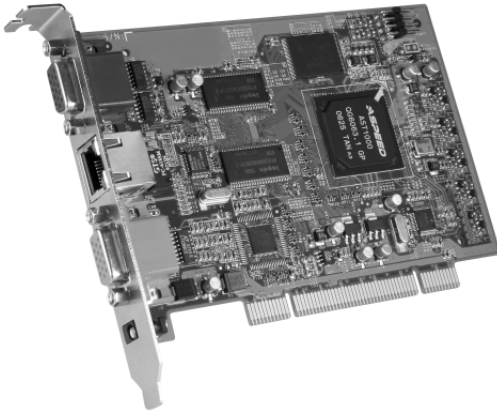# Remote Management PCI Card
IP8000
User Manual

www.aten.com

FCC Information

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

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

RoHS

This product is RoHS compliant.

SJ/T 11364-2006

The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

○: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。

●: 表示符合欧盟的豁免条款，但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

✕: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

User Information

Online Registration

Be sure to register your product at our online support center:

International		http://support.aten.com
North America	ATEN TECH	http://www.aten-usa.com/product_registration
	ATEN NJ	http://support.aten.com

Telephone Support

For telephone support, call this number:

International		886-2-8692-6959
North America	ATEN TECH	1-888-999-ATEN
	ATEN NJ	1-732-356-1703

User Notice

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

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

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

Package Contents

The IP8000 package consists of:

- 1 IP8000 Remote Management PCI Card
- 1 Custom KVM Cable Set
- 1 Feature Cable
- 1 Power Adapter
- 1 Software CD
- 1 User Manual*
- 1 Quick Start Guide

Check to make sure that all the components are present and that nothing got damaged in shipping. If you encounter a problem, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit, and/or any of the devices connected to it.

---

* Features may have been added to the IP8000 since this manual was printed. Please visit our website to download the most up-to-date version of the manual.

Contents

About this Manual

This User Manual is provided to help you get the most from your IP8000. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the IP8000. Its purpose, features and benefits are presented, and its components are described.

Chapter 2, Hardware Setup, provides step-by-step instructions for connecting up your installation.

Chapter 3, Browser Login, describes how to log into the IP8000 with a browser, and explains the functions of the icons and buttons that appear on the opening web page.

Chapter 4, Administration, explains the administrative procedures that are employed to configure the IP8000's working environment.

Chapter 5, The Windows Client, explains how to connect to the IP8000 with the browser-based Windows Client software, and describes how to use the OSD to access and control the server that the card is installed in.

Chapter 6, The Java Applet, describes how to connect to the IP8000 with the Java Applet software, and explains how to use the OSD to access and control the server that the card is installed in.

Chapter 7, The Log File, shows how to use the log file utility to view the events that take place on the IP8000.

Chapter 8, The Log Server, explains how to install, configure, and use, the Log Server

Chapter 9, AP Operation, describes how to configure and operate the IP8000 using the stand-alone Windows and Java AP programs, instead of the browser.

An Appendix, at the end of the manual provides technical and troubleshooting information.

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
⚠	Indicates critical information.

Product Information

For information about all ATEN products and how they can help you connect without limits, visit ATEN on the Web or contact an ATEN Authorized Reseller. Visit ATEN on the Web for a list of locations and telephone numbers:

International		http://www.aten.com
North America	ATEN TECH	http://www.aten-usa.com
	ATEN NJ	http://www.aten.com

Introduction

Overview

The IP8000 is a PCI card implementation of a control unit that provides "over-IP" access and control of the server it is installed in. In addition to local console operation, the IP8000 allows multi-platform access and control of the server from remote locations using a standard Internet browser or with a stand-alone Windows-based application.

The IP8000 installs in any available PCI slot, then connects to the Internet, an Intranet, LAN, or WAN using industry standard Category 5 cable. Because the IP8000 uses TCP/IP for its communications protocol, the server it is connected to can be accessed from any computer on the Net - whether that computer is located down the hall, down the street, or half-way around the world.

For ease of operation, a user-friendly *Windows GUI Client* and a *Java Applet* are available in browser-based versions. A stand-alone Windows application version is provided, as well. Inclusion of the Java applet ensures that the IP8000 is platform independent, and is able to work with all operating systems.

Operators at remote locations connect to the IP8000 via its IP address. Once a connection has been established and authorization granted, remote users can exchange keyboard, video and mouse signals with the server just as if they were physically present and working on the equipment directly.

Administrator utilities are provided to configure the system; limit access from remote computers; manage users; and maintain the system with firmware and software module updates. In addition, a *Log Server* records all the events that take place on the IP8000 for the administrator to analyze.

System administrators can handle a multitude of tasks with ease - from installing and running GUI applications, to BIOS level troubleshooting, routine monitoring, maintenance, system administration, rebooting and even pre-booting functions.

Your IP8000 investment is protected by a *Firmware Upgrade Utility*. You can stay current with the latest functionality improvements by downloading firmware update files from our website as they become available, and then using the utility to quickly and conveniently perform the upgrade.

Features

- Standard PCI-sized card provides over-IP access and control of a remote server from anywhere in the world

- Virtual media via USB 2.0 data transmission

- Remote power control and reset support

- Up to 64 user accounts – Up to 32 concurrent user logins for single-bus sharing

- Message board feature allows logged in users to communicate with each other, and allows a user to take exclusive control of the KVM functions

- External authentication support: RADIUS

- Web-based Windows and Java implementations allow the server to be controlled from any browser.

- Windows GUI and Java client software for non-browser access – the Java client works with practically all operating systems

- Supports TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP

- Supports 10Base-T, 100Base-T

- Superior video resolution: up to 1600 x 1200 @ 60Hz; 24-bit color depth for remote sessions

- Bandwidth optimization via grayscale and video quality setting

- Advanced security features include password protection and advanced encryption technologies

- Secure 128-bit SSL encryption

- Enable/disable browser operation

- Three level authentication: Multi- Administrators, Users, Viewers

- Event logging

- Remote firmware upgrading

- Host-side OS support: Windows 2000/2003/XP/NT; Redhat 7.1 and above; FreeBSD, Novell

System Requirements

General

- For best results we recommend that the computers used to access the IP8000 control unit have at least a P III 1 GHz processor, and that the screen resolution is set to 1024 x 768.

- Browsers must support 128-bit SSL data encryption.

- For best results we recommend that the internet connection speed be at least 128 kbps.

- For the browser-based Java Applet and AP Java Client, you must have Sun's Java Runtime Environment (JRE) 6, Update 3, or higher.

- For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.

Video

Only **non-interlaced** video signals at the following resolutions and refresh rates are supported:

Resolution	Refresh Rates
640 x 480	60, 72, 75, 85, 90, 100, 120
720 x 400	70, 75
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 1024	60, 70, 75
1600 x 1200	60

Cables

* Two cable sets are provided with this package: a KVM cable set to link the IP8000 to a server; and a feature cable to link the IP8000 to the mainboard power control header.

Note: Only cable sets specifically designed to work with the IP8000 may be used for the above purposes.

---

* Cat 5 or higher cable should be used to connect the IP8000 to the LAN, WAN, or Internet.

Operating Systems

Supported operating systems are shown in the table, below:

OS	Version	
Windows	2000 and higher	
Linux	RedHat	7.1 and higher
	SuSE	8.2 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	4.2 and higher
Novell	Netware	5.0 and higher

Virtual Media Support

* USB CDROM Drives
* USB Floppy Drives
* USB Flash Drives
* IDE CDROM Drives
* Image Files

IP8000 Layout Diagram
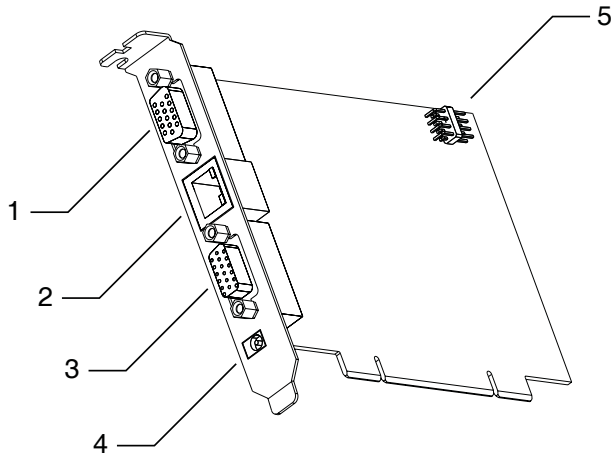
No.	Component	Description
1.	Monitor Port	The video cable from your monitor plugs in here
2.	LAN Port	The cable that connects to the WAN, LAN, Intranet, or Internet plugs in here.
3.	KVM Port	The Custom KVM cable that links the card to your server's Video and USB ports plugs in here.
4.	Power Jack	The power adapter cable plugs in here. **Note:** Use of the power adapter is optional. If it is not used, however, you will be unable to perform a remote Power On.
5	Feature Cable Connector	The feature cable plugs in here. See *Feature Cable Installation*, page 9 for details.

This Page Intentionally Left Blank

Chapter 2
Hardware Setup

Before You Begin

⚠

1. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.

2. Avoid Electrostatic Discharge (ESD). Keep your IP8000 card in its antistatic bag until it is ready to be installed. Avoid contact with any component or connector on any adapter card, printed circuit board, or memory module. Handle these components by the mounting bracket.

3. Perform all unpacking and installation procedures on a ground connected antistatic mat. Wear an antistatic wristband grounded at the same point as the antistatic mat. You can also use a sheet of conductive aluminum foil grounded through a one megaohm resistor instead of the antistatic mat. Similarly, a strip of conductive aluminum foil wrapped around the wrist and grounded through a one megaohm resistor serves the same purpose as a wristband.

Basic Installation

After installing the IP8000 into any available PCI slot on the server's mainboard, refer to the installation diagram below (the diagram numbers correspond to the step numbers), and do the following:

1. Plug the local monitor cable into the IP8000's video port.

2. Plug the local keyboard and mouse into the server's keyboard and mouse ports.

Note: The installation diagram depicts a PS/2 Mouse and Keyboard. If you use USB mice and keyboards, plug them into USB ports.

7

3. Use the *KVM Cable* provided with this package to connect the IP8000's KVM port to the server's video port and USB port.

4. Plug the LAN or WAN cable into the IP8000's LAN port.

5. Plug the power adapter cable into the IP8000's power jack, then plug the power adapter into an AC power source.

> **Note:** Use of a power adapter is optional. If a power adapter isn't used, however, you will not be able to perform a remote Power On.
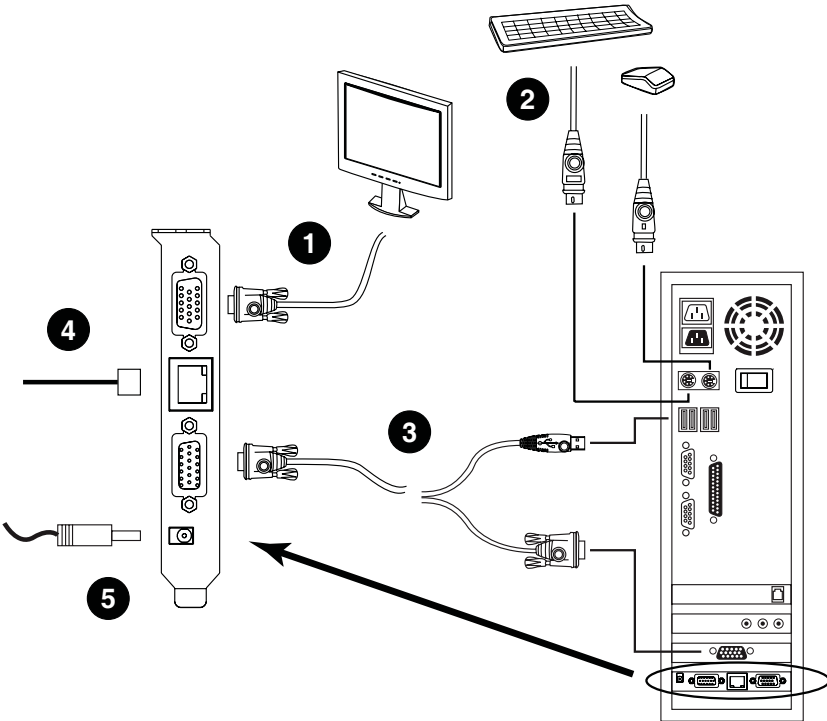

> **Note:** Although the IP8000 plugs into a server's PCI slot, it has its own environment and operates independently of the server it resides on – using its I/O ports to link to the server it controls. It can even link to (with steps 2 and 3), and control, a server other than the one it actually resides on.

