: 3 sec (0-255)

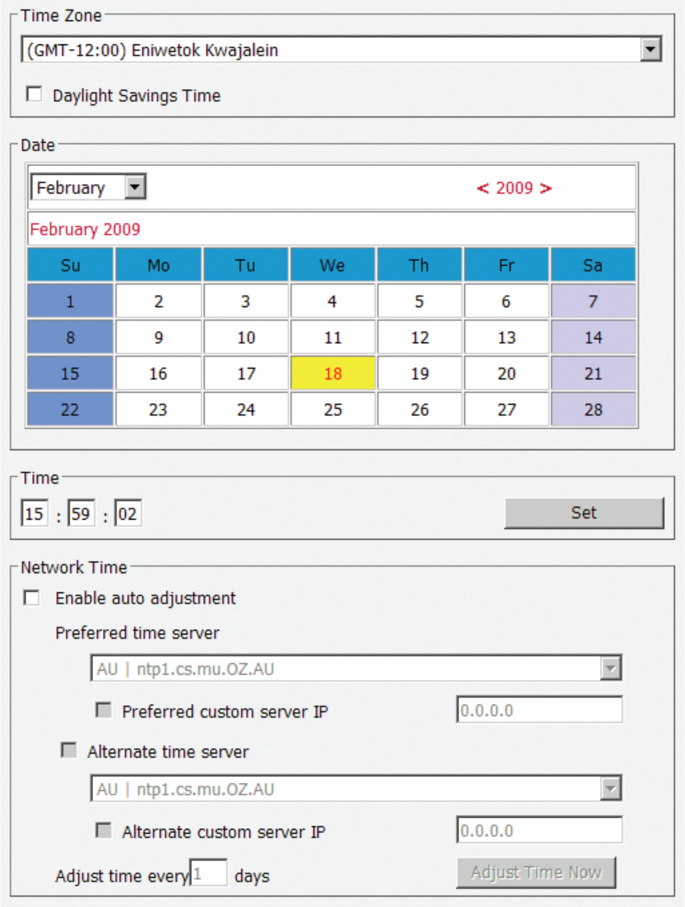
Reset

□ Reset on exit

- **Mode**
  - o **Force All to Grayscale**—Changes the remote displays of all devices connected to the B051-000 to grayscale. This can speed up I/O transfer in low-bandwidth situations.
  - o **Enable Client AP Device List**—The unit appears in the Server List when using the non-browser WinClient or Java Client AP. If this option is not checked, you can still connect to the unit, but its name will not appear in the Server List.
- **USB IO Settings**
  - o **OS**—Specifies the operating system the server on the connected port is using. Choose from Win, Mac, Sun and Other. The default is Win.
  - o **Language**—Specifies the OS language being used by the server on the connected port. The drop-down menu shows the available choices. The default is English US.
- **Multiuser Mode**—Defines how a port is to be accessed when multiple users have logged on, as follows:
  - o **Exclusive**—The first user to switch to the port has exclusive control over it. No other users can view the port.
  - o **Occupy**—The first user to switch to the port has control over the port, but additional users may view the port's video display.
  - o **Share**—Users simultaneously share control of the port. Input from the users is placed in a queue and executed chronologically. Under these circumstances, users can take advantage of the Message Board, which allows a user to take control of the keyboard/mouse or keyboard/mouse/video of a Share port.
  - o **Occupy Timeout**—If there is no user input for the amount of time specified here, the control privilege is released and transferred to the next user who moves the mouse or uses the keyboard.
- **Reset**—After making network changes, be sure to check the Reset on *exit* checkbox before logging out. This allows changes to take effect without having to power the unit off and on. Click *Reset Default Values* to use the default factory settings.

Date/Time

The *Date/Time* page allows the user to set the date and time parameters for the KVM switch. The following section describes the settings on this page.



Time Zone

(GMT-12:00) Eniwetok Kwajalein

□ Daylight Savings Time

Date

February

< 2009 >

February 2009

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Time

15 : 59 : 02

Network Time

□ Enable auto adjustment

Preferred time server

AU | ntp1.cs.mu.OZ.AU

□ Preferred custom server IP 0.0.0.0

□ Alternate time server

AU | ntp1.cs.mu.OZ.AU

□ Alternate custom server IP 0.0.0.0

Adjust time every 1 days

Time Zone

- Use the drop-down menu at the top of this section to select the Time Zone where the B051-000 is located.
- If your area uses Daylight Savings Time, check the *Daylight Savings Time* checkbox.

To manually set the date and time, do the following:

1. In the *Date* section, select the current month using the drop-down menu.
2. If needed, click the < or > buttons in the *Date* section to move backward or forward to the correct year.
3. In the calendar in the *Date* section, click on the current day.
4. In the *Time* section, enter the current time using the 24-hour HH:MM:SS format.
5. Click the *Set* button in the *Time* section to apply your changes.

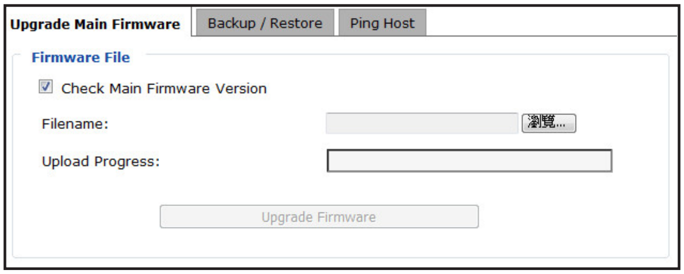
Network Time

To have the time automatically synchronized to a network time server, do the following:

1. Check the *Enable Auto Adjustment* checkbox.
2. Select a time server from the *Preferred Time Server* drop-down list, or check the *Preferred Custom Server IP* checkbox, and enter the IP of your preferred time server.
3. If desired, repeat step 2 to enter an *Alternate Time Server*.
4. Key in the desired number of days between synchronization in the *Adjust Time Every _ _ Days* field.
5. Click the *Adjust Time Now* button to synchronize immediately.

Maintenance

The *Maintenance* page allows *Administrators* and *Select* accounts who have been given *Configure* permission (See the *User Management* section in this manual for details) to upgrade the B051-000 firmware, as well as back up and restore the settings of the unit. The settings found in this page are described in the following sections.



Firmware Upgrade

As firmware upgrades become available, you can find them online at www.tripplite.com/support. To upgrade the firmware, follow the steps below:

1. Go to www.tripplite.com/support to download the most current firmware and save it to a computer that is not connected to the B051-000.
2. Log in to the Admin Utility, and navigate to the *Maintenance* page.
3. By default, the *Check Firmware Version* box is checked, which causes the unit to check if the current firmware installed on the B051-000 is the same or newer than that of the file you are using to upgrade the firmware. If the current version is the same or newer, you will not be allowed to continue with the upgrade. If you wish to perform an upgrade without checking to see if the current firmware version is the same or newer than the upgrade file, simply uncheck this checkbox.
4. Click the *Browse* button, and then navigate to and select the firmware upgrade file you downloaded from the Tripp Lite website.
5. Click the *Upgrade Firmware* button to begin the upgrade.
6. When the upload is complete, a message appears stating the operation was successful. Log out of the unit, and click *Yes* on the prompt that appears to notify you that a system reset will take place. The unit will reboot (this may take a few minutes), and the upgrade will be complete. In the event of a firmware upgrade failure, see the *Upgrade Recovery* section below.

Firmware Upgrade Recovery

Should the firmware upgrade procedure fail, and the unit becomes unusable, follow the steps below to restore it.

***Note**: It is strongly recommended that you take advantage of the B051-000 backup functionality (See* Backup *section for details) in the event that you may need to use this procedure.*

1. Power off the unit.
2. Press and hold the Reset button on the front of the unit.
3. Power on the B051-000 while holding down the Reset button.
4. The B051-000 will be restored to its original firmware version and settings. You will now be able to access the unit and try upgrading the firmware again.

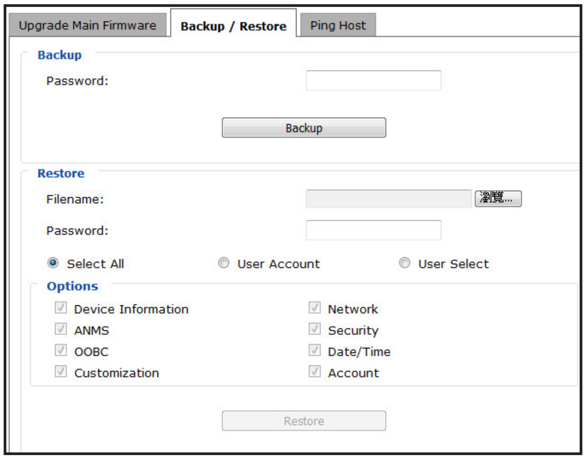
Backup

The *Backup* section allows you to create a backup file of the B051-000 settings, in the event you need to restore the settings of the unit to those of a previous time period. To create a backup of the B051-000, follow the steps below.

1. Key in a password in the *Password* field, to be used when restoring the settings of the unit.

   ***Note**: Setting a password is optional. If you do not wish to use a password, you can skip this step.*

2. Click the *Backup* button.
3. A pop-up appears asking you to save the backup file. Browse to a desired location on your computer and save the file.



● Select All ○ User Account ○ User Select

Options

☑ Device Information ☑ Network
☑ ANMS ☑ Security
☑ OOBC ☑ Date/Time
☑ Customization ☑ Account

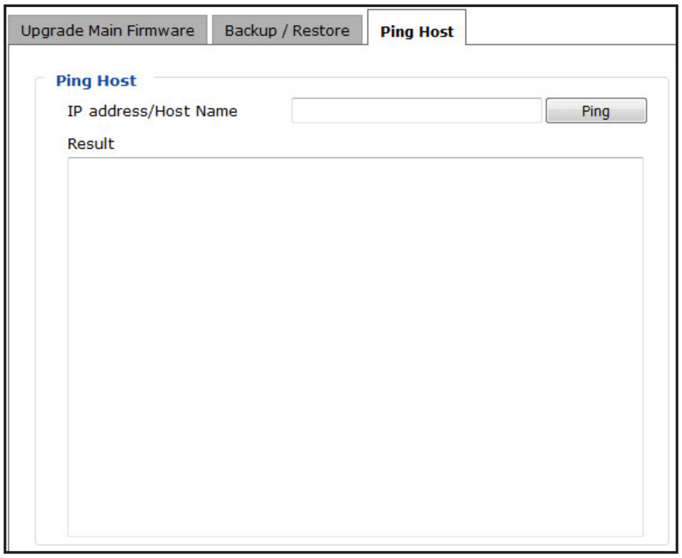
Restore

The *Restore* section allows you to restore the settings of the unit using a previously saved backup file. Information on the unit will be replaced with that of the backup file. To restore the settings of the unit using a backup file, follow the steps below.