Feature Cable Installation

The feature cable provides the ability to perform remote power on/off and reset operations. The cable plugs into a header block located at the upper right of the card. The block contains two rows of pins. The upper row comprises pins 1, 3, 5, and 7; the lower row comprises pins 2, 4, 6, and 8. To install the feature cable, do the following:

1. Plug the feature cable's large connector (the one containing all 4 wires) into to the *lower* row of pins (pins 2–8) with the white wire at the top; the orange wire at the bottom.

2. Unplug the leads from the computer mainboard's *Reset* pin header. (These are the ones coming from the computer case's Reset switch).

3. Plug the feature cable connector containing the white and blue wires into the mainboard's *Reset* pin header.

4. Unplug the leads from the computer mainboard's *Power* pin header. (These are the ones coming from the computer case's Power switch).

5. Plug the feature cable connector containing the white and orange wires into the computer mainboard's Power header.
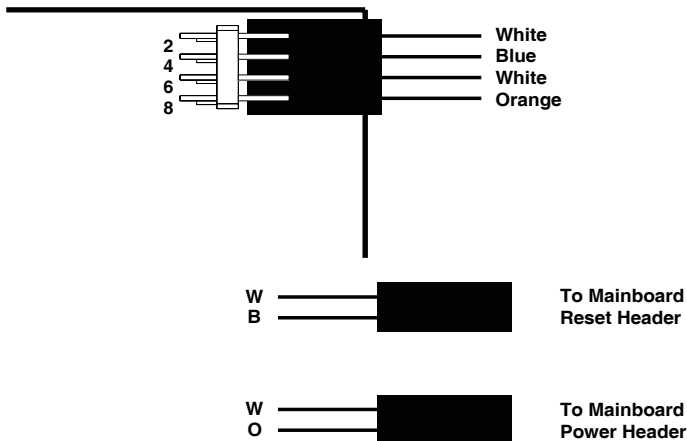
(Continues on next page.)

(Continued from previous page.)

6. Plug the leads from computer case's Reset switch into pins 1–3 (on the upper row) of the IP8000's feature cable pin header.

7. Plug the leads from the computer case's Power switch into pins 5–7 (on the upper row) of the IP8000's feature cable pin header.

```
1
3          From Case
5          Reset Switch
7          From Case
           Power Switch
```
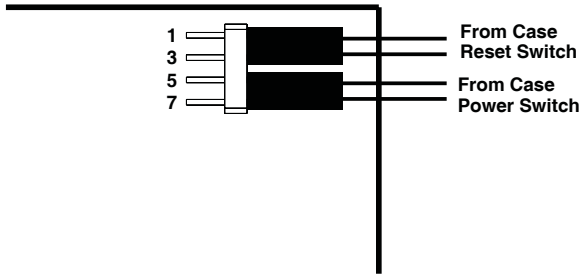
Note: It is not necessary to pay attention to the plug alignment (i.e., which wire is aligned with which pin) when you plug the leads from the feature cable into the mainboard headers, or when you plug the leads from the case into the feature cable header.

Browser Login

The IP8000 can be accessed either from an internet type browser, or via stand-alone Windows and Java applications. The next several chapters describe browser-based operations. Stand-alone AP operation is discussed in Chapter 9.

Logging In

To operate the IP8000 from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the IP8000 you want to access in the browser's URL location bar.

   Note: 1. 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 along with the IP address when you log in. For example:

   ```
   192.168.0.100/ip8k
   ```

   If you don't know the IP address and login string, ask your Administrator.

   2. If you are the administrator, and are logging in for the first time, the various ways to determine the IP8000's IP address are described in the Appendix on page 83.

(Continues on next page.)

(Continued from previous page.)

2. A *Security Alert* dialog box appears.

Accept the certificate – it can be trusted. (See *Trusted Certificates*, page 91, for details.) If a second certificate appears, accept it as well.

The IP8000 login page appears:

3. Provide a valid Username and Password (set by the IP8000 administrator), then Click **Login** to continue.

> **Note:** 1. If you are the administrator, and are logging in for the first time, use the default Username: *administrator*; and the default Password: *password*. For security purposes, we strongly recommend you remove these and give yourself a unique Username and Password (see *User Management*, page 27).
>
> 2. If you supplied an invalid login, the login entry boxes will become blank. Log in again being careful to specify a valid Username and Password.

13

After you have successfully logged in, the IP8000 Main Screen appears:

Screen Elements

The Main Screen consists of Utility icons arranged vertically down the left side; Administration icons arranged across the top; and a *Remote Console Preview* with icons to launch the Java Applet and Windows Client displayed in the center.

Note: If a user doesn't have permission to perform a particular activity, the icon for that activity doesn't appear. See *User Management*, page 27, for permission details.

(Continues on next page.)

(Continued from previous page.)

Utility Icons

The icons arranged down the left side perform the following functions:

Icon	Purpose
	Remote Console: Clicking this icon closes whatever is displayed on the Main Screen, and brings back the *Remote Console Preview*.
	Power Management: If the feature cable has been properly installed (see *Feature Cable Installation*, page 9), and you have the proper permission (see *User Management*, page 27), clicking this icon will bring up an interface that allows you to Power On, Power Off, or Reset the remote server.
	Log: All the events that take place on the IP8000 are recorded in a log file. If you have the proper permission (see *User Management*, page 27), clicking this icon displays the contents of the log file. See Chapter 7, *The Log File*, for further details.
	Logout: Click this icon to log out and end your IP8000 session. It is important to log out when you end your session. Otherwise, you must wait until the timeout setting has expired before the IP8000 can be accessed again. (See *Timeout*, page 29.)

Administration Icons

The icons arranged across the top of the page are linked to the administration utilities, which are used to configure the IP8000. The ability to make configuration changes depends on the permissions associated with a user's login information (see *User Management*, page 27). The administrative functions are discussed in Chapter 4.

Remote Console Preview

The main portion of the screen shows a snapshot of the remote display.

The active elements of the *Remote Console Preview* are described in the following table:

Element	Action
Refresh	Clicking *Refresh* updates the snapshot of the remote display.
Open Java Applet	If you are on a platform other than Windows, clicking *Open Java Applet* uses a Java applet to open the remote server's display on your desktop.
Open Windows Client	If you are running Windows, clicking *Open Windows Client* uses a Windows plugin to open the remote server's display on your desktop.

Note: 1. If a user doesn't have permission to open the Java Applet, the icon to launch the applet does not appear.

2. If a user doesn't have permission to open the Windows Client, the icon to launch the client does not appear.

IP8000 operation using the Java applet is discussed in Chapter 6; IP8000 operation using the Windows client is discussed in Chapter 5.

Administration

Introduction

The administration utilities, represented by the icons located across the top of the IP8000 web page, are used to configure the IP8000's operating environment.

This chapter discusses each of them in turn.

Note: 1. As you make your configuration changes in each dialog box, click **Apply** to save them.

2. Some configuration changes only take effect after an IP8000 reset. For those changes, a check is automatically put in the *Reset on Exit* box (see *Customization*, page 29). To have the changes take effect, log out and then log back in again.

3. If you don't have Configuration privileges (see *User Management*, page 27), the Administration configuration dialogs are not available.

General

The *General* page is the first of the Administration pages, and provides information about the IP8000's status.

An explanation of each of the screen items is given in the table below:

Item	Explanation
Device Name:	To make it easier to manage installations that have more than one IP8000, each one can be given a name. To assign a name for the IP8000, key in one of your choosing here (16 characters max.).
MAC Address:	The IP8000's MAC Address displays here.
Firmware Version:	Indicates the IP8000's current firmware version level. New versions of the IP8000's firmware can be downloaded from our website as they become available (see *Firmware*, page 31). You can reference this number to see if there are newer versions available on the website.
Last IP from DHCP Server	If the IP8000 is on a network that uses DHCP assigned IP addresses, this item is a convenient way of ascertaining what its IP address is, in order to inform the Users which IP to use when they log in. **Note:** If the switch has a fixed IP address, this item doesn't appear.

Network

The Network dialog is used to specify the IP8000's network environment.

Access Ports

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. Users must specify the port number as part of the IP address If an invalid port number (or no port number) is specified, the IP8000 will not be found. An explanation of the fields is given in the table below:

Field	Explanation
Program:	This is the port number used for keyboard, mouse, video, and message data transfers. Valid entries are from 1024–65535. The default is 9000.
Virtual Media:	This is the port number used for data transfer using the IP8000's virtual media feature. Valid entries are from 1024–65535. The default is 9003.
HTTP:	The port number for a browser login. Valid entries are from 1–65535. The default is 80.
HTTPs:	The port number for a secure browser login. Valid entries are from 1–65535. The default is 443.

Note: The access ports cannot have the same value. You must set a different value for each one.

IP Address

The IP8000 can either have its IP address assigned dynamically at bootup (DHCP), or it can be given a fixed IP address.

◆ For dynamic IP address assignment, select the *Obtain an IP address automatically*, radio button.

> **Note:** If the IP8000 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 83, for information.

◆ To specify a fixed IP address, select the *Set IP address manually*, radio button and fill in the IP address.

DNS Server

The IP8000 can either have its DNS server address assigned automatically, or a fixed address can be specified.

◆ For automatic address assignment, select the *Obtain DNS server address automatically*, radio button.

◆ To specify a fixed address, select the *Use the following DNS server address*, radio button and fill in the required information.

> **Note:** Specifying the Primary DNS Server address is required; the Alternate DNS Server address is optional.

Finishing Up

After making any network changes, be sure *Reset on exit* on the *Customization* page (see *Customization*, page 29) has been enabled (there is a check in the checkbox), before logging out. This allows network changes to take effect without having to power the IP8000 off and on.

Security

The Security page controls access to the IP8000.
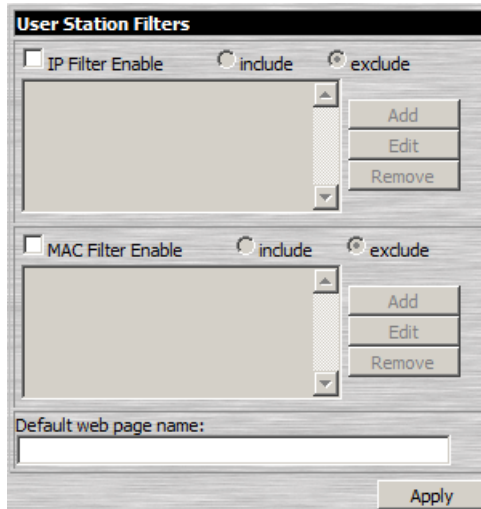
Overview

◆ *IP* and *MAC Filters* control access to the IP8000 based on the IP and/or MAC addresses of the computers attempting to access the system. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.

◆ The *Default web page name* lets the Administrator specify a login string (in addition to the IP address) that users must include when they access the IP8000 with a browser. For example:

```
192.168.0.126/abcdefg
```

Users must include the forward slash and the string when they specify the IP address in the browser's URL bar. For security purposes, we recommend that you change this string from time to time.

Note: If no string is specified here, anyone can access the IP8000 with a Web browser using the IP address alone. This makes the installation less secure.

Filtering

To enable IP and/or MAC filtering, **Click** to put a check mark in the *IP Filter Enable* and/or *MAC Filter Enable* checkbox. There are a maximum of 100 filters allowed for each.

◆ If the *include* button is checked, all the addresses within the filter range are allowed access; all other addresses are denied access.

◆ If the *exclude* button is checked, all the addresses within the filter range are denied access; all other addresses are allowed access.
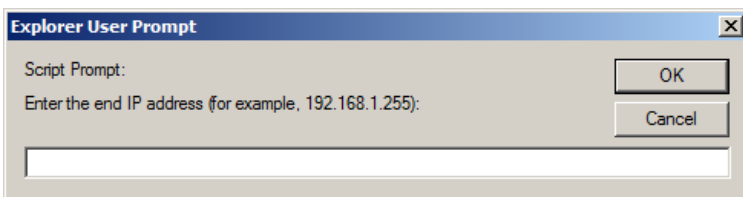
IP Filtering

To add an IP filter:

1. Click **Add**. A dialog box similar to the one below appears:
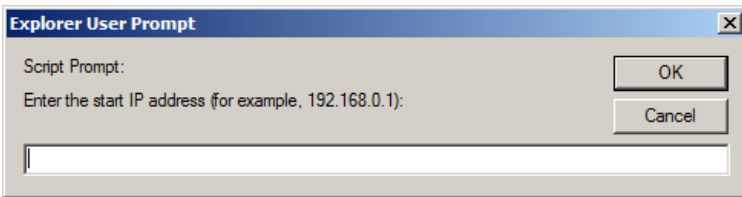
2. Specify the filter address in the dialog box, then Click **OK**.

   A second dialog box, similar to the one below, appears:

3. To filter a single IP address, key in the same address as the start IP. To filter a continuous range of addresses, key in the end number of the range.

4. After filling in the address, click **OK**.

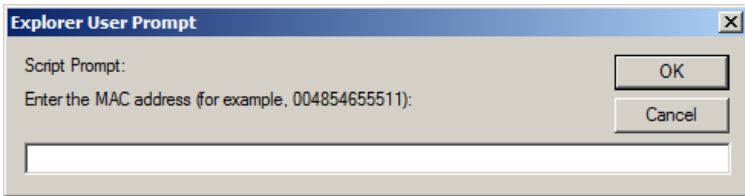5. Repeat these steps for any additional IP addresses you want to filter.

To delete a filter, select it and Click **Remove**.

To modify a filter, select it and Click **Edit**. The *Edit* dialog box is similar to the *Add* dialog box. When it comes up, simply delete the old address and replace it with the new one.

MAC Filtering

To add a MAC filter:

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

2. Specify the MAC address in the dialog box, then Click **OK**.

3. Repeat these steps for any additional MAC addresses you want to filter.

To delete a filter, select it and Click **Remove**.

To modify a filter, select it and Click **Edit**. The *Edit* dialog box is similar to the *Add* dialog box. When it comes up, simply delete the old address and replace it with the new one.

ANMS

The Advanced Network Management Settings dialog box allows you to set up login authorization management from a external sources. It is divided into three main panels, as described, below:

RADIUS Settings

To allow authorization for the IP8000 through a RADIUS server, do the following:

1. Check **Enable RADIUS**.

2. Fill in the IP addresses and Service Ports for the Primary and Alternate RADIUS servers.

3. In the *Timeout* field, set the time in seconds that the IP8000 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* field, key in the character string that you want to use for authentication between the IP8000 and the RADIUS Server.

(Continues on next page.)

(Continued from previous page.)

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

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via Java.
P	Allows the user to Power On/Off, Reset the computer that the IP8000 is connected to.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the virtual media function.

Note: 1. The characters are not case sensitive. Upper or lower case work equally well.

2. Characters are comma delimited.

3. An invalid character in the configuration string will prohibit access to the IP8000 for the user.

RADIUS Examples
RADIUS Server access rights examples are given in the table, below::

String	Meaning
c,w,p	User has administrator privileges; user can access the system via the Windows Client; user can manage the attached Power over the NET device.
w,j,l	User can access the system via the Windows Client; user can access the system via the Java Client; user can access log information via the user's browser.

CC Management Settings

To allow authorization for the IP8000 through a CC (Control Center) server, check *Enable CC Management* and fill in the CC Server's IP address and the port that it listens on in the appropriate fields.

Log Server Settings

Important transactions that occur on the IP8000, such as logins and internal status messages, are kept in an automatically generated log file. See Chapter 8, *The Log Server*, for details on setting up the log server.

- Specify the MAC address of the computer that the Log Server runs on in the *MAC address* field.

- Specify the port used by the computer that the Log Server runs on to listen for log details in the *Port* field. The valid port range is 1—65535. The default port number is 9001.

User Management

The User Management dialog box is used to create and manage user profiles.
Up to 64 user profiles can be established.
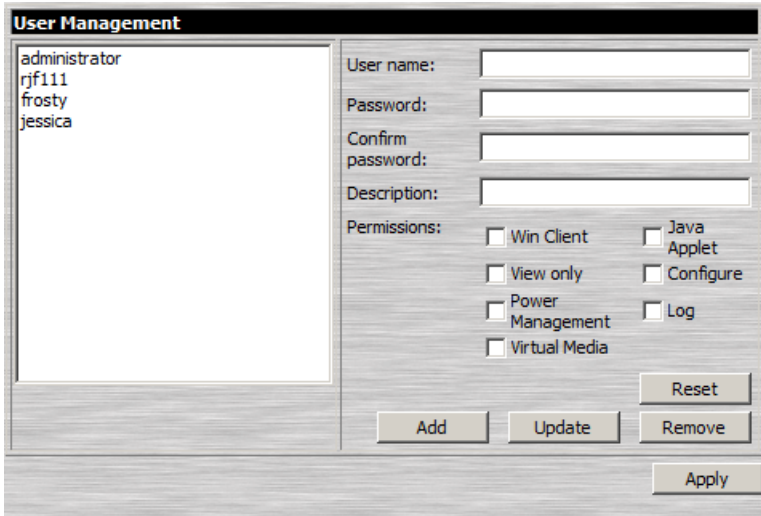
* To add a user profile, fill in the information asked for in the *User Info* panel and click **Add**. The user's name appears in the *User List* panel.

* To delete a user profile, select it from the names displayed in the *User List* panel, and click **Remove**. The user's name is removed from the *User List* panel.

* To modify a user profile, first select it from the list in the upper panel; then change the information that appears in the *User Info* dialog box.

> **Note:** The user's password is not displayed – the *Password* and *Confirm* fields are blank. If you do not want to change the user's password, simply leave the two fields blank. If you do want to change the user's password, key the new password in the *Password* field, then key it in again in the *Confirm* field.

When you have made all your changes, click **Update**.

* The **Reset** button clears all the information shown in the *User Info* fields.

(Continues on next page.)

(Continued from previous page.)

An explanation of the profile items is given in the table below:

Item	Explanation
Username	A minimum of 6 and a maximum of 16 characters is allowed.
Password	A minimum of 6 and a maximum of 16characters is allowed.
Confirm Password	To be sure there is no mistake in the password you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Permissions	Click to place/remove a check mark next to an item to grant/withhold access to that aspect of the IP8000's operation.
	Win Client: Checking *Win client* allows a user to access the IP8000 via the Windows Client software.
	View Only: Checking *View Only* allows a user to view the video of the display of the computers attached to the ports of the KVM switch connected to the IP8000, but they are not allowed to perform any operations on the computers.
	Power Management: Checking *Power Management* allows a user to Power On / Power Off / Reset the computer that the IP8000 is connected to.
	Log: Checking *Log* allows a user to view the contents of the log file.
	Virtual Media: Checking *Virtual Media* allows a user to utilize the IP8000's virtual media capabilities (see *Virtual Media*, page 40 for details).
	Java Applet: Checking *Java Applet* allows a user to access the IP8000 via the Java Applet software.
	Configure: Checking *Configure* gives a user Administrator privileges, and allows the user to set up and modify the IP8000's operating environment.

Customization

This configuration dialog allows the Administrator to set *Timeout*, *Login failure*, and *Working mode* parameters.

An explanation of the Customization parameters is given in the table below:

Parameter		Explanation
Timeout		If the IP8000 doesn't receive any input from a computer that is accessing it with the Windows Client or Java Applet for the amount of time specified here, it ends the connection.
Login failures	Allowed	Sets the number of consecutive failed login attempts that are permitted from a remote computer.
	Timeout	*S*ets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures.

*(Continues on next page.)*

(Continued from previous page.)

Item		Explanation
Working Mode	Enable ICMP	If *ICMP* is **enabled**, the IP8000 can be pinged. If it is not enabled, the device cannot be pinged.
	Enable device list	If this item is **enabled**, the device will show up in the list of local IP8000 units (see *Starting Up*, page 66). If it is not enabled, it will not show up.
	Enable browser	Placing a check in this box allows the user to access the IP8000 from a browser. If this function is not enabled, users will not be able to log into the unit via their browsers.
	Enable multiuser	Enabling *Multiuser* operation permits up to 32 users to log into the IP8000 at the same time through any combination of: the browser-based Windows Client, the AP Windows Client, the browser-based Java Applet, and the AP Java Client.
Mouse Sync Mode	Automatic	This is the default. *Automatic* causes an automatic synching of the remote and local mouse pointers when a connection to the remote display is made. **Note:** This feature only supports USB mice on Windows systems. For all other configurations, you must select *Manual*.
	Manual	Selecting Manual means that no automatic mouse pointer synching takes place. All synching must be done manually with the Windows Client and Java Applet synching procedures. (See *Auto-Sync*, page 39, and page 50 and *Adjust Mouse*, page 37). Also see *Additional Mouse Synchronization Procedures*, page 89, for further help, if necessary.
Reset		Some configuration changes only take effect after an IP8000 reset. These include changes on the Network page; a Log Server port change; enabling/disabling browser access; and upgrading the firmware. For those changes, a check is automatically put in the *Reset on Exit* box. To have the changes take effect, log out and then log back in again. A wait of approximately 30 to 60 seconds is necessary before logging in following the reset. **Note:** If the IP8000's performance degrades, reset it by putting a check in the *Reset on Exit* box, and then log out / log in.

Firmware

As new versions of the IP8000 firmware become available, they can be downloaded from our website. Check the website regularly to find the latest information and packages.

To upgrade the firmware, do the following:

1. Download the new firmware file to a computer that is not the one that your IP8000 is installed on.

2. From that computer, open your browser; log in to the IP8000; and click the *Firmware* icon to bring up the *Firmware File* dialog box:
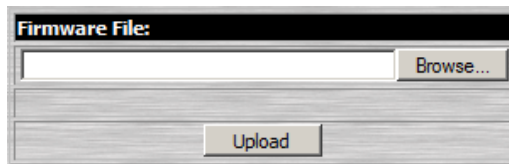
3. Click **Browse**; navigate to the directory that the new firmware file is in and select the file.

4. Click **Upload**.

5. After the upload completes, the *Reset on exit* checkbox
(See *Customization*, page 29) will automatically be enabled. To have the new firmware take effect, click **Logout** at the bottom left of the Main web page to exit and reset the IP8000, then login again.

This Page Intentionally Left Blank

The Windows Client

Starting Up

After you log in (see *Logging In*, page 11), Click the *Open Windows Client* link on the *Remote Console Preview* screen.

Note: 1. The first time you run the Windows client, you are prompted to install a plugin (*ip8000plugin.exe*) that is required for its operation:
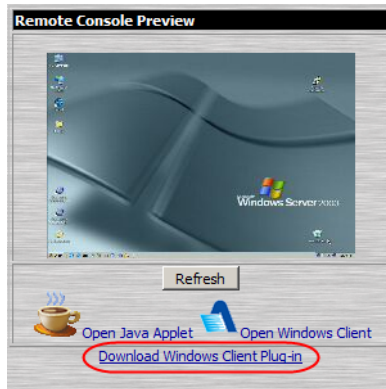
Click the link; in the dialog box that comes up, click **Run**.

If the dialog box doesn't have a *Run* option, click **Save**, then, with the browser still open, run the file.

This brings up the plugin installation wizard. Click **Next** to start the installation, then follow along with the wizard to complete it.

Now, go back to the login screen and click **Open Windows Client** again.

2. To uninstall the plugin, use the Windows *Add or Remove Programs* function (Start → Control Panel → Add or Remove Programs).