1. Click on the *Browse* button to the right of the filename field, and then navigate to and select the backup file.
2. If you set up a password when creating the backup file, enter it in the *Password* field.
3. Select as many of the options that are presented as you wish to restore, and then click the *Restore* button. Once complete, a message appears to inform you that the procedure succeeded, and that the changes will take place upon the next login.

Ping Host

The *Ping Host* page lets you ping the IP address of a device to see if it's responding on the network. To ping a device, enter its IP address, and click *Ping*.



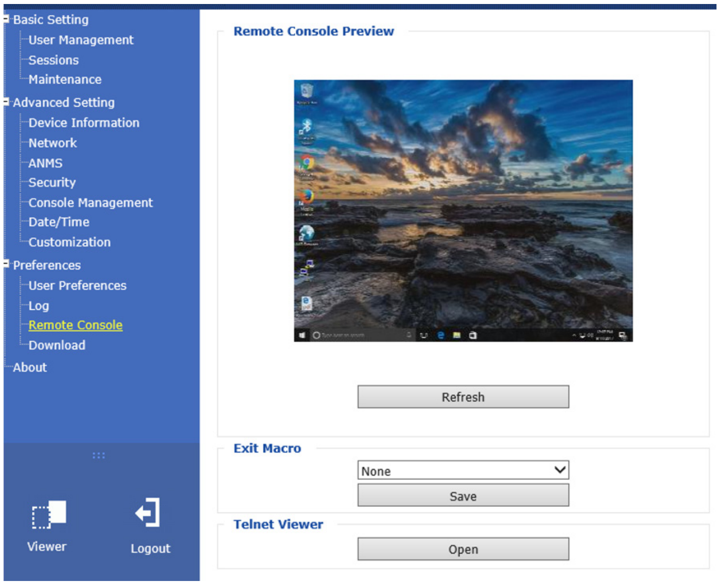
Remote Session Operation

Depending on whether you login to the B051-000 via web browser or one of the non-browser applications, you will initiate a remote session in different ways.

***Note**: If you are initiating a remote session for the first time, you will be prompted to install an ActiveX Control when using the Windows Client. When using the Java Client, you may be prompted to confirm that the site can be trusted. Proceed with any prompts that appear.*

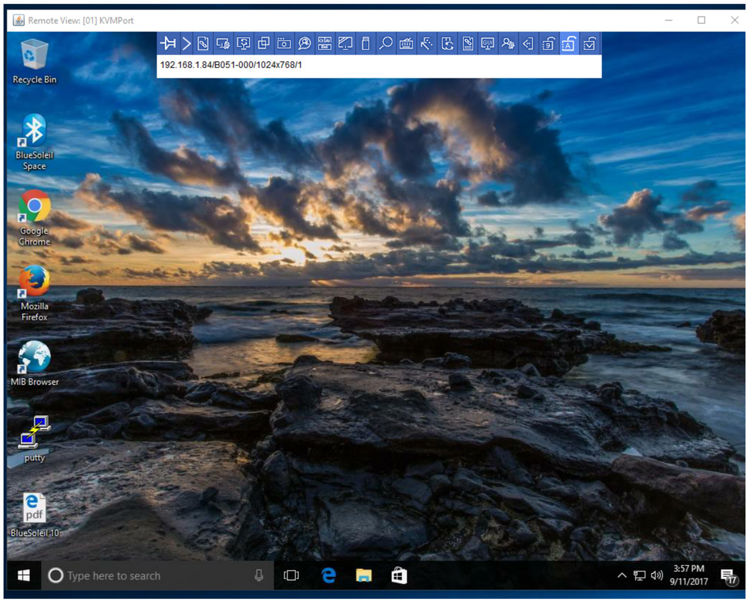
Remote Console Preview

The *Remote Console Preview* displays a snapshot of the screen of the connected computer/KVM. Clicking *Refresh* below the preview screen will refresh the snapshot to display the current screen image.



Java Applet and Windows Client

On the left side of the *Remote Console Preview* screen is a viewer link that allows you to initiate a remote session. By default, the admin utility is set to automatically detect what browser you are using and display the appropriate link. For example, if using Internet Explorer, the *Windows Client* link will be the default. If using a browser other than Internet Explorer, the *Java Applet* link will be the default. The *Java Applet* can be used in both Internet Explorer and non-Internet Explorer browsers, but the *Windows Client* can only be used in Internet Explorer. To use the *Java Applet* in Internet Explorer, you must access the *User Preferences* page and select it. (See the *User Settings* section in this manual for details) Clicking on one of these links will initiate a remote session.



When a remote session is initiated, the screen of the computer/KVM switch that is connected to the B051-000 will appear with a *Control Panel* located in the top-center.

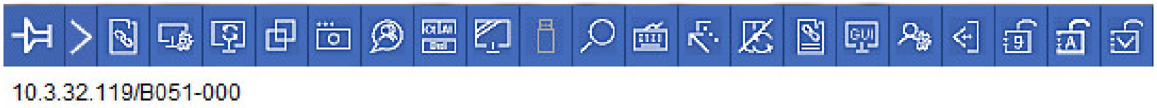
***Note**: If connected to a KVM switch, you will need to use the KVM's OSD or Hotkey Commands to switch between computers connected to it.*

Remote Session Operation

Control Panel

The *Control Panel* is provided as a way for the user to optimize and control the remote session. Regardless of how you initiated a remote session, the *Control Panel* and its functionality remain the same. When a remote session is initiated, the *Control Panel* appears at the top-center of the screen for a few seconds and then disappears. To display the *Control Panel* after it has disappeared, simply hover your mouse pointer over the top-center of the screen.

The *Control Panel* consists of an icon bar at the top and two text bars at the bottom. When the mouse pointer is hovered over an icon, the description of the icon is displayed in the text bar. When the mouse pointer is not over an icon, the text bars display the video resolution of the selected computer and the IP address of the B051-000. You can drag the control panel to any location on the remote screen by hovering over the text bar, and then clicking-and-dragging it. Each of the icons contained in the *Control Panel* and their functionality is described in the sections that follow.



10.3.32.119/B051-000

Always on Top / Auto Hide – Click this button to toggle between displaying the control panel all the time, or to allow it to disappear after a few seconds of inactivity.

Hotkeys / Macros – The *Hotkeys / Macros* page allows the user to use Hotkeys and Macros to manipulate the remote computer. The user can enable/disable hotkeys, and create/edit *User Macros* and *System Macros*. The sections that follow describe how these features work.

Hotkeys

Various configuration actions related to the keyboard, video and mouse can be performed via hotkey combinations. The *Hotkey* setup utility is accessed by clicking on the *Hotkey / Macros* icon and then clicking on the *Hotkeys* button at the top of the screen. The *Hotkeys* screen displays the available hotkeys and their corresponding hotkey combinations.

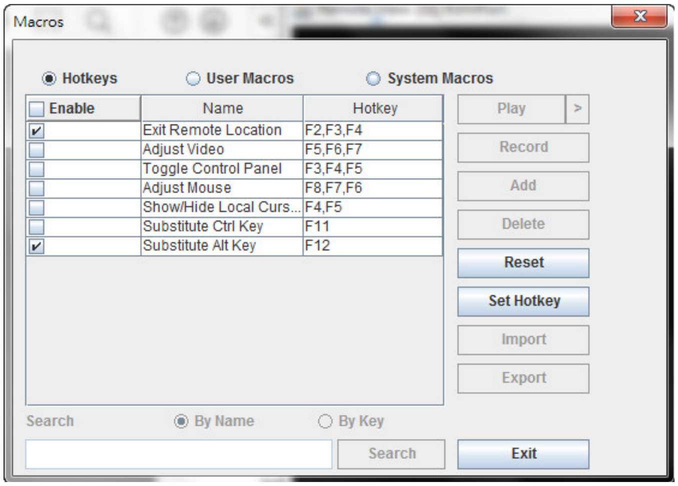
By default, the only hotkeys that are enabled are the *Exit Remote Location* and *Substitute Alt Key* hotkeys. To enable/disable a hotkey, simply check/uncheck the box to the left of it. To change a hotkeys command sequence, follow the steps below.

1. Highlight the desired hotkey and click on the Set Hotkey button.
2. Key in the desired hotkey combination, one key at a time. The keys will be displayed in the hotkey column as they are entered.

   ***Note**: Clicking the Cancel button will cancel the recording process. Clicking on the* Clear *button will delete any keys that you entered while keeping the recording process active.*

3. When finished entering the hotkey sequence, click on the *Save* button.

   ***Note**: Clicking the Reset button will restore all of the default hotkey command sequences, and enable/disable defaults. You can use the same function keys for more than one hotkey command sequence, as long as the first key is not the same. For example, you can use [F1, F2, F3] for one action and [F2, F1, F3] for another, but you cannot use [F1, F3, F2] once [F1, F2, F3] has been used.*



Macros

● Hotkeys ○ User Macros ○ System Macros

□ Enable	Name	Hotkey
☑	Exit Remote Location	F2,F3,F4
□	Adjust Video	F5,F6,F7
□	Toggle Control Panel	F3,F4,F5
□	Adjust Mouse	F8,F7,F6
□	Show/Hide Local Curs...	F4,F5
□	Substitute Ctrl Key	F11
☑	Substitute Alt Key	F12

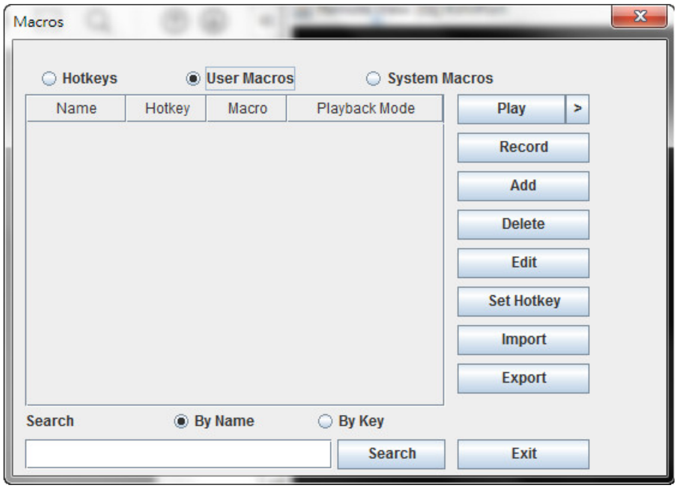
Search ● By Name ○ By Key

Remote Session Operation

The table below lists the default hotkeys, along with a description of their functions and their default command sequences.

Hotkey	Description	Command Sequence
Exit Remote Location	Closes you out of a remote session.	[F2, F3, F4]
Adjust Video	Opens the Video Settings screen.	[F5, F6, F7]
Toggle Control Panel	Toggles the Control Panel off and on. When off, you will not be able to access the control panel.	[F3, F4, F5]
Adjust Mouse	When the local and remote mouse pointers go out of sync, this command brings them back together again.	[F8, F7, F6]
Show/Hide Local Cursor	Toggles the local mouse pointer on/off.	[F4, F5]
Substitute Ctrl Key	By default, hotkey combinations that use the Ctrl key, such as [Ctrl, Alt, Delete], get sent to the local computer. This hotkey allows you to set a substitute Ctrl key that can be used for the remote computer.	F11
Substitute Alt Key	By default, hotkey combinations that use the Alt key, such as [Ctrl, Alt, Delete], get sent to the local computer. This hotkey allows you to set a substitute Alt key that can be used for the remote computer.	F12

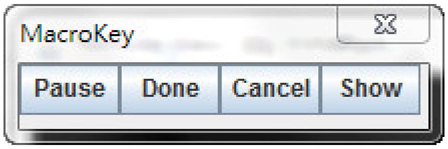
User Macros



The *User Macros* page allows you to add macros to the unit that can be performed on the connected computer using the *Macro List* feature of the control panel (See *Macro List* section for details). By default, the *User Macros* page is displayed when the *Hotkeys / Macros* icon is clicked on. To display the page when it isn't selected, click on the *User Macros* button at the top of the *Hotkeys / Macros* screen.

To create a macro, follow the steps below.

1. Click the *Add* button on the right side of the screen.
2. In the name field that appears, key in a name for the macro you are adding.
3. With the new macro highlighted, click the *Record* button on the right side of the screen. Recording will begin and the following panel will be displayed in the upper-left corner of the remote screen.



4. Enter in the macro hotkey sequence and then click the *Done* button. You will be returned to the *User Macros* screen, with your macro name and hotkey combination added to the list. Repeat this procedure for any additional macros you wish to create.

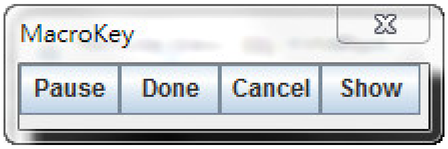
   ***Note**: Clicking the* Pause *button will pause/unpause the recording of the hotkey sequence. Clicking the Cancel button will cancel the recording of the hotkey sequence. Clicking the Show button will display the hotkeys as they are entered.*

System Macros

The *System Macros* page allows you to add macros to the unit that can be performed automatically upon closing a session. For example, you can create a macro that sends the Winkey-L combination, causing a computer's login page to come up the next time it is accessed. To display the *System Macros* page when it isn't selected, click on the *System Macros* button at the top of the *Hotkeys* / *Macros* screen.

To create a macro, follow the steps below.

1. Click the *Add* button on the right side of the screen.
2. In the name field that appears, key in a name for the macro you are adding.
3. With the new macro highlighted, click the *Record* button on the right side of the screen. Recording will begin and the following panel will be displayed in the upper-left corner of the remote screen.

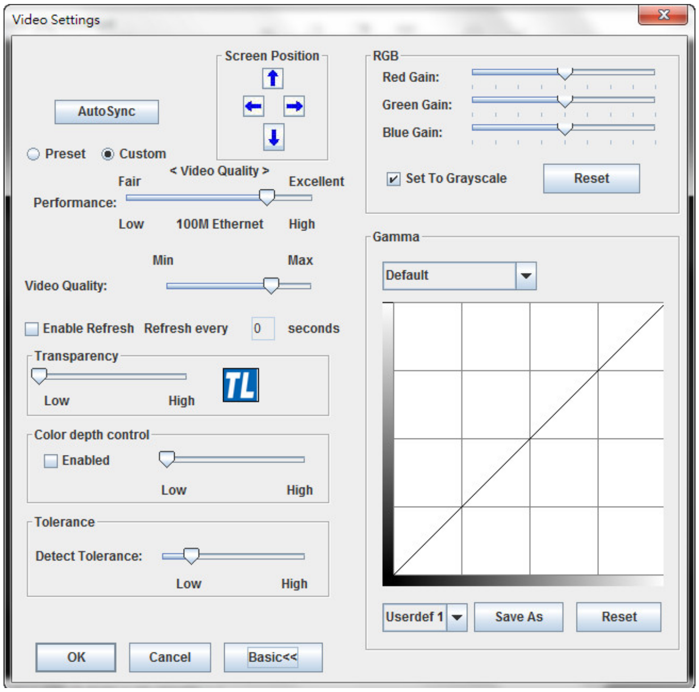


4. Enter the macro hotkey sequence and then click the *Done* button. You will be returned to the *System Macros* screen, with your macro name and hotkey combination added to the list. Repeat this procedure for any additional macros you wish to create.

   Note*: Clicking the* Pause *button will pause/unpause the recording of the hotkey sequence. Clicking the* Cancel *button will cancel the recording of the hotkey sequence. Clicking the* Show *button will display the hotkeys as they are entered.*

Once system macros are created, they are available to be assigned via the *Exit Macro* setting (See the *Exit Macro* section in this manual for details).

Video Settings – The *Video Settings* screen allows you to adjust the placement and picture quality of the remote screen. The quality of the image display has a direct effect on the keyboard and mouse response time. Higher-quality video results in more information being transferred over the network, which can cause slow keyboard and mouse response time in slower networks. Click this icon to open the *Video Settings* screen.



☑ Set To Grayscale

□ Enable Refresh Refresh every 0 seconds

□ Enabled

Default

Userdef 1

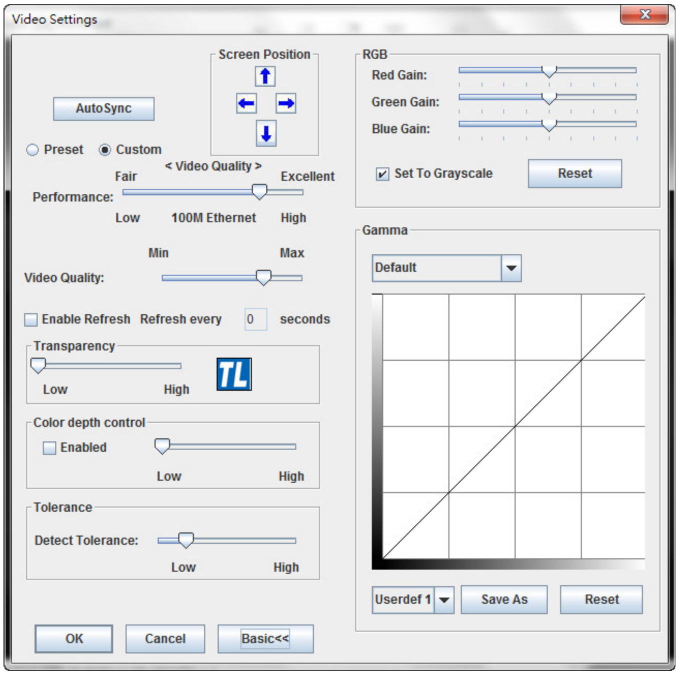
The table below describes the contents of the *Video Settings* screen:

Setting	Description
Screen Position	Adjust the horizontal and vertical position of the screen using the *Screen Position* arrows.
Auto Sync	Click this button to automatically detect the vertical and horizontal position settings of the remote screen. If the local and remote mouse pointers are not synced, performing this function will normally bring them back into alignment. If *Auto Sync* fails to align the screen properly, use the *Screen Position* arrows to make manual adjustments.
RGB	Move the RGB (Red, Green, Blue) slider bars to adjust the corresponding color component of the video image. Check the *Set to Grayscale* checkbox to display the video of the remote computer in black and white. If the remote keyboard and mouse response time is slow or choppy, checking the *Set to Grayscale* option can speed them up.
Gamma	This section allows you to adjust the video display's gamma level. This function is discussed in detail in the *Gamma Adjustment* section following this table.
Performance	Select the type of internet connection that exists between the Local Client computer and the B051-000. The B051-000 will use that selection to automatically adjust the *Video Quality* and *Detect Tolerance* settings to optimize the quality of the video display. Because network conditions vary, if none of the preset choices works well, you can select *Customize* and use the *Video Quality* and *Detect Tolerance* slider bars to adjust settings to suit your conditions.
Video Quality	Drag the slider bar to adjust the overall quality of the video of the remote computer. On slower networks, lowering the video quality can help improve keyboard and mouse response time.
Enable Refresh	The remote screen can be set to be redrawn every 1 to 99 seconds, eliminating unwanted artifacts that would otherwise remain on the screen. Click the *Enable Refresh* checkbox to activate this feature, and then enter in the desired refresh rate.
Transparency	Adjusts the transparency of the toolbars displayed by the Windows and Java Clients. Move the slider bar until the transparency is set to the desired level.
Color Depth Control	Allows you to adjust the amount of color information sent over the network for the remote monitor. For slower networks, setting the color depth to a lower setting can help improve remote session performance. Enable checkbox to activate this setting.
Detect Tolerance	This setting governs allowable pixel changes. A high setting limits changes, resulting in lower video quality and less data transfer. A low setting allows more changes, resulting in higher video quality and more data transfer. On slower networks, a high detect tolerance setting can help improve keyboard and mouse response time.