(Continued from previous page.)
A second or two after you click the *Open Windows Client* link, the remote server's display appears as a window on your desktop:
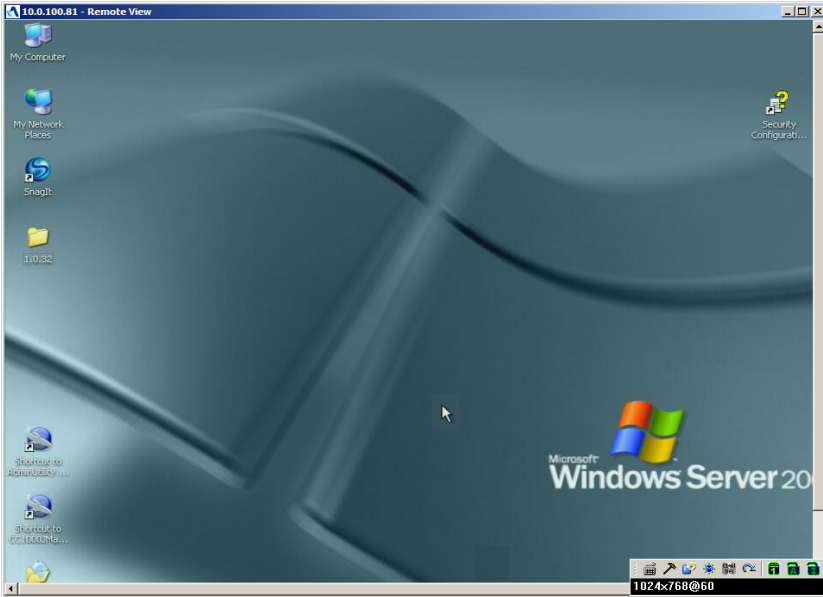
Navigation

You can work on the remote system via the screen display on your monitor just as if it were your local system.

Note: 1. You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.

2. Due to *net lag*, there might be a slight delay before your keystrokes show up. You may also have to wait a bit for the remote mouse to catch up to your local mouse before you click.

3. Due to *net lag*, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

The Windows Client Control Panel

The Windows Client control panel – located at the bottom right of the screen –
provides utilities to help you control remote KVM operations.

The panel consists of an icon bar with a text bar below it. The text bars displays
the remote server's video resolution.

Note: You can move the control panel to any convenient location on the screen
by moving the mouse pointer over one of its borders and dragging.

(Continues on next page.)

(Continued from previous page.)

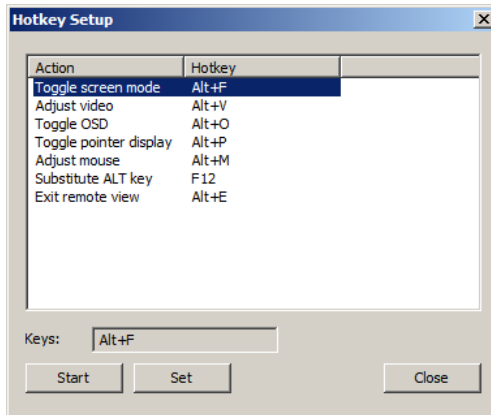The functions that the icons perform is described in the table below:

Icon	Function
	Click to bring up the *Hotkey setup* dialog box (see *Hotkey Setup*, page 37 for details).
	Click to bring up the *Video settings* dialog box.
	Click to bring up the *Virtual media* dialog box.
	Click to bring up the *Message board*.
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to exit the remote view.
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. When the lock state is *On*, the LED is bright green and the lock hasp is closed.; When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. **Note:** When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.

The Windows Client Control Panel icons and their functions are described in the sections that follow.

Hotkey Setup

Various actions related to manipulating the remote server can be accomplished with hotkeys. The *Hotkey Setup* utility is accessed by clicking the *Keyboard* icon on the Control Panel. The actions performed by the Hotkeys are listed in the left panel; the currently defined keys that invoke the actions are shown in the panel to the right.

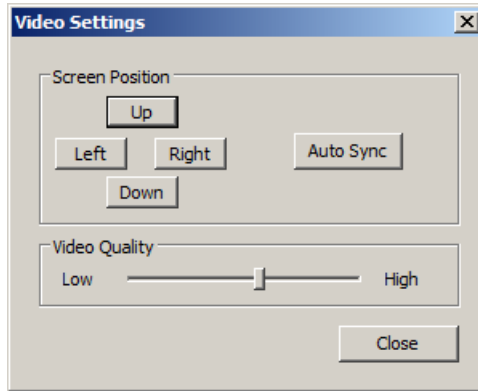| Action	Explanation
Toggle screen mode	Toggles the screen display between full screen and windowed modes.
Adjust Video	Brings up the video setting dialog box.
Toggle OSD	Toggles the control panel Off and On.
Toggle pointer display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to hide the non-functioning pointer. Since this function is a toggle - use the hotkeys again to bring the pointer display back to its original configuration.
Adjust Mouse	Synchronizes the movement of the local and remote mice.
Substitute Alt Key	Although all other keyboard input is captured and sent to the IP8000, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, a function key is substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del].
Exit remote view	Ends the remote connection to the IP8000 and returns to local operation.

Configuring the Hotkeys

If you find the default Hotkey combinations inconvenient, you can configure them by following these steps:

1. Highlight the Action, then Click **Start**

2. Key in the new combination. The key names appear in the *Key* field as you press them.

3. Click **Set**

4. Click **Close**.

Video Settings

The *Video settings* dialog box allows you to adjust the placement and picture quality of the remote screen (as displayed on your monitor).

The meanings of the adjustment options are given in the table below:

| Option	Usage
Screen Position	Adjust the horizontal and vertical position of the remote computer window by Clicking the Arrow buttons.
Auto-Sync	Click Auto-Sync to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. **Note:** This function works best with a bright screen. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually.
Video Quality	Drag the slider bar to adjust the overall Video Quality. The higher the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may slow down response time.

Virtual Media

The IP8000's virtual media feature allows a USB 2.0 device (Floppy drive, CDROM, Flash Drive, etc.), or an image file, on a user's system, to appear, and act, as if it were installed on the remote server.
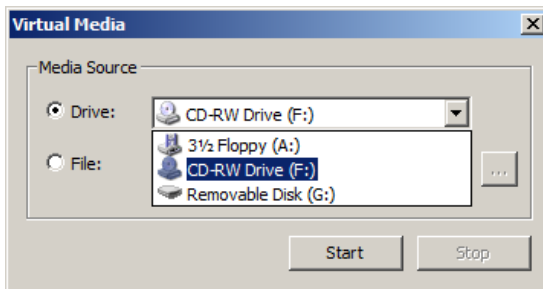
To implement this redirection feature, do the following:

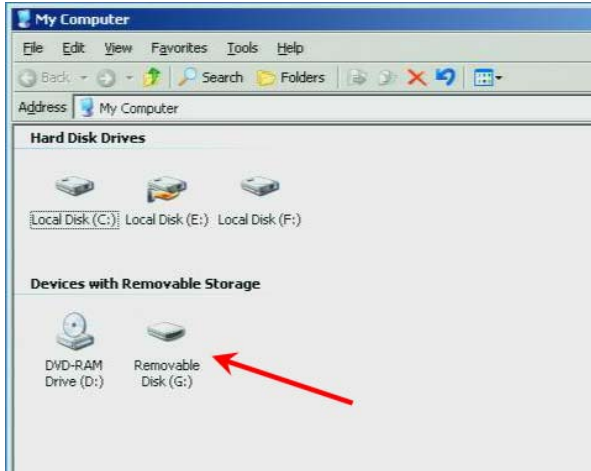1. Bring up the *Virtual media* dialog box:
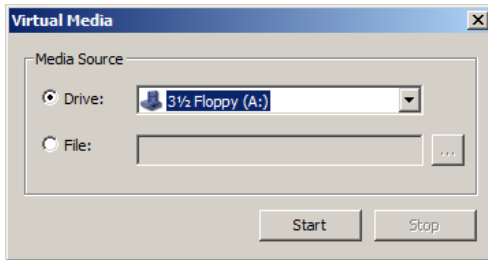
2. Select the media source.

   a) If you select *Drive*, drop down the drive list to select the appropriate drive:

   b) If you select *File*, click the button with the three dots to browse to your image file.

3. After you have made your media source selection, click **Start**. The device (or image file) that you have selected is then redirected to the remote server, where it shows up as a drive on the remote server's file system.

Note: You can dismiss the *Virtual media* dialog box at this point – the redirection will stay in effect.

You can treat the folder as if it were really on the remote server – drag and drop files to/from it; open files on the remote system for editing and save them to the redirected drive, etc.

Files that you save to the redirected drive, will actually be saved to the USB device on your local system. Files that you drag from the redirected drive will actually come from the USB device on your local system.

4. To end the redirection, bring up the *Virtual media* dialog box and click **Stop**.

Message Board

The IP8000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board, similar to an internet chat program, allows users to communicate with each other:
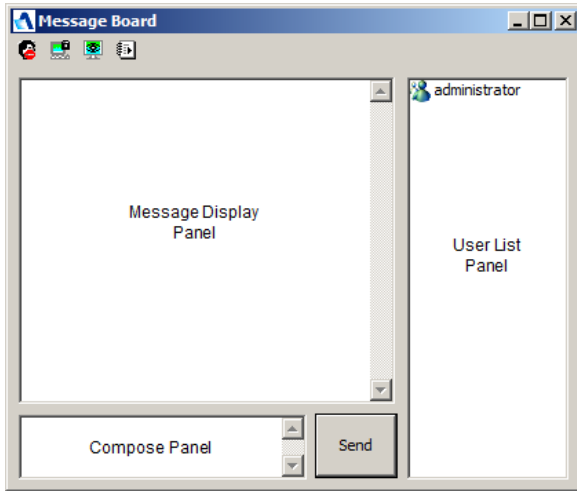
(Continues on next page.)

(Continued from previous page.)

The Button Bar

The buttons on the Button Bar are toggles. Their actions are described in the table below:

| Button	Action
	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The icon displays next to the user's name in the User List panel when he has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The icon displays next to the user's name in the User List panel when he has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The icon displays next to the user's name in the User List panel when he has occupied the KM.
	Show/Hide User List. When you Hide the User List, the User List panel closes.

Compose Panel

Key in the messages that you want to post to the board in this panel. Click **Send**, or press **[Enter]** to post the message to the board.

Message Display Panel

Messages that users post to the board - as well as system messages - display in this panel. If you disable Chat, however, messages that get posted to the board won't appear.

User List Panel

◆ The names of all the logged in users appear in the *User List* panel. Select the names of the users that you wish to send the message to before sending your message.

◆ If a user has disabled Chat, its icon displays before the user's name to indicate so.

◆ If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.
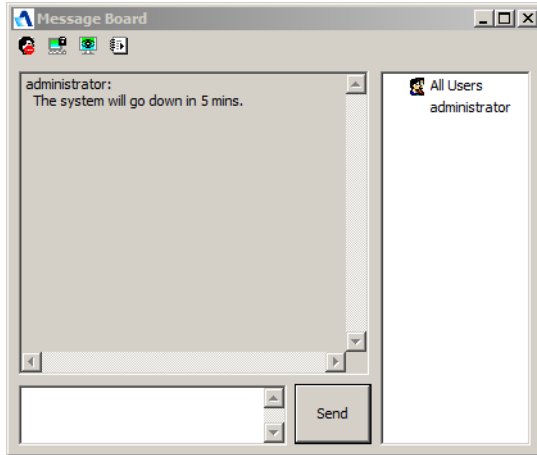
Introduction

The Java Applet makes the IP8000 accessible to all platforms that have JRE 6 Update 3 or higher installed. Java is available for free download from Sun's Java web site (http://www.java.com or http://java.sun.com). To access the IP8000 with the Java Applet:

After you log in (see *Logging In*, page 11), Click the *Open Java Applet* link on the *Remote Console Preview* screen.

Note: If a Security Warning dialog box appears, click **Run**, to accept it.

After a second or two, the remote server's display appears as a window on your desktop:

Navigation

You can work on the remote system via the screen display on your monitor just as if it were your local system.

◆ You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.

◆ You can switch between your local and remote programs with [Alt + Tab].

Note: 1. Due to *net lag*, there might be a slight delay before your keystrokes show up. You may also have to wait a bit for the remote mouse to catch up to your local mouse before you click.

2. Due to *net lag*, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

The Java Applet Control Panel

The Java Applet control panel – located at the bottom right of the screen – provides utilities to help you control remote KVM operations.