Gamma Adjustment

If it is necessary to correct the gamma level for the remote computer, use the *Gamma* function in the *Video Settings* screen. Under the *Basic* configuration, the gamma drop-down list includes ten preset and four user-defined gamma levels to choose from. Simply select the desired setting from the drop-down list. To set your own gamma levels, follow the instructions below.

1. Click the *Advanced* button to bring up the gamma adjustment settings.



Video Settings

○ Preset ● Custom

Performance: 100M Ethernet

☐ Enable Refresh Refresh every 0 seconds

☐ Enabled

☑ Set To Grayscale

Gamma: Default

Userdef 1

2. Click and drag the diagonal line at as many points as you wish to achieve the display output you desire. Click the *Reset* button at any time to abandon changes and return to the default gamma settings. Click the *Cancel* button to abandon changes and close the *Video Settings* screen.
3. To save the new gamma settings, select a user-defined setting from the drop-down list and click the *Save* button. Your gamma settings will be saved to the selected user defined option.

Video Auto Sync – Click this icon to have the vertical and horizontal offset values of the remote screen automatically detected and synchronized with the local screen.

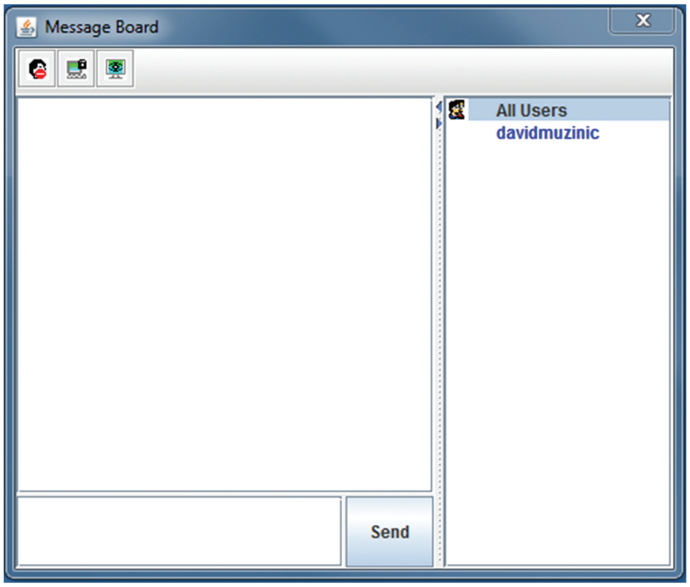
Note: *If the local and remote mouse pointers are out of sync, performing a video auto sync will normally bring them back into alignment. If the video auto sync fails to align the screen properly, use the screen position arrows in the Video Settings screen to make manual adjustments.*

Screen Mode – Click this icon to toggle *Full Screen* mode on/off. For those accessing the unit via one of the Windows clients, right-clicking this icon will toggle *Keep Screen Size* on/off. When *Keep Screen Size* is enabled, turning on *Full Screen* mode will not change the size of the remote screen. For example, remote screens that are set to resolutions lower than that of the local monitor will be displayed as a box inside the local display. When both *Keep Screen Size* and *Full Screen Mode* are enabled, the remote screen will be displayed as a box with a black background. If Keep Screen Size is disabled and Full Screen Mode is enabled, the screen will be stretched to fit the entire local monitor.

Note: *Keep Screen Size can only be toggled on/off when using one of the Windows clients. When using one of the Java clients, Keep Screen Size is always enabled.*

Snapshot – Clicking this icon will take a screenshot of the remote computer and save it to the local computer. By default, snapshots are saved to the local computer's desktop. The file type, quality and location can be changed via the *Customize Control Panel* page.

Message Board – The B051-000 supports multiple user logins, which can give rise to access conflicts. To alleviate this problem, a message board feature has been provided that allows users to communicate with each other.



The buttons on the button bar at the top of the message board are toggles. The actions for each of these buttons are described in the table below.

Button	Function
	Enable/Disable Chat – When disabled, this icon displays next to the disabled user's name in the *User List* panel of all users' message boards. Messages directed to the disabled user are not displayed on the message board. The button is shadowed when chat is 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 *User List* of all users' message boards.
	Occupy/Release Keyboard/Mouse – When you occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed, and this icon displays next to the occupying user's name in the *User List* of all users' message boards.

User List Panel

- To hide/unhide the *User List* panel, click on the arrows in the panel separator.
- The names of all the logged-in users appear in the *User List* panel. Select the names of the users that you wish to communicate with before sending your message.
- If a user has disabled chat, its icon displays before that user's name.
- If a user has occupied the KVM or the KM, the corresponding icon displays before that user's name.

Remote Session Operation

Compose Panel

Type your message into this panel and then click the Send button or press the [Enter] key to post the message to the message board.

***Note**: You must select the user that you want to communicate with from the user list. 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 do not appear.

Ctrl – Alt – Delete – Click this icon to send the [Ctrl, Alt, Delete] command to the remote computer.

Set to Grayscale – Click this icon to display the remote video in black and white. On slower networks, displaying the remote video in black and white can help improve keyboard and mouse response time.

Virtual Media – The *Virtual Media* function allows a drive, folder, image file, smart card reader or removable disk on a user's system to be accessible on the remote server. The following media are supported via the B051-000 *Virtual Media* functionality.

Browser and non-Browser Windows Client

- IDE CD-ROM/DVD-ROM Drives – Read Only
- IDE Hard Drives – Read Only
- USB CD-ROM/DVD-ROM Drives – Read Only
- USB Hard Drives – Read/Write*
- USB Flash Drives – Read/Write*
- USB Floppy Drives – Read/Write
- Smart Card Readers
- ISO Files – Read Only
- Folders – Read/Write

** These drives can be mounted either as a Drive or as a Removable Disk. Mounting as a Removable Disk allows the user to boot the remote server if the disk contains a bootable OS. If the disk contains more than one partition, the remote server can access all of the partitions.*

Browser and non-Browser Java Client

- ISO Files – Read Only
- Folders – Read/Write

Virtual Media Operation

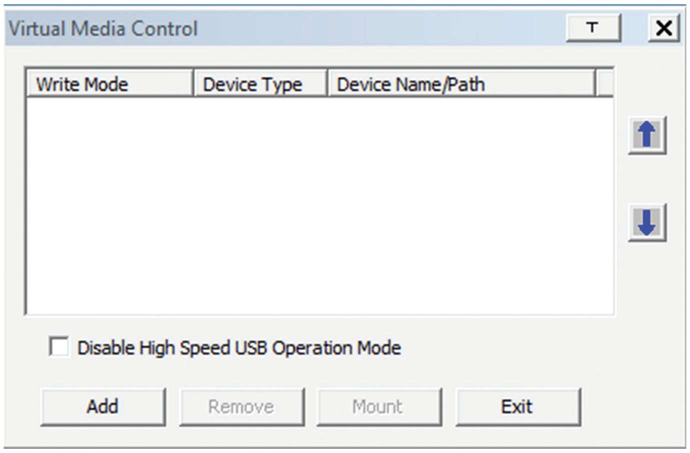
When accessing a connected computer remotely, you can use media from the computer you are accessing the unit with on the remote computer. To access virtual media via remote session, follow the instructions below.

***Notes**:*

1. *In order to use the Virtual Media functionality, the USB virtual media cable that came with the B051-000 must be connected from the unit to the computer.*
2. *When accessing the unit remotely with a Windows Vista or 7 computer, you must run Internet Explorer as an administrator for virtual media to function properly.*
3. *When mounting a smart card reader, the smart card reader driver must be installed on both the computer being used to access the B051-000 and the computer connected to the B051-000.*
4. *When mounting a smart card reader, no other virtual media can be mounted at the same time.*
5. *The Java Client only supports the mounting of ISO Files and Folders. The Windows Client must be used for all other media.*

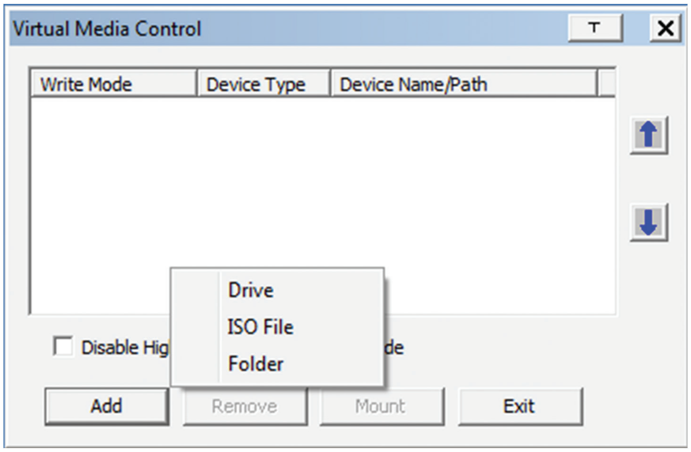
Remote Session Operation

1. Click the *Virtual Media* icon on the control panel to bring up the following screen.



***Note**: The T button in the upper-right corner brings up a slider bar that allows you to adjust the transparency of the virtual media screen. When you're finished making an adjustment, simply click anywhere on the screen to close the slider bar.*

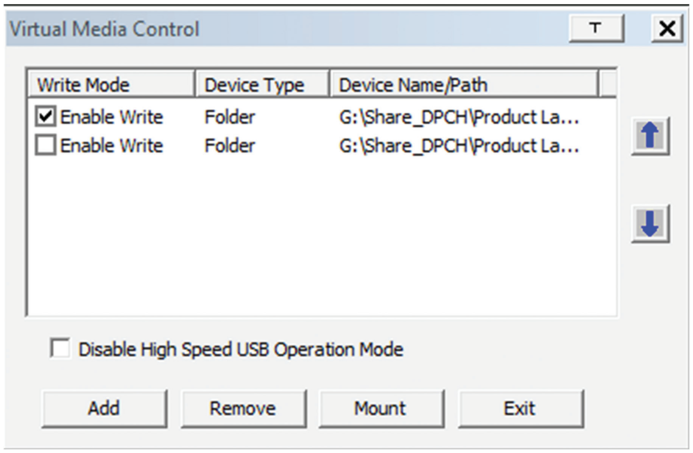
2. Click the *Add* button and then select the desired media from the list of media sources that appears. Each selected media source will allow you to choose the available drive, file, folder or removable disk.



***Note**: If your media source is USB 1.1, check the* Disable High Speed USB Operation Mode *checkbox.*

3. Repeat this step to add as many media sources as you want to the *Virtual Media* screen. To remove a media source from the list, highlight it and click the *Remove* button.

***Note**: When mounting a smart card reader, no other virtual media can be mounted at the same time. Otherwise, up to 3 media sources can be used at any one time, with the top 3 sources in the list being the active devices. To rearrange the device order, highlight the desired device and use the arrow keys on the right of the screen to move the device up or down in the list.*



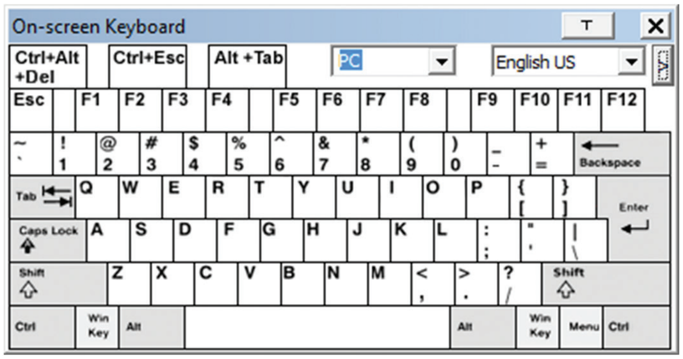
Write Mode	Device Type	Device Name/Path
☑ Enable Write	Folder	G:\Share_DPCH\Product La...
□ Enable Write	Folder	G:\Share_DPCH\Product La...

4. Some media sources are *Read Only*, whereas others are *Read/Write*. Those that are *Read/Write* can be viewed on the remote computer, and can have data from the remote computer added to them. Those that are *Read Only* can only be viewed. *Read Only* media sources will be grayed out in the list, not allowing you to check the *Enable Write* checkbox to the left of the source. *Read/Write* sources will not be grayed out, and you will be able to decide whether data can be added to them or not. By default, *Read/Write* sources are displayed with the *Enable Write* checkbox unchecked, which means that data cannot be added to them. To allow data from the remote computer to be added to a media source, simply check the *Enable Write* checkbox to the left of it in the list.
5. Once all media sources are added, and the desired 3 media sources are at the top of the list, click the Mount button to close the dialog box and open the media sources on the remote computer.

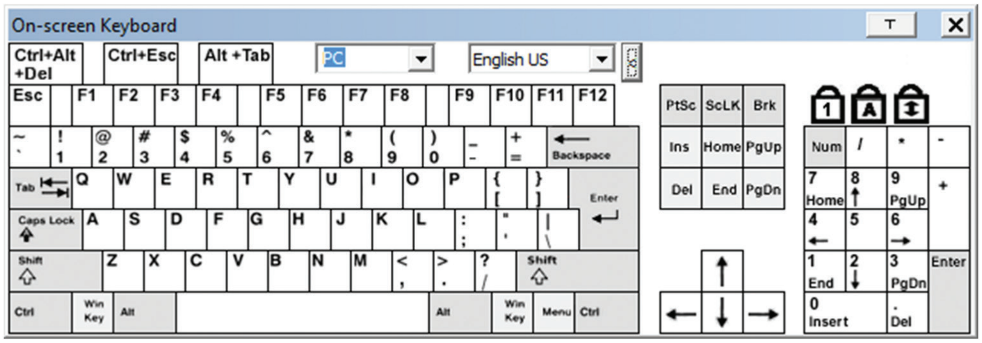
   ***Note**: Depending on the speed of your network and the size of the media source, it may take 30 seconds or so for the dialog box to close and the media to open on the remote computer.*
6. To disconnect the media sources from the remote computer, click on the *Virtual Media* icon in the control panel.

Zoom – Click this icon to zoom in on the remote display. You can choose to display the screen at 100%, 75%, 50% or 25%. Checking the 1:1 checkbox will keep the screen contents sized in a 1:1 ratio, regardless of whether you choose to display the remote session at 100%, 75%, 50% or 25%.

On-Screen Keyboard – The Control Panel features an on-screen keyboard, available in multiple languages, with all of the standard keyboard keys for each language. Click this icon to display the on-screen keyboard.



- To switch to a different language keyboard, open the drop-down list in the upper-right of the on-screen keyboard and select the desired language.
- To expand the keyboard to include the number pad, click on the arrow icon to the right of the language drop-down menu.



Mouse Pointer – Click to choose how the local and remote mouse pointers are displayed. You can choose to display *Dual* mouse pointers, *Crosshairs* mouse pointers, the local mouse pointer as a tiny dot (not available via Java) or only the remote mouse pointer. *Dual* mouse pointers display both local and remote mice as arrows. *Crosshairs* mouse pointers display the local mouse as a cross, and the remote mouse pointer displays the remote mouse as an arrow. When displaying the local mouse pointer as a tiny dot, the remote mouse pointer will be displayed as an arrow.

Mouse Sync Mode – Click to toggle between automatic and manual mouse sync modes. When set to automatic, the icon shown on the left appears. When set to manual, a slash appears over the icon.

***Note**: This icon is only active on computers that are connected using the USB KVM cable kit. The auto sync functionality only supports Windows and Mac (G4 and higher), and the USB IO settings OS drop-down must be set to Windows or Mac (See* Customization *section in this manual).*

Mac and Linux Considerations

A second Mac auto-sync setting is available for Mac OS X 10.4.11 and higher. If you find that enabling automatic mouse sync per the instructions above does not provide satisfactory results, right-click the mouse in the black text area of the control panel, highlight the Mouse Sync Mode option and select Automatic for MAC 2.

Although Linux does not support automatic mouse sync mode, there is an additional setting in the Mouse Sync Mode drop-down menu for Redhat AS3.0 systems. If you are having difficulty synchronizing the local and remote mice, try right-clicking the mouse in the black text area of the control panel, highlight the Mouse Sync Mode option and select Automatic for Redhat AS3.0.

Manual Mouse Synchronization

If the local mouse pointer goes out of sync with the remote system's mouse pointer, there are a number of methods to bring them back into sync.

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 that follow. The *Mouse Properties Settings* should be set on the computers attached to the B051-000, not the computer you are using to access it.

***Note**: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS 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
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 and later:

1. Open the *Mouse Properties* dialog box
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

Sun / Linux:

Open a terminal session and issue the following command:

Sun: xset m 1

Linux: xset m 0

Mouse Synchronization Procedures

If you are having syncing problems after adjusting the mouse properties, try the following methods to help synchronize the local and remote mouse pointers, as well as improve response time.

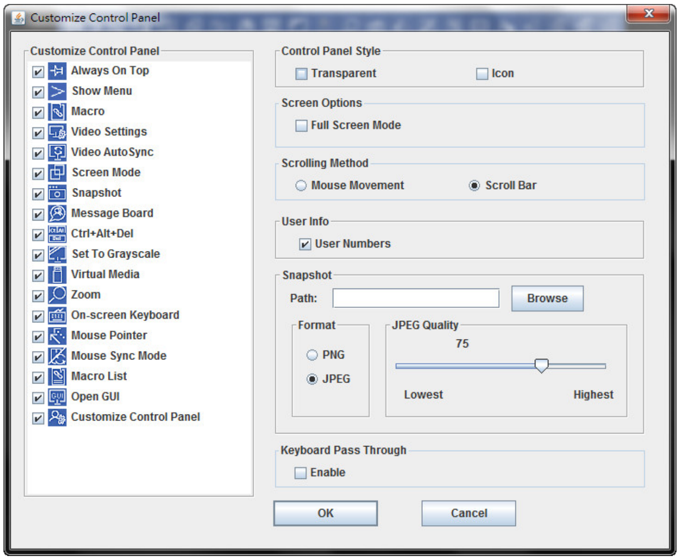
***Note**: Mouse synchronization may require several seconds to take effect. Wait 15 to 30 seconds to ensure that the mouse has had enough time to sync.*

- When in a remote session, move the mouse pointer to the upper-center of the screen to open the control panel, and then move it back into the remote screen.
- When in a remote session, move the mouse pointer to all four corners of the screen.
- Click the *Video Auto Sync* icon in the control panel. In most cases, the local and remote mouse pointers will sync following the video auto-sync.
- Activate and invoke the *Adjust Mouse* hotkey command (see *Hotkeys* section for details). This hotkey command defaults at F8, F7, F6.
- To improve response time, adjust the video settings to decrease the amount of information being transferred over the network. The less data that is being sent, the faster the response time. In particular, the *Quality* and *Detect Tolerance* settings in the *Video Settings* screen (see *Video Settings* section for details) can help improve keyboard and mouse response time.
- To improve response time, go to the *Network* page in the OSD and reduce the *Network Transfer Rate* setting (See *Network* section under *Device Management* in *OSD Operation* for details).
- To improve response time, go to the display settings section of the remote computer and lower the video resolution, refresh rate and color settings.
- If the remote computer has a graphic desktop background, change it to a solid color background.

Macro List – Click this icon to display a drop-down list of the User Macros (see *User Macros* section for details) that have been added. Select a macro to run it on the selected computer.

Open GUI – Click this icon to open the Admin Utility.