The panel consists of an icon bar with a text bar below it. The text bars displays the remote server's video resolution.

Note: You can move the control panel to any convenient location on the screen by moving the mouse pointer over one of its borders and dragging.

(Continues on next page.)

(Continued from previous page.)

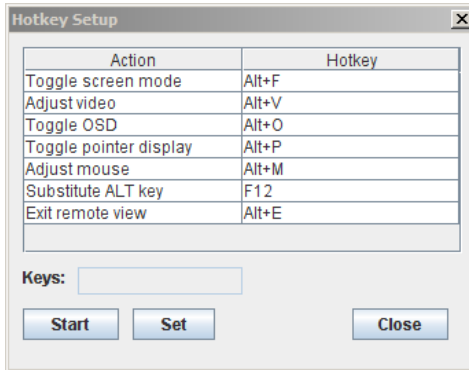The functions that the icons perform is described in the table below:

Icon	Function
	Click to bring up the *Hotkey setup* dialog box (see *Hotkey Setup*, page 48 for details).
	Click to bring up the *Video settings* dialog box.
	Click to bring up the *Message board* (see page 51).
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to exit the remote view.
	The Lock Key LEDs show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer.
	◆ When the lock state is *Off*, the LED is dull green and the lock hasp is open.
	◆ When the lock state is *On*, the LED turns bright green and the lock hasp is closed.
	Click on the icon to toggle the status.
	Note: When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.

The Java Applet Control Panel icons and their functions are described in the sections that follow.

Hotkey Setup

Various actions related to manipulating the remote server can be accomplished with hotkeys. The *Hotkey Setup* utility is accessed by clicking the *Keyboard* icon on the Control Panel. The actions performed by the Hotkeys are listed in the left panel; the currently defined keys that invoke the actions are shown in the panel to the right.

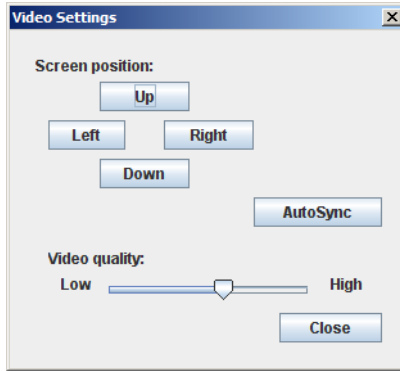| Action	Explanation
Toggle screen mode	Toggles the screen display between full screen and windowed modes.
Adjust Video	Brings up the video setting dialog box.
Toggle OSD	Toggles the control panel Off and On.
Toggle pointer display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to hide the non-functioning pointer. Since this function is a toggle - use the hotkeys again to bring the pointer display back to its original configuration.
Adjust Mouse	Synchronizes the movement of the local and remote mice.
Substitute Alt Key	Although all other keyboard input is captured and sent to the IP8000, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, a function key is substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del].
Exit remote view	Ends the remote connection to the IP8000 and returns to local operation.

Configuring the Hotkeys

If you find the default Hotkey combinations inconvenient, you can reconfigure them by following these steps:

1. Highlight the Action, then click **Start**.

2. Key in the new combination. The key names appear in the *Key* field as you press them.

3. Click **Set**.

4. Click **Close**.

Video Settings

The *Video settings* dialog box allows you to adjust the placement and picture quality of the remote screen (as displayed on your monitor).

The meanings of the adjustment options are given in the table below:

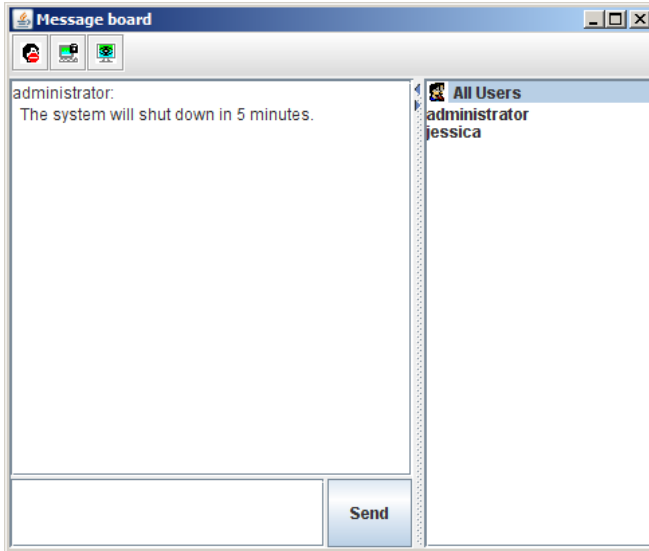| Option	Usage
Screen position	Adjust the horizontal and vertical position of the remote computer window by Clicking the Arrow buttons.
AutoSync	Click Auto-Sync to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen.
	If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync.
	Note: This function works best with a bright screen.
	If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually.
Video quality	Drag the slider bar to adjust the overall Video Quality (right is higher; left is lower). The higher the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may slow down response time.

Message Board

The IP8000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature, similar to an internet chat program, allows users to communicate with each other:
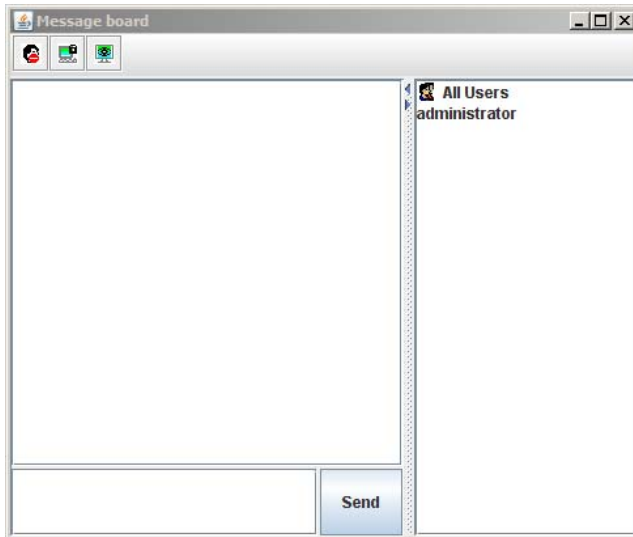
The buttons on the Button Bar are toggles. Their actions are described in the table below:

	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The icon displays next to the user's name in the User List panel when he has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The icon displays next to the user's name in the User List panel when he has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The icon displays next to the user's name in the User List panel when he has occupied the KM.

 ◆ The names of all the logged in users appear in the *User List* panel.

   ◆ Select the users that you want to post to before sending your message. Users that aren't selected won't see the message.

   ◆ To Hide/Unhide the User List panel, click on the arrows in the panel separator.

   ◆ If a user has disabled Chat, the *Disabled Chat* icon displays before the user's name to indicate so.

   ◆ If a user has occupied the KVM or the KM, the corresponding icon displays before the user's name to indicate so.

 ◆ Key in the messages that you want to post to the board in the *Compose* panel. Click **Send**, to post the message to the board.

 ◆ Messages that users post to the board – as well as system messages – display in the *Message Display* panel. If you disable Chat, however, messages that get posted to the board do not appear.

Ctrl+Alt+Del

Clicking this button sends a Ctrl+Alt+Del signal to the remote system.

Exit

Click this button to exit the Java Applet and return to local operation.

Lock LEDs

The Lock Key LEDs show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer.

 When the lock state is *Off*, the LED is dull green and the lock hasp is open.

 When the lock state is *On*, the LED turns bright green and the lock hasp is closed.

Click on the icon to toggle the status.

Note: When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.
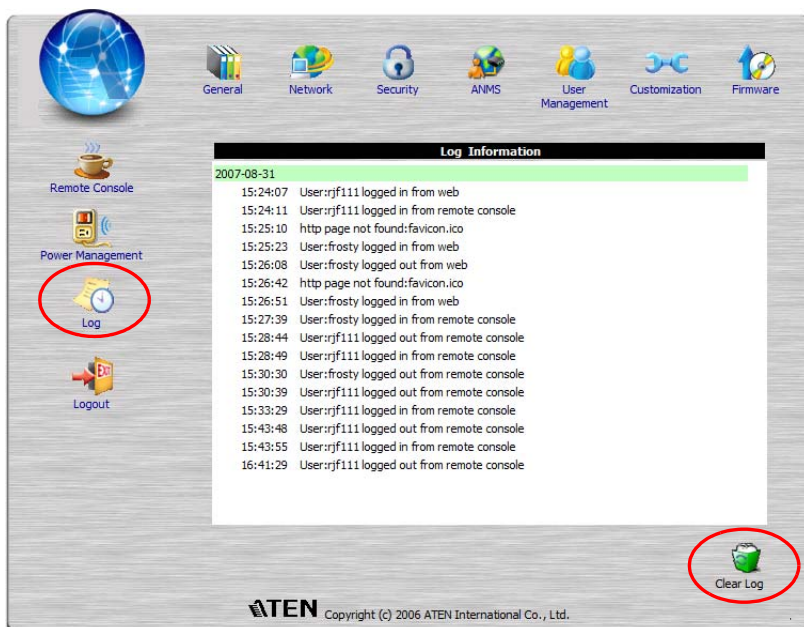
This Page Intentionally Left Blank

The Log File

The Log File Screen

The IP8000 logs all the events that take place on it. To view the contents of the log file in the browser, click the *Log* icon at the left of the web page. A screen similar to the one below appears:

A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded. To clear the log file, click on the *Clear Log* icon at the lower right of the page.

Note: If the server that the IP8000 is installed in is shut down, and the IP8000's power adapter isn't plugged in, the contents of the browser-based log file are lost. If the *Log Server* has been properly installed and configured, however, the log data can be retrieved from there. See Chapter 8, *The Log Server*, for details

This Page Intentionally Left Blank

The Log Server

Introduction

The Windows-based Log Server is an administrative utility that records all the events that take place on selected IP8000 units and writes them to a searchable database. The installer for the Log Server program – *LogSetup.exe* – can be found on the IP8000 software CD. This chapter describes how to install and configure the Log Server.

Installation

Installation

To install the Log Server program, do the following:

1. Copy *LogSetup.exe* from the software CD to a convenient location on your hard disk.

2. Run the program and follow along with the installation dialog boxes.

When the installation completes, an icon – *LogServer* – is placed on your desktop and a program entry is made in the Windows *Start* menu:
(Start → All Programs → LogServer → LogServer).

(Continued from previous page.)

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:
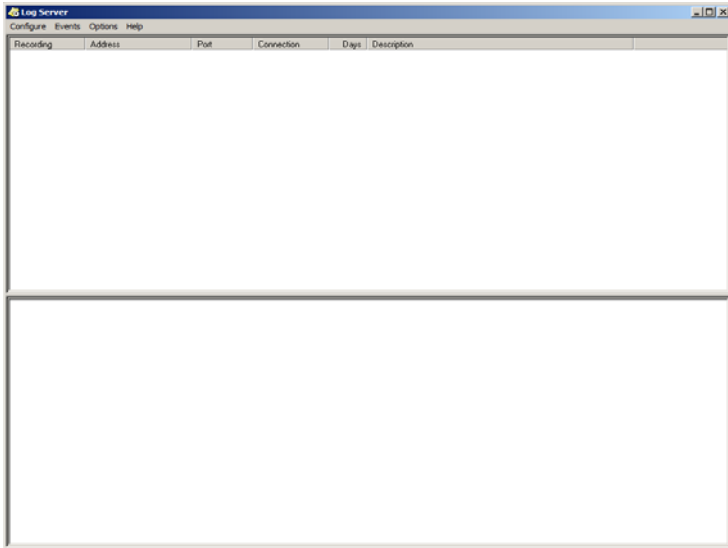
> **Note:** 1. The MAC address of the Log Server computer must be specified in the *ANMS* settings – see page 24 for details.
>
> 2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database.

The screen is divided into three components:

- A *Menu Bar* at the top

- A panel that will contain a list of IP8000 units in the middle (see *The Log Server Main Screen*, page 63, for details).

- A panel that will contain an *Events List* at the bottom

Each of the components is explained in the sections that follow.