Customize Control Panel – Click this icon to bring up the Customize Control Panel screen, which allows you to choose which icons are displayed in the control panel, as well as edit some of its features.



Customize Control Panel

Customize Control Panel
- ☑ Always On Top
- ☑ Show Menu
- ☑ Macro
- ☑ Video Settings
- ☑ Video AutoSync
- ☑ Screen Mode
- ☑ Snapshot
- ☑ Message Board
- ☑ Ctrl+Alt+Del
- ☑ Set To Grayscale
- ☑ Virtual Media
- ☑ Zoom
- ☑ On-screen Keyboard
- ☑ Mouse Pointer
- ☑ Mouse Sync Mode
- ☑ Macro List
- ☑ Open GUI
- ☑ Customize Control Panel

Control Panel Style: □ Transparent □ Icon

Screen Options: □ Full Screen Mode

Scrolling Method: ○ Mouse Movement ● Scroll Bar

User Info: ☑ User Numbers

Snapshot
Path: Browse
Format: ○ PNG ● JPEG
JPEG Quality: 75 (Lowest – Highest)

Keyboard Pass Through: □ Enable

OK Cancel

Customize Control Panel – The box on the left side of the screen displays a list of the available control panel features, with a checkbox next to each one. Check/uncheck a checkbox to display or remove the corresponding features icon from the control panel. By default, all features are included in the control panel.

Control Panel Style – This section allows you to determine how the control panel is displayed when it is dragged out of the default position in the top-center of the screen.

Note*: There is a second default position for the control panel at the bottom-center of the screen.*

- When the *Transparent* checkbox is checked, dragging the control panel away from one of the default locations will leave it displayed transparently in whatever location it was dragged to.
- When the *Icon* checkbox is checked, dragging the control panel away from one of the default locations will leave it displayed as an icon in whatever location it was dragged to.
- When both the *Transparent* and *Icon* checkboxes are checked, dragging the control panel away from one of the default locations will leave it displayed as a transparent icon in whatever location it was dragged to.
- When neither checkbox is checked, dragging the control panel away from one of the default locations will leave it displayed as normal in whatever location it was dragged to.
- If the control panel is located in either the top-center or bottom-center default locations, checking these checkboxes will have no effect.

Screen Options – This section allows you to make *Full Screen Mode* the default setting when a remote session is activated.

- Check the *Full Screen Mode* checkbox to display the remote screen in *Full Screen Mode* starting with the next time you log in to a remote session.

User Info – The *User Info* section includes a checkbox labeled *Show User Numbers*, which is checked by default. When checked, it displays the number of logged-in users in the text box of the *Control Panel*.

Snapshot – The *Snapshot* section allows you to determine where snapshots are sent to; what file type they are saved as; and, if saved as a JPEG, the quality of the JPEG image. Although the Snapshot section is available to both Windows and Java users, the two differ in the types of files that can be saved. The Windows clients allow you to choose between a BMP and a JPEG file, whereas the Java clients allow you to choose between PNG and JPEG.

- **Path –** To select a location for snapshots to be saved in, click on the *Browse* button next to the *Path* field. Navigate to the desired location and select it.
- **Format –** Check the button of the file type that you want the snapshot to be saved in.
- **JPEG Quality –** If you select to save snapshots as JPEGs, you can adjust the quality of the JPEG image here. The higher the quality of the image, the larger the file size.

Keyboard Pass Through – When selected, the [Alt, Tab] function will be sent to the remote computer. When it is not selected, the [Alt, Tab] function is sent to the local computer. It is deactivated by default.

Exit – Click this icon to exit the remote session.

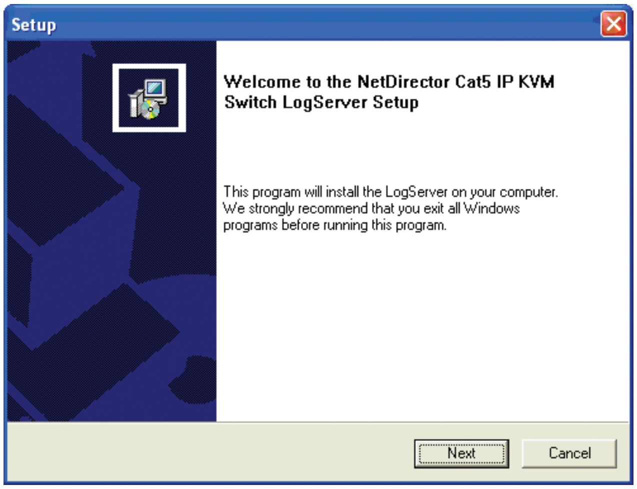
Lock LEDs – These icons display the status of the keyboard Num Lock, Caps Lock and Scroll Lock LEDs. You can click on them to toggle the corresponding lock function on/off. When first initiating a remote session, you may have to toggle these off/on to make sure they are synced up with your keyboard.

The Log Server

The Windows-based Log Server is an administrative utility that records all the events that take place on selected B051-000 units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. From the computer that you want to use as the Log Server, open your browser and log into the B051-000.
2. You will need to get the Log Server file off the CD that came with the unit. If you do not have access to the CD, contact your system administrator to obtain the Log Server file.
3. Navigate to where you saved the Log Server file and double-click it to open it. If any security warning dialog boxes appear, ignore them and click *Run* or *Open*. The Log Server installation screen appears:



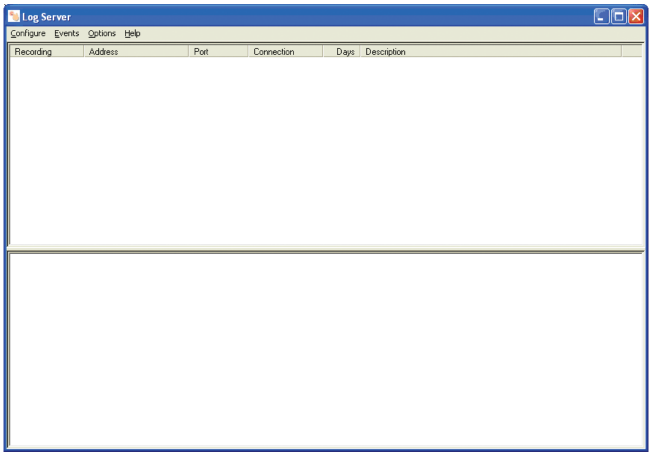
Welcome to the NetDirector Cat5 IP KVM Switch LogServer Setup

This program will install the LogServer on your computer. We strongly recommend that you exit all Windows programs before running this program.

4. Click *Next*. Then follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.
5. Before starting up the Log Server, go to the ANMS page in the Admin Utility. In the corresponding fields, enter the MAC Address and Port Number for the computer/server that you have installed the Log Server on. (See *the ANMS section in this manual* for details)

Starting Up

To bring up the Log Server, either double-click the program icon, or key in the full path to the program on the command line. The first time you run it, a screen similar to the one below appears:



Note: *The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database.*

The screen is divided into three components:

- A *Menu Bar* at the top
- A panel that will contain a list of all B051-000 units in the middle
- A panel that will contain an *Events List* at the bottom

The Menu Bar

The Menu bar consists of four drop-down menus:

- Configure
- Events
- Options
- Help

Note: *If the Menu Bar appears to be disabled, select one of the* B051-000 *units from the list window to enable it.*

Configure

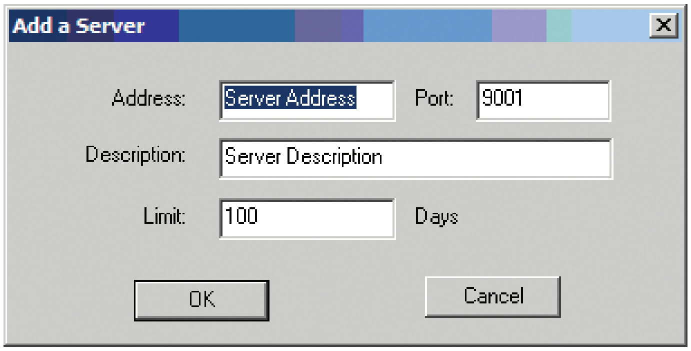
The *Configure* menu consists of three functions: *Add, Edit* and *Delete.*

Add

Select the *Add* function when you need to add a new B051-000 to the list of units that the Log Server records events for.

Note: *You must first add a B051-000 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:



Address: Server Address
Port: 9001
Description: Server Description
Limit: 100 Days

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

Field	Description
Address	This can either be the IP address of the B051-000 or its DNS name (if the network administrator has assigned it a DNS name). This value must be entered into the ANMS page to communicate with the Log Server. (See *ANMS* section for details.)
Port	Key in the port number that was specified in the ANMS page. If the port number differs between the B051-000 and the Log Server, the two will not be able to communicate with each other.
Description	This field is provided so that you can enter additional information that will help differentiate this unit from the rest of the devices the Log Server is recording information for.
Limit	This specifies the number of days that an event is kept in the Log Server's database before it can be deleted. To remove all events that have passed the expiration date set in this field, use the *Maintenance* function in the *Events* menu.

Edit

Select the *Edit* function to modify the information pertaining to an existing B051-000. To edit an existing B051-000, select it from the list and open the *Edit* function from the *Configure* drop-down menu. A dialog box will appear showing the exact information that was entered for the B051-000 when it was added using the *Add* function. Edit this information and click *OK*.

Delete

To delete a B051-000, simply select it from the list and open the *Delete* function. A dialog box will appear which will display the B051-000 information and ask you to click *OK* to delete it. If you want to remove it from the Log Server, click *OK*.

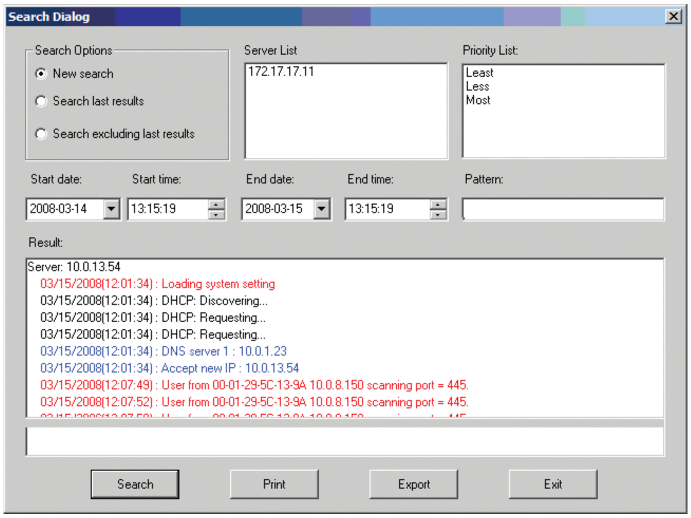
The Log Server

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 below appears:



Search Options

● New search

○ Search last results

○ Search excluding last results

Server List: 172.17.17.11

Priority List: Least, Less, Most

Start date: 2008-03-14 Start time: 13:15:19 End date: 2008-03-15 End time: 13:15:19

```
Server: 10.0.13.54
   03/15/2008(12:01:34) : Loading system setting
   03/15/2008(12:01:34) : DHCP: Discovering...
   03/15/2008(12:01:34) : DHCP: Requesting...
   03/15/2008(12:01:34) : DHCP: Requesting...
   03/15/2008(12:01:34) : DNS server 1 : 10.0.1.23
   03/15/2008(12:01:34) : Accept new IP : 10.0.13.54
   03/15/2008(12:07:49) : User from 00-01-29-5C-13-9A 10.0.8.150 scanning port = 445.
   03/15/2008(12:07:52) : User from 00-01-29-5C-13-9A 10.0.8.150 scanning port = 445.
```

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

Item	Description
Search Options	**New search:** When selected, the search is performed on all the events in the database for the selected B051-000. **Search last results:** This is a secondary search performed on the events that resulted from the last search. **Search excluding last results:** This is a secondary search performed on all the events in the database for the selected B051-000 *excluding* the events that resulted from the last search.
Server List	B051-000 units are listed 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	Sets the level for how detailed the search results display should be. If nothing is selected, all results will display. If all results do display, entries highlighted in red are of high or *Most* important to installations security. Entries highlighted in blue are of medium or *Less* important to installations security. Entries highlighted in black are of low or *Least* important to installations security.
Start Date	Select the date that you want the search to start from. The format follows the MM/DD/YYYY convention. (e.g. 11/15/2018)
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 at. The format follows the MM/DD/YYYY convention. (e.g. 11/15/2018)
End Time	Select the time that you want the search to end at.
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 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 Log Server search results as a text file.
Exit	Click this button to exit the Search dialog box.

Maintenance

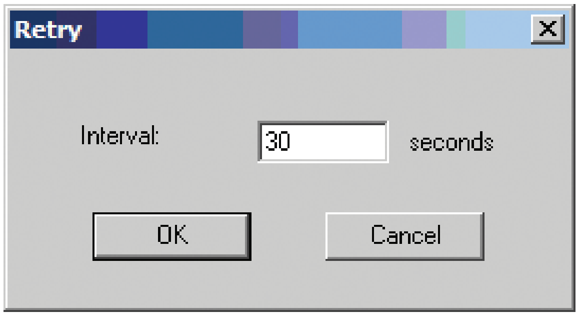
This function allows the administrator to remove all records that have passed their expiration limit. (See *Configure* under *The Log Server* for limit details) In order to delete old files from the log server, the maintenance function must be performed.

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 if the previous connection attempt failed. When you click this item, a dialog box similar to the one below appears:



Interval: 30 seconds

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

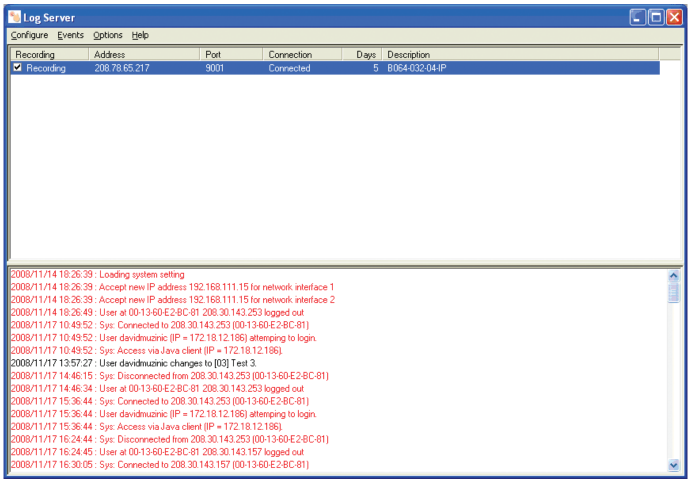
Selecting the Contents function brings up an online Windows Help file. The Help file contains instructions on how to set up, operate and troubleshoot the Log Server.

About Log Server

Selecting the *About Log Server* option brings up a dialog box that displays the version number of the Log Server.

The Log Server Main Screen — Overview

The Log Server Main Screen is divided into two main panels: an upper (List) panel that displays all devices that have been added to the Log Server and a lower (Event) panel that displays the log events for the currently selected B051-000. To select a B051-000 in the list, simply click on it.



Recording	Address	Port	Connection	Days	Description
☑ Recording	208.78.65.217	9001	Connected	5	B064-032-04-IP

```
2008/11/14 18:26:39 : Loading system setting
2008/11/14 18:26:39 : Accept new IP address 192.168.111.15 for network interface 1
2008/11/14 18:26:39 : Accept new IP address 192.168.111.15 for network interface 2
2008/11/14 18:26:49 : User at 00-13-60-E2-BC-81 208.30.143.253 logged out
2008/11/17 10:49:52 : Sys: Connected to 208.30.143.253 (00-13-60-E2-BC-81)
2008/11/17 10:49:52 : User davidmuzinic (IP = 172.18.12.186) attemping to login.
2008/11/17 10:49:52 : Sys: Access via Java client (IP = 172.18.12.186).
2008/11/17 13:57:27 : User davidmuzinic changes to [03] Test 3.
2008/11/17 14:46:15 : Sys: Disconnected from 208.30.143.253 (00-13-60-E2-BC-81)
2008/11/17 14:46:34 : User at 00-13-60-E2-BC-81 208.30.143.253 logged out
2008/11/17 15:36:44 : Sys: Connected to 208.30.143.253 (00-13-60-E2-BC-81)
2008/11/17 15:36:44 : User davidmuzinic (IP = 172.18.12.186) attemping to login.
2008/11/17 15:36:44 : Sys: Access via Java client (IP = 172.18.12.186).
2008/11/17 16:24:44 : Sys: Disconnected from 208.30.143.253 (00-13-60-E2-BC-81)
2008/11/17 16:24:45 : User at 00-13-60-E2-BC-81 208.30.143.157 logged out
2008/11/17 16:30:05 : Sys: Connected to 208.30.143.157 (00-13-60-E2-BC-81)
```

The Log Server

The List Panel

The List panel contains the following fields:

Field	Description
Recording	Determines whether the Log Server records log events for the corresponding B051-000. If the Recording check box is checked, the field displays Recording, and log events are recorded. If the *Recording* check box is not checked, the field displays *Paused*, and log events are not recorded. ***Note:*** *Even if a B051-000 is not currently selected, if its Recording check box is checked, the Log Server will still record its log events.*
Address	This is the IP Address or DNS name that was given to the B051-000 when it was added to the Log Server.
Port	This is the port number that was assigned to the B051-000 when it was added to the Log Server.
Connection	If the Log Server is properly connected to the B051-000, this field displays *Connected*. If it is not connected, this field displays *Waiting*. This means that the Log Server is not communicating with the B051-000, and will not record its events. This occurs when the Log Server's MAC address and/or port number have not been set properly. The MAC Address and Port for the Log Server computer must be entered into the ANMS page. In addition, the B051-000's IP Address and Port must be entered when adding it to the Log Server. If the Port numbers in the B051-000 and the Log Server do not match, they will not be able to communicate.
Days	This field displays the number of days that the B051-000's log events are to be kept in the Log Server's database before it is eligible for deletion.
Description	This field displays the descriptive information given for the B051-000 when it was added to the Log Server.

The Event Panel

The lower panel displays event information for the currently selected B051-000.

General Operation Troubleshooting

Problem	Action
Erratic Operation.	Power off the installation and power everything on according to the installation instructions in this manual. •Reset the unit by pressing and holding the Reset button on the front of the unit for longer than three seconds.
I can't access the B051-000, even though I have specified the IP address and port number correctly.	If the B051-000 is behind a router, the router's Port Forwarding (also referred to as Virtual Server) feature must be configured.
Mouse and/or Keyboard not responding.	•If accessing the unit via local console, unplug and replug the cable(s) from the console port(s). •Turn the connected computer/server off and then back on. All connected devices need to be powered off when connecting to the unit.
Sudden loss of network connection.	Close your B051-000 connection. Wait approximately 30 seconds, and log in again.
No video display on the remote console.	Make sure the resolution of the monitor being used to display the remote computer/server is higher than that of the remote computer/server.
When logging in from a browser, the following message appears: 404 Object Not Found.	If a login string has been set (see *Login String* section in this manual for details), make sure to include the forward slash and correct login string when you specify the B051-000 IP address.
When I log in, the browser generates a CA Root certificate is not trusted or a Certificate Error response.	The certificate can be trusted; you can proceed.
There are two mouse pointers after the remote system is accessed.	The B051-000 automatically defaults to show both the local and remote mouse pointers. You can choose to display both mouse pointers at the same time or only the remote mouse pointer. (See *Mouse Pointer* section in this manual for details.)
The display on the remote console is distorted, and performing an Autosync doesn't resolve the problem.	•Switch ports to a port with a different resolution and then switch back. •Lower the resolution and refresh rate for the computer/server connected to the port.
I have been given an account, but I am unable to log in.	•Make sure that you have correctly entered your username and password. •Make sure that your System Administrator has given you proper access to the unit.
The Lock LEDs on the Control Panel do not accurately portray my Lock status.	Click the LEDs on the *Control Panel* until they match those on your keyboard. Once matched up, changing a Lock LED on the keyboard will also change it in the *Control Panel* and vice versa.
When I open a viewer, the web page does not display properly, and I receive an error message that says "Problems with this Web page might prevent it from being displayed properly…."	•By default, IE6 and some versions of IE5 use the High security level for the Restricted Sites zone. Windows Server 2003 uses High security for the Restricted Sites and Internet zones. You may need to enable Active Scripting, ActiveX Controls and Java Applets. To do so: 1) In IE, open the *Tools* menu, and select *Internet Options*. 2) Click *Security*. 3) Click *Default Level*, and then *OK* when prompted •Verify that Active Scripting, ActiveX Controls and Java Applets are not blocked. If some client computers work and others don't, verify that IE or other programs on your client computer are not configured to block. •Verify your anti-virus program is not set to scan the Temporary Internet Files or Downloaded Program Files folders. •Delete all temporary internet-related files by following these steps: 1) In IE, open the *Tools* menu, and select *Internet Options*. 2) Click the *General* tab. 3) Under *Temporary Internet Files*, click *Settings*. 4) Click *Delete Files*, then *OK* when prompted. 5) Click *Delete Cookies*, then *OK* when prompted. 6) Under *History*, click *Clear History*, then *Yes* and *OK* when prompted •Make sure you have the latest versions of Microsoft DirectX and Java installed.
When the remote server is running Fedora, the mouse pointer is unresponsive, whether I am accessing it via the local console or a remote session.	If the remote server is connected using the PS/2 KVM cable kit, *Mouse Sync Mode* must be set to manual. (See the *Mouse Sync Mode* section in this manual for details)