The Menu Bar

The Menu bar consists of four items:

- Configure
- Events
- Options
- Help

These are discussed in the sections that follow.

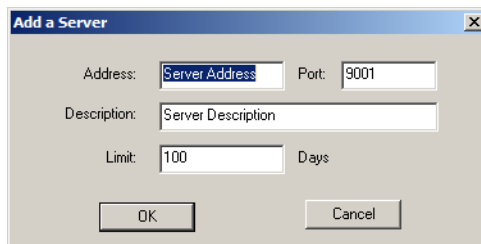---

Note: If the Menu Bar appears to be disabled, click in the IP8000 List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new IP8000 units to the IP8000 List, edit the information for units already on the list, or delete IP8000 units from the list.

- To add a IP8000 to the IP8000 List, click **Add**.
- To edit or delete a listed IP8000, first select the one you want in the IP8000 List window, then open this menu and click **Edit** or **Delete**.

When you choose *Add* or *Edit*, a dialog box, similar to the one below appears:

59

Download from Www.Somanuals.com. All Manuals Search And Download.

A description of the fields is given in the table, below:

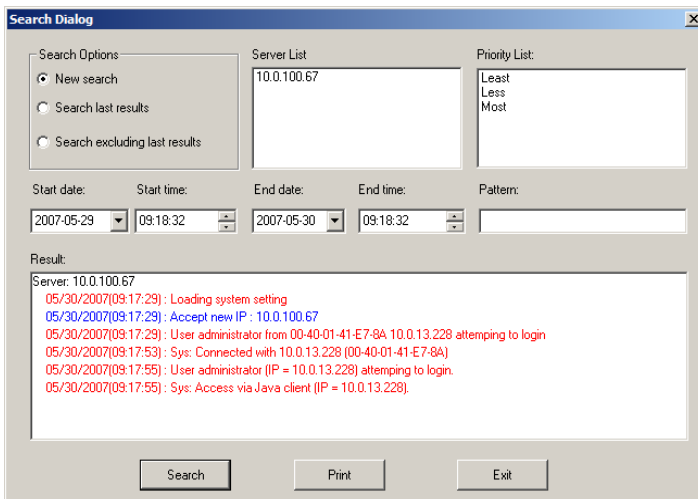| Field	Explanation
Address	This can either be the IP address of the IP8000 or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the IP8000 in the *ANMS* settings (see *ANMS*, page 24).
Port	Key in the port number that was specified for the IP8000 in the *ANMS* settings (see *ANMS*, page 24).
Description	This field is provided so that you can put in a descriptive reference for the unit to help identify it.
Limit	This specifies the number of days that an event should be kept in the Log Server's database before it expires and it is cleared out.

Fill in or modify the fields, then click **OK** to finish.

Events

The Events Menu has 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:

A description of the items is given in the table below:

Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected IP8000.
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 IP8000 *excluding* the events that resulted from the last search.
Server List	IP8000 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. 1 is the most general; 3 is the most specific.
Start Date	Select the date that you want the search to start from. The format follows the MM/DD/YYYY convention, as follows: 11/04/2005
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.
End Time	Select the time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (%) is supported. E.g., h%ds would match *hands* and *hoods*.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results.
Exit	Click this button to exit the Search dialog box.

Maintenance

This function allows the administrator to perform manual maintenance of the database, such as erasing specified records before the expiration time that was set with the *Limit* setting of the Edit function (see page 60).

Options

Network Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect if the previous attempt to connect failed. When you click this item, a dialog box, similar to the one below appears:
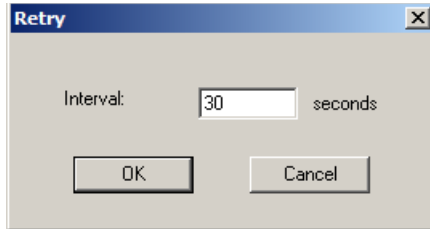
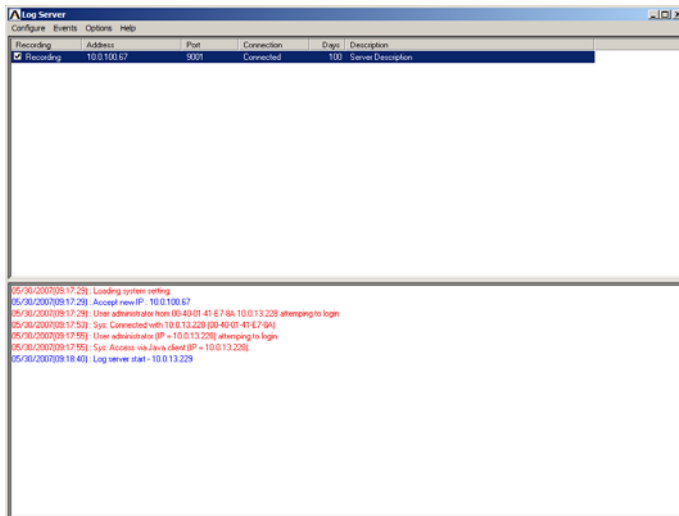Key in the number of seconds, then click **OK** to finish.

Help

From the Help Menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

The Log Server Main Screen is divided into two main panels.

◆ The upper (List) panel lists the IP8000 units that have been selected for the Log Server to track (see *Configure*, page 59).

◆ The lower (Event) panel displays the log events for the currently selected IP8000 (the highlighted one - if there are more than one). To select a IP8000 unit in the list, simply click on it.

The List Panel

The List panel contains six fields:

Field	Explanation
Recording	Determines whether the Log Server records log events for this IP8000 or not. 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 though a IP8000 is not the currently selected one, 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 IP8000 when it was added to the Log Server (see *Configure*, page 59).
Port	This is the port number that was assigned to the IP8000 when it was added to the Log Server (see *Configure*, page 59).
Connection	If the Log Server is connected to the IP8000, this field displays *Connected*.
	If it is not connected, this field displays *Waiting*. This means that the Log Server's MAC address and/or port number has not been set properly. It needs to be set in the *ANMS* settings (see page 24) and specified in the *Configure* dialog box (see *Configure*, page 59).
Days	This field displays the number of days that the IP8000's log events are to be kept in the Log Server's database before expiration (see *Configure*, page 59).
Description	This field displays the descriptive information given for the IP8000 when it was added to the Log Server (see *Configure*, page 59).

The Tick Panel

The lower panel displays tick information for the currently selected IP8000. Note that if the installation contains more than one switch, even though a switch isn't currently selected, if its *Recording* checkbox is checked, the Log Server records its tick information and keeps it in its database.

AP Operation

Introduction

In addition to the browser based client utilities, the IP8000 also provides stand-alone Windows and Java applications that can be used without a browser. Both applications can be found on the IP8000 software CD. The installer for the Windows Client program is called *ip8000winclient.exe*; the Java Client program is called *iClientJ.jar*.

The AP Windows Client

Installation

To install the stand-alone Windows Client program, do the following:

1. Copy *ip8000winclient.exe* from the software CD to a convenient location on your hard disk.

2. Run the program and follow along with the installation dialog boxes.

When the installation completes, an icon – *IP8000 WinClient* – is placed on your desktop and a program entry is made in the Windows *Start* menu: (Start → All Programs → IP8000 → IP8000 WinClient).

(Continues on next page.)

(Continued from previous page.)

Starting Up

To connect to the IP8000, either click its icon on the desktop or click its entry on the Start menu.
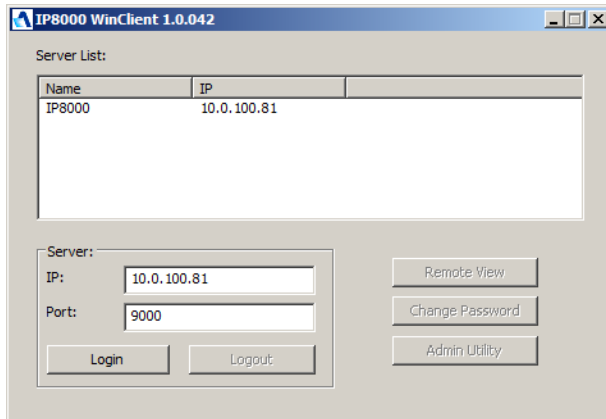
If this is the first time that you are running the utility, a dialog box appears requesting you to input your serial number.
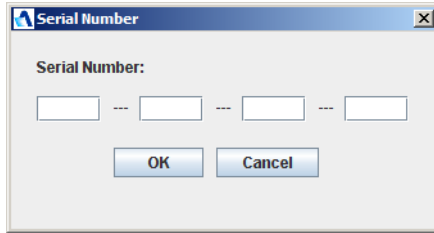
The serial number can be found on the IP8000's CD case. Key in the serial number - 5 characters per box - then click **OK** to bring up the IP8000 Connection Screen.

Note: 1. Letters in the serial number must be entered in capitals.

2. This dialog box only appears the first time you run the program. In the future, you go directly to the Windows Client Connection screen.

The Windows Client Connection Screen

A description of the Connection Screen is given in the following table:

Item	Description
Server List	Each time the WinClient program is run, it searches the user's local LAN segment for IP8000 units, and lists whichever ones it finds in this box. If you want to connect to one of these units, select it, then click **Login**. When you have finished with your session, Click **Logout** to end the connection.
Server	This area is used when you want to connect to a IP8000 at a remote location. You can drop down the *IP* list box and select an address from the list. If the address you want isn't listed, you can key in the IP address you want. Then, key in the Port number in the *Port* field. If you don't know the Port number, contact the Administrator.
	When the IP address and Port number for the unit you wish to connect to have been specified, click **Login** to start the connection. When you have finished with your session, Click **Logout** to end the connection.
Login	Starts the connection to the IP8000.
Logout	These buttons become active once you log into the IP8000. See page 69 for details.
Remote View	
Change Password	
Admin Utility	

Logging In

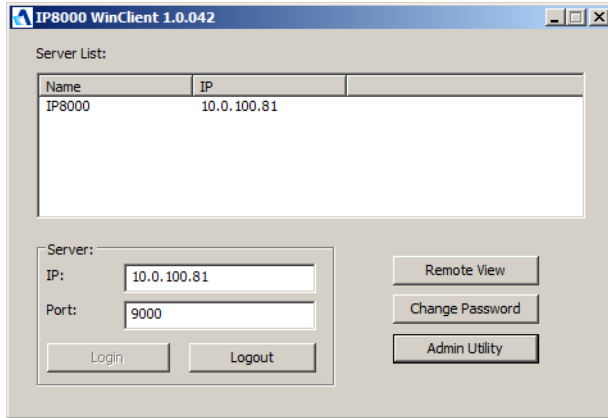Once the IP8000 connects to the unit you specified, a login window appears:
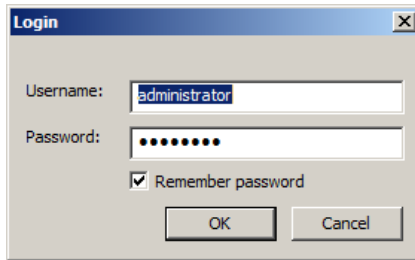
Provide a valid Username and Password, then Click **OK** to continue.

Note: The default Username is *administrator*; the default Password is
password. For security, we strongly recommend that you change these
to something unique (see *User Management*, page 74, for details).

(Continues on next page.)

(Continued from previous page.)

After you have successfully logged in, the Connection screen reappears:

At this time there are four active buttons, as described in the table, below:

Button	Action
Logout	Breaks the connection to the IP8000.
Remote View	In some cases, administrator's do not wish to have users connect to the IP8000 with a browser. *Remote View* solves this problem. It opens a window on the user's desktop containing the remote server's display that is the same as the one that appears with the browser-based Windows client. Refer to Chapter 5, *The Windows Client*, for operation details.
Change Password	Allows users to change their passwords without administrator intervention.
Admin Utility	The Administrator Utility provides administrators with a non-browser based method for configuring and controlling IP8000 operations. The Administrator Utility is discussed in the sections that follow.

The Administrator Utility

The Administrator Utility appears as a notebook with six tabs. Each tab represents a different administrative function. A description of the functions and how to configure their settings is provided in the sections that follow.

General

The Settings notebook opens with the *General* page displayed:
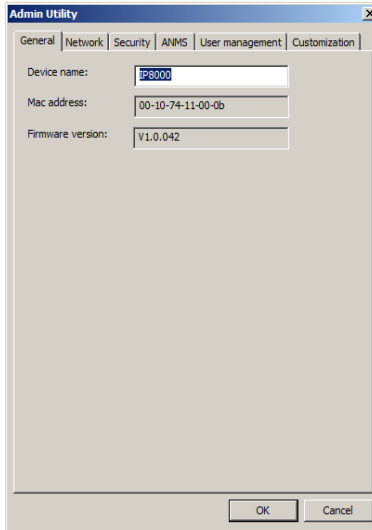
The General page provides information about the IP8000's status, as explained in the table, below:

Item	Description
Device Name:	To make it easier to manage installations that have more than one IP8000, each one can be given a name. To assign a name for the IP8000, erase the current name and key in one of your choosing (16 characters max.).
MAC Address	The IP8000's MAC Address displays here.
Main Firmware Version:	Indicates the mainboard's current firmware version level. New versions of the IP8000's firmware and authentication software can be downloaded from our web site as they become available (see *Upgrading the Firmware*, page 76, for details).

Network

This page is used to specify the IP8000's network environment.

The settings on this page are essentially the same as that of the browser-based version. See *Network*, page 19, for details.

Note: Be sure to enable *Reset on exit* on the *Customization* page (see page 75) before exiting the Administrator Utility. This allows network changes to take effect without having to power the IP8000 off and on.

Security

The Security page is used to control access to the IP8000.
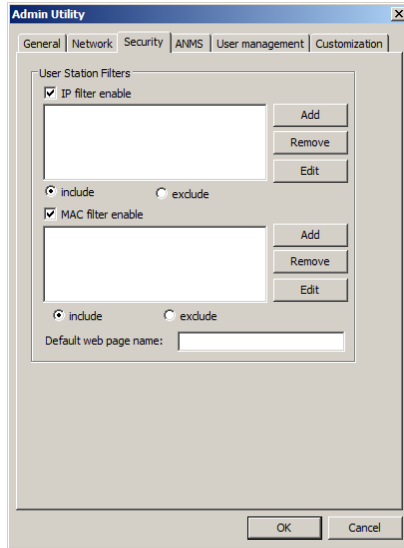
The settings on this page are essentially the same as that of the browser-based version. See *Security*, page 21, for details.

ANMS

The Advanced Network Management Settings dialog box allows you to set up login authorization management from a external sources.

The settings on this page are essentially the same as that of the browser-based version. See *ANMS*, page 24, for details.

User Management

This page is used to set up and manage user profiles. It defines the access rights of each user. Up to 64 user profiles can be established
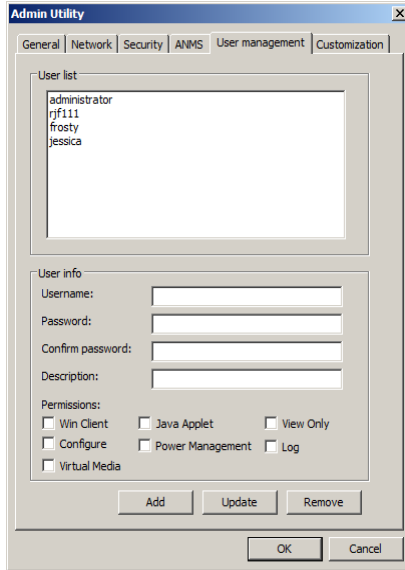
The settings on this page are essentially the same as that of the browser-based version. See *User Management*, page 27, for details.

Customization

This page allows the Administrator to upgrade the firmware and to set to set various working parameters.
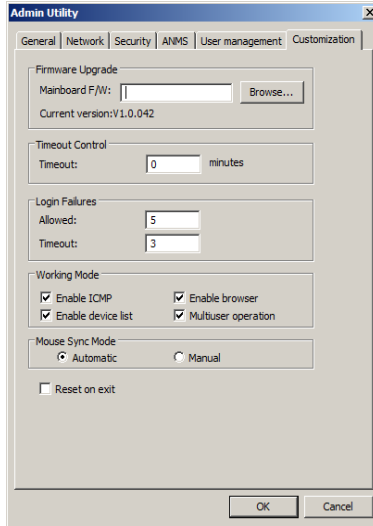

Except for the *Firmware Upgrade* section, the settings on this page are essentially the same as that of the browser-based version. See *Customization*, page 29, for details on setting *Timeout*, *Login failure*, *Working mode,* and *Mouse Sync Mode* parameters.

The Firmware Upgrade section is used when upgrading the IP8000's firmware. Upgrading the firmware is discussed in the next section.

Upgrading the Firmware

New versions of the Mainboard firmware files can be downloaded from our website as they become available. After downloading the new firmware file, to upgrade the firmware, do the following:

1. On the *Customization* page of the Administration Utility's configuration notebook (see page 75) click the *Browse* button.

2. In the *File Open* dialog box that appears, navigate to the directory that the downloaded firmware upgrade file is in; select the file; then click **Open**.
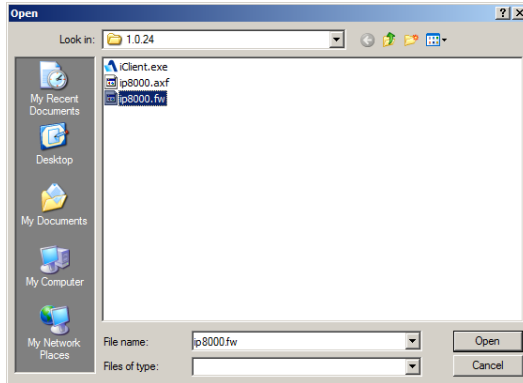
3. When you return to the Customization page, the file appears in the *Mainboard F/W* field. Click **OK** to perform the upgrade.

The AP Java Client

The Java Client is provided to make the IP8000 accessible to all platforms. Systems that have JRE 6 Update 3 or higher installed can connect. If you don't already have Java, it is available for free download from Sun's Java web site (http://www.java.com or http://java.sun.com).

Starting Up

To connect to the IP8000 with the stand-alone Java Client program, copy *iClientJ.jar* to a convenient location on your hard disk; then double-click its icon – or key in the full path to the program on the command line – to bring up the Java Client Connection screen.

Note: 1. Letters in the serial number must be entered in capitals.

2. If this is the first time that you are running the program a dialog box appears requesting you to input your serial number.
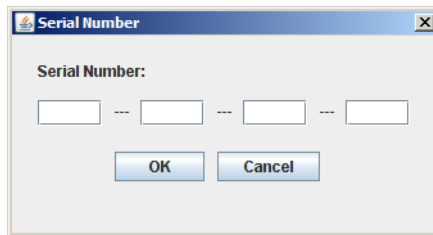
The serial number can be found on the IP8000's CD case. Key in the serial number - 5 characters per box - then click **OK** to bring up the IP8000 Connection Screen.

After performing this operation the first time you run the program, this dialog box doesn't appear again – you go directly to the Java Client Connection screen.
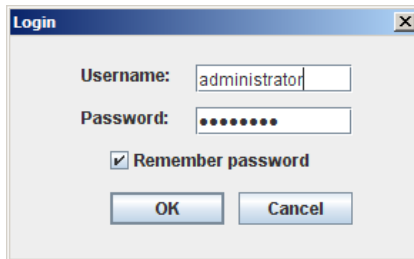
The Java Client Connection Screen
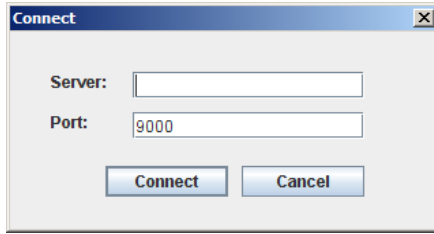
To connect to the IP8000

1. Key in its IP address in the Server field.

2. If the port number shown isn't correct, key in the correct number.

3. Click **Connect**.

Logging In

Once the IP8000 connects to the unit you specified, a login window appears:

Provide a valid Username and Password, then Click **OK**.

Note: The default Username is *administrator*; the default Password is *password*. For security, we strongly recommend that you change these to something unique (see *User Management*, page 74, for details).

After you have successfully logged in, a window opens on your desktop containing the remote server's display. This is the same window that appears when you run the browser-based Java applet. Refer to Chapter 6, *The Java Applet*, for operation details.

Appendix

Safety Instructions

General

- Read all of these instructions. Save them for future reference.

- Follow all warnings and instructions marked on the device.

- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.

- Do not use the device near water.

- Do not place the device near, or over, radiators or heat registers.

- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.

- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.

- Never spill liquid of any kind on the device.

- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.

- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.

- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.

- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or un-interruptible power supply (UPS).

- Position system cables and power cables carefully; Be sure that nothing rests on any cables.

* When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  * Install the power supply before connecting the power cable to the power supply.
  * Unplug the power cable before removing the power supply.
  * If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
* Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
* Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
* If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  * The power cord or plug has become damaged or frayed.
  * Liquid has been spilled into the device.
  * The device has been exposed to rain or water.
  * The device has been dropped, or the cabinet has been damaged.
  * The device exhibits a distinct change in performance, indicating a need for service.
  * The device does not operate normally when the operating instructions are followed.
* Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.

Technical Support

International

Email Support		support@aten.com
Online Support	Technical Support	http://support.aten.com
	Troubleshooting Documentation Software Updates	http://www.aten.com
Telephone Support		886-2-8692-6959

North America

Email Support		ATEN TECH	support@aten-usa.com
		ATEN NJ	sales@aten.com
Online Support	Technical Support	ATEN TECH	http://www.aten-usa.com/support
		ATEN NJ	http://support.aten.com
	Troubleshooting Documentation Software Updates	ATEN TECH	http://www.aten-usa.com
		ATEN NJ	http://www.aten.com
Telephone Support		ATEN TECH	1-888-999-ATEN
		ATEN NJ	1-732-356-1703

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.

- Your computer configuration, including operating system, revision level, expansion cards, and software.

- Any error messages displayed at the time the error occurred.

- The sequence of operations that led up to the error.

- Any other information you feel may be of help.

Specifications

Function			Specification
Connectors	Console Ports	Video	1 x HDB-15 Female
	KVM Link		1 x SPHD-15 Female
	LAN		1 x RJ-45 Receptacle
	Power		1 x DC Jack 5V
LEDs	Link		1 (Green)
	10/100 Mbps		1 (Orange/Green)
Emulation	Keyboard/Mouse		USB; PS/2
Video			1600 x 1200 @ 60 Hz; DDC2B
Power Consumption			DC 5 V; 5.5 W
Environment	Operating Temp.		0–50º C
	Storage Temp.		-20–60º C
	Humidity		0–80% RH
Physical Properties	Weight		0.10 kg
	Dimensions (L x W x H)		15.35 x 12.00 x 2.15 cm

IP Address Determination

If you are an administrator logging in for the first time, you need to access the IP8000 in order to give it an IP address that users can connect to. There are two methods to choose from: 1) *Resetting Your Computer Address*; and 2) running the *Windows Client* program.

The first method is useful for determining the IP value of devices with fixed addresses. The Windows Client method is good for determining the IP value of devices with either fixed or DHCP derived IP addresses. With either method your computer must be on the same network segment as the IP8000.

Note: The Windows Client method is especially useful if the device's DHCP assigned address changes.

After you have connected and logged in to the IP8000, you can give it a fixed network address in the *Network Settings* dialog box (see page 19).

Resetting Your Computer Address

For non-Windows computers, a browser based method for setting the IP8000's IP address is available. It is based on the fact that when the IP8000 starts, if it doesn't find a DHCP environment after 30 seconds, it automatically sets its IP address to 192.168.0.60. To set the IP8000's address with this method, do the following:

1. Set your computer's IP address to 192.168.0.*XXX*

   Where *XXX* represents any number or numbers except 60.

2. Specify the switch's default IP address (192.168.0.60) in the URL entry box of your browser.

3. After you connect and log in, click the *Network* icon (see page 19) to assign a fixed IP address for the IP8000 that is suitable for the network segment that it resides on.