Administration Troubleshooting

Problem	Action
After upgrading the firmware and logging back in, the B051-000 appears to still be using the old firmware version.	Clear your browser's cache. Delete all temporary internet files and cookies. Close the browser and reopen it to log in with a new session.

Mouse Troubleshooting

Problem	Action
My mouse and/or keyboard is not responding.	•Turn off the computer/server you are having trouble with. Turn the computer/server back on.
Mouse movement is extremely slow.	There is too much data going through your connection. •If the remote computer's wallpaper has a lot of graphics, switch it to a plain wallpaper. •Adjust your video settings to reduce the amount of data per the instructions in the *Video Setting*s section of this manual. •Refer to the *Mouse Synchronization Procedure*s section in this manual.
There are 2 mouse pointers on my screen. How do I fix this?	You can choose between 3 different pointer types. See *Mouse Pointer section* in this manual.
My mouse pointers don't sync.	See *Mouse Synchronization Procedure*s section in this manual.

Virtual Media Troubleshooting

Problem	Action
There is no Virtual Media icon on my control panel.	•Make sure that your System Administrator has given you access to the *Virtual Media* functionality.
I can't boot my remote server from my Virtual Media drive.	Your remote server's BIOS may not support booting from a USB drive. Check to see if there is a new firmware and BIOS version for the mainboard that does support USB.
If I connect a USB floppy drive to a remote server, it can boot the remote server; however, if I map it to the remote server as a Virtual Media drive, it cannot boot the remote server.	USB floppy drives have two types of format: UFI and CBI. Both can be used for OS level Virtual Media functions, but only UFI is currently supported for BIOS level, which includes boot functions.
I cannot mount a Folder as a Virtual Media device.	If the folder is formatted with the FAT16 file system, it must be less than 2 Gb to be mounted.
When using the Virtual Media functionality, I can mount an ISO file, but I am unable to access it.	Only ISO files that are less than 4 Gb are supported. Anything 4 Gb or larger will not be accessible.

AP Windows Client Troubleshooting

Problem	Action
Windows Client won't connect to the B051-000.	DirectX 8.0 or higher must be installed on your computer.
Part of remote window is off my monitor.	•If Keep Screen Size is not enabled (see *Screen Mode* section in this manual for details), try performing a Video Auto Sync (see *Video Setting*s section) to sync the local and remote monitors. If this does not work, you may have to manually adjust the Screen Position in the Video Settings screen. •If Keep Screen Size is enabled, areas that are off the screen can be accessed by positioning the mouse pointer on the far side of the area you want to scroll to.
The remote screen is rotated 90 degrees.	Enable Keep Screen Size (See Keep Screen Size section).
I cannot run Net Meeting when the Windows Client is running.	Enable Keep Screen Size (See Keep Screen Size section).
My B051-000 is not showing up in the device list when I open the AP Windows Client.	•The port number entered into the *Program* field of the *Network* page must match the port number entered into the AP Windows Client's *Port* field. Only B051-000s that match the port number entered into this field will show up in the device list. •The *Enable Device* List option must be checked on the *Customization* page for your B051-000 to show up in the Device List.
After upgrading the firmware to my B051-000, the AP Windows Client no longer works.	The old version of your .ocx file was not deleted. Open *Explorer* and search for *WinClient.ocx*. Delete all occurrences.

WinClient ActiveX Viewer Troubleshooting

Problem	Action
The WinClient ActiveX Viewer will not connect to the B051-000.	DirectX 8.0 or higher must be installed on your client computer.
After upgrading the firmware to my B051-000, the WinClient ActiveX Viewer no longer works.	The old version of your .ocx file was not deleted. Open *Internet Explorer > Tools > Manage Add-ons*. Delete or disable all occurrences of *WinClient*.
Part of the remote window is off my monitor.	•If Keep Screen Size is not enabled (see *Screen Mode* section under *Remote Session Operation*), try performing a Video Auto Sync (see *Video Settings* section). If this does not work, you may have to manually adjust the video via the *Video Settings* page. •If Keep Screen Size is enabled, areas that are off the screen can be accessed by positioning the mouse pointer on the far side of the area you want to scroll to.
The remote screen is rotated 90 degrees.	Enable the *Keep Screen Size* function. (See *Keep Screen Size* section for details.)
I cannot run Net Meeting when the WinClient is running.	Enable the *Keep Screen Size* function. (See *Keep Screen Size* section for details.)
After logging in, I can't open the WinClient ActiveX viewer.	•You don't have the authority to install the *WinClient Control Add-on* on your client computer. Have your system administrator run the program for you the first time. •Under Vista and 7, you must also add the B051-000's URL to the list of trusted sites. Go to *Tools > Internet Options > Security > Trusted Sites > Sites.*
When using Vista or 7, I open the WinClient ActiveX Viewer and try to mount a driver or removable disk, but I am getting a message that says "Driver not ready."	This is due to User Account Control (UAC). If you are the computer's administrator, open your browser by right-clicking on it and selecting *Run as Administrator*. If you are not the administrator, you will need to have the administrator disable UAC.
My antivirus program reports that there is a Trojan when I use the web browser Windows Client.	The web browser Windows Client uses an Active X plugin that some antivirus programs identify as a virus or Trojan. We have thoroughly tested our software and have found no evidence of a virus or Trojan, and therefore recommend it safe for use. You can either continue using the Windows Client and add it to your antivirus programs White List, or you can use the Java Client instead.

Java Applet & AP Java Client Troubleshooting

Problem	Action
The AP Java Client won't connect to the B051-000.	•Java Runtime Environment 6, Update 3 or higher must be installed on your computer. •If a login string has been set, make sure to include the forward slash and correct string (see *Login String* section for details) when you specify the IP address. •Make sure you have been given access to the Java Client by your administrator. •Try closing the Java client and opening it again.
Pressing the Windows Menu key has no effect.	Java doesn't support the Windows Menu key.
Java Client performance deteriorates.	Exit the program and start again.
After upgrading the firmware of my KVM switch and logging into the OSD, my switch is still showing the old firmware version number.	You need to delete your Java temporary internet files. Open *Control Panel > Java*, and click on the *Settings* button in the *Temporary Internet Files* section. In the *Disk Space* section, click on *Delete Files*. When prompted, click *OK*.
When I try to add a folder to be mounted as a Virtual Media Drive, I am unable to select the folder. The only option I have is desktop.	In the folder selection entry field, enter the root directory of the folder you want to add. After that, the folders contained under the root directory will be displayed.

Log Server Troubleshooting

Problem	Action
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows versions through 10. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com/data/download.htm to retrieve the driver file: MDAC 2.7 RTM Refresh (2.70.9001.0) Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Appendix

Sun Systems Troubleshooting

Problem	Action
Video display problems with HD15 interface systems (e.g. Sun Blade 1000 servers).*	•The display resolution should be set to 1024 x 768 @ 60 Hz: **Under Text Mode** go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all **Under XWindow:** 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
Video display problems with 13W3 interface systems. (e.g. Sun Ultra servers)*	•The display resolution should be set to 1024 x 768 @ 60 Hz: **Under Text Mode** go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all **Under XWindow:** 1. Open a console and issue the following command: ffbconfig -res 1024x768x60 2. Log out 3. Log in
The local and remote mouse pointers do not sync.	See Manual Mouse Synchronization section.

* These solutions work for most common Sun VGA cards. If using them fails to resolve the problem, consult the Sun VGA card's manual.

Keyboard Emulation

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

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.*

Specifications

Feature	Specification
PC/KVM Port	HD18 Female
PS/2 – USB Console Port	HD18 Female
RS-232 Port	DB9 Male
Power	DC Jack
LAN	RJ45 Female
Laptop USB Console (LUC)	USB 5-Pin Mini-B Female
Max Video Resolution	1920 x 1080 @ 60 Hz; DDC2B
Power Consumption	DC 5.3V, 13W
Operating Temperature	0 to 40 C (32 to 104 F)
Storage Temperature	-20 to 60 C (-4 to 140 F)
Humidity	0 to 80% RH, Non-Condensing
Dimensions (H x W x D)	0.98 x 7.95 x 3.2 in. (2.5 x 20.2 x 8.1 cm)
Weight	1.1 lb. (0.5 kg)

Warranty and 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.

3-Year Limited Warranty

TRIPP LITE warrants its products to be free from defects in materials and workmanship for a period of three (3) years 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

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.

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.

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.

Manufacturing
Excellence.

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