4. After you log out, be sure to reset your computer's IP address to its original value.

The Windows Client

For computers running Windows, the IP8000's IP address can be determined with the Windows stand-alone application program.

When you run the Windows stand-alone application (see page 65), it searches the network segment for IP8000 devices, and displays what it finds in a dialog box similar to the one below:
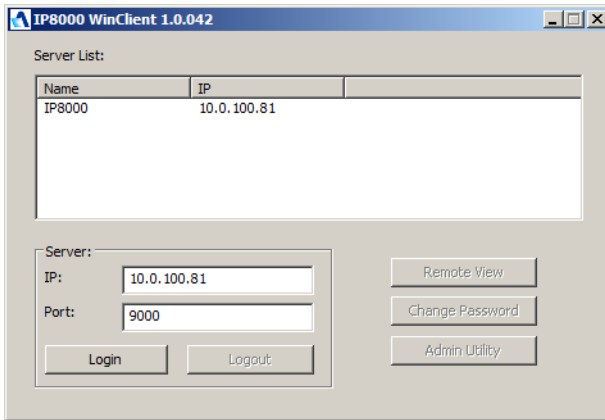
You can now use this network address if it is suitable to do so. You can change it to a more suitable one if you wish, by clicking **Login**, logging in, clicking **Admin Utility**, and clicking the *Network* tab. See *Network*, page 71, for details.

Administrator Login Failure

If you are unable to perform an Administrator login to the IP8000 (because the Username and Password information has become corrupted, or you have forgotten it, for example), there is a procedure you can use to clear the login information.

Note: Performing this procedure also returns all settings to their defaults.

To clear the login information (and return all settings to their defaults), do the following:

1. Power off the IP8000 by unplugging its power adapter cable.

2. Power off the server that the IP8000 is installed in and remove its housing.

3. Short the jumper on the IP8000 labeled *J2 Default Password*.
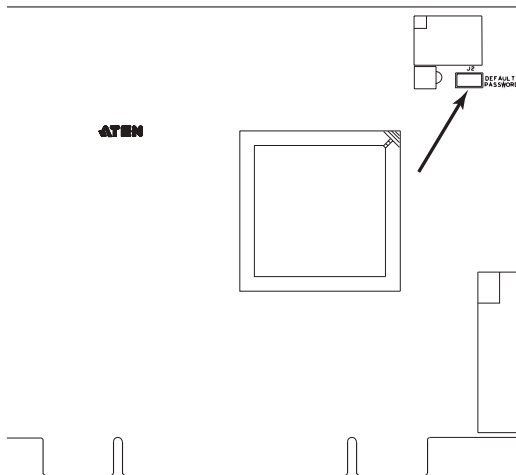
4. Power on the IP8000 by plugging its power adapter cable back in. Wait a few seconds, then unplug it again.

5. Remove the jumper cap from J2.

6. Close the housing and start the server back up.

7. Plug the IP8000's by power adapter cable back in.

   After you complete these steps, you can use the default Username and Password (see page 13) to log into the IP8000.

Troubleshooting

Overview

Operation problems can be due to a variety of causes. The first step in solving them is to make sure that all cables are securely attached and seated completely in their sockets.

In addition, updating the product's firmware may solve problems that have been discovered and resolved since the prior version was released. If your product is not running the latest firmware version, we strongly recommend that you upgrade. See *Upgrading the Firmware*, page 76, for upgrade details.

The Windows Client

Problem	Resolution
Remote mouse pointer is out of step.	Use the *AutoSync* feature (see *Video Settings*, page 39), to synch the local and remote monitors.
	If the method shown above fail to resolve the problem, use the *Toggle Mouse Display* function (see page 37).
	If the procedures above fail to resolve the problem, perform the operations described under *Additional Mouse Synchronization Procedures*, page 89, on both the local and remote computers.
Part of remote window is off my monitor.	Use the *AutoSync* feature (see *Video Settings*, page 39), to sync the local and remote monitors.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 91, for details.

The Java Client

Symptom	Action
Java Client won't connect to the IP8000	1. JRE 6 Update 3 or higher must be installed on your computer. 2. Close the Java Client, reopen it, and try again.
Java Client performance deteriorates.	Exit the program and start again.
National language characters don't appear.	When entering national language characters, if your local keyboard is set to a non-English national language layout, you must set the remote computer's keyboard layout to English.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 91, for details.
There is no Virtual Media icon on my Control Panel.	The virtual media function only supports the Windows browser and AP client programs.

The Log Server

Problem	Resolution
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 ME, 2000 and XP. 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.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g., Sun Blade 1000 servers).[1]	The display resolution should be set to 1024 x 768: Under Text Mode: 1. 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: Under Text Mode: 1. 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
The local and remote mouse pointers do not sync	For USB mice on Windows systems. the local and remote mouse pointers are designed to automatically sync when you connect. For other mice and computer platforms, you must select *Manual* as the *Mouse Sync Mode* choice, and sync the pointers manually. See *Mouse Sync Mode*, page 30 for further details.

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

Additional Mouse Synchronization Procedures

If the mouse synchronization procedures mentioned in the manual fail to resolve mouse pointer problems for particular computers, try the following:

Windows:

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.

1. Windows 2000:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse → Mouse Properties)

   b) Click the *Motion* tab

   c) Set the mouse speed to the middle position (6 units in from the left)

   d) Set the mouse acceleration to *None*
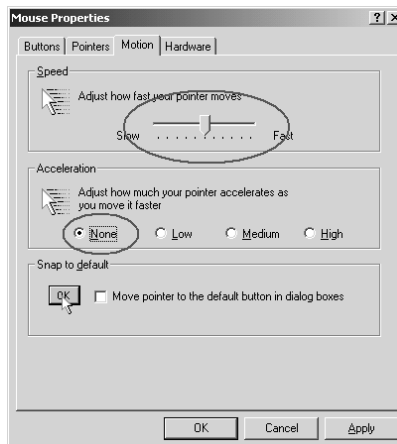
2. Windows XP / Windows Server 2003:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse)

   b) Click the *Pointer Options* tab

   c) Set the mouse speed to the middle position (6 units in from the left)

   d) Disable *Enhance Pointer Precision*
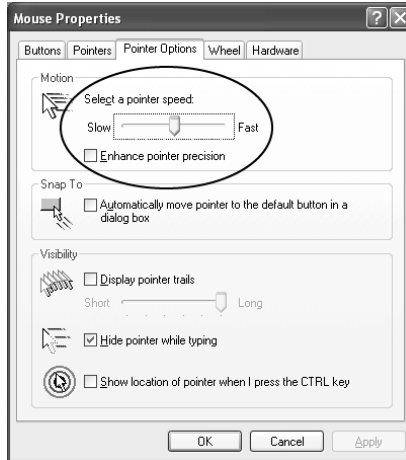
3. Windows ME:

   Set the mouse speed to the middle position; disable mouse acceleration (click **Advanced** to get the dialog box for this).

4. Windows NT / Windows 98 / Windows 95:

   Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.
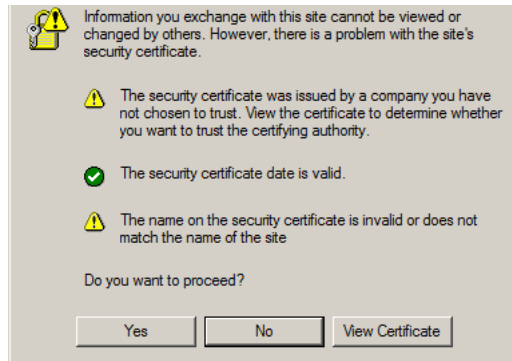
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

◆ If you are working on a computer at another location, accept the certificate for just this session by clicking **Yes.**

◆ If you are working at your own computer, install the certificate on your computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Installing the Certificate

To install the certificate, do the following:

1. In the *Security Alert* dialog box, click **View Certificate.** The *Certificate Information* dialog box appears:
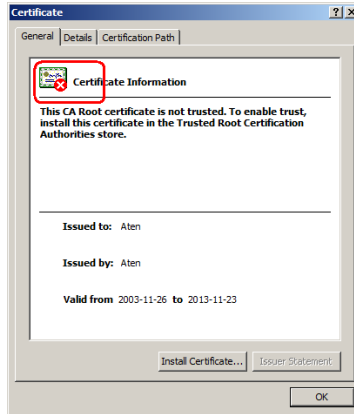
Note: There is a red and white **X** logo over the certificate to indicate that it is not trusted.

---

2. Click **Install Certificate.**

3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.

4. When the Wizard presents a caution screen:
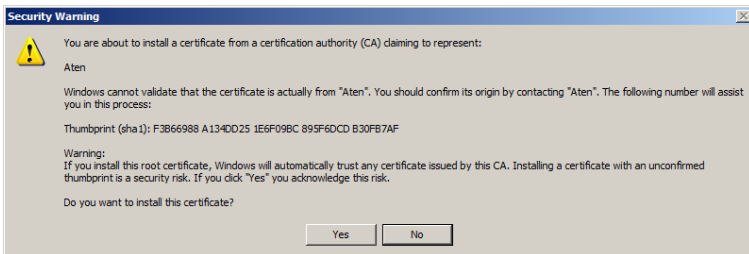
  Click **Yes**.

5. Next, click **Finish** to complete the installation; then click **OK** to close the dialog box.

<u>Certificate Trusted</u>

The certificate is now trusted:
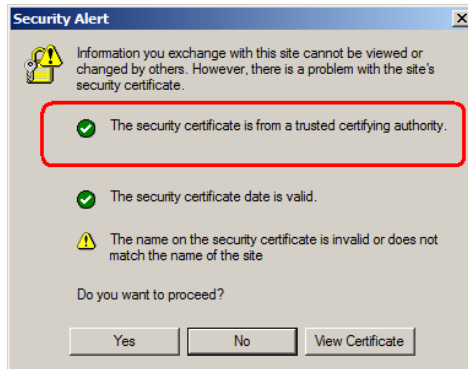
When you click *View Certificate*, you can see that the red and white **X** logo is no longer present – further indication that the certificate is trusted:
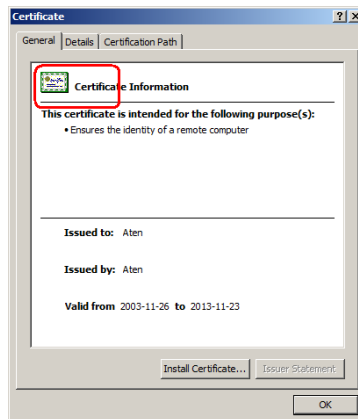
About SPHD Connectors

This product uses SPHD connectors for its KVM and/or Console ports. We have specifically modified the shape of these connectors so that only KVM cables that we have designed to work with this product can be connected.

Limited Warranty

ALTUSEN warrants this product against defects in material or workmanship for a period of one (1) year from the date of purchase. If this product proves to be defective, contact ALTUSEN's support department for repair or replacement of your unit. ALTUSEN will not issue a refund. Return requests can not be processed without the original proof of purchase.

When returning the product, you must ship the product in its original packaging or packaging that gives an equal degree of protection. Include your proof of purchase in the packaging and the RMA number clearly marked on the outside of the package.

This warranty becomes invalid if the factory-supplied serial number has been removed or altered on the product.

This warranty does not cover cosmetic damage or damage due to acts of God, accident, misuse, abuse, negligence or modification of any part of the product. This warranty does not cover damage due to improper operation or maintenance, connection to improper equipment, or attempted repair by anyone other than ALTUSEN. This warranty does not cover products sold AS IS or WITH FAULTS.

IN NO EVENT SHALL ALTUSEN'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. FURTHER, ALTUSEN SHALL NOT BE RESPONSIBLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. ALTUSEN SHALL NOT IN ANY WAY BE RESPONSIBLE FOR, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT OR PROPERTY, AND ANY EXPENSES FROM RECOVERY, PROGRAMMING, AND REPRODUCTION OF ANY PROGRAM OR DATA.

ALTUSEN makes no warranty or representation, expressed, implied, or statutory with respect to its products, contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose.

ALTUSEN reserves the right to revise or update its product, software or documentation without obligation to notify any individual or entity of such revisions, or update.

For details about extended warranties, please contact one of our dedicated value added resellers.

Index

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com