KVM On the NET™

CN8000

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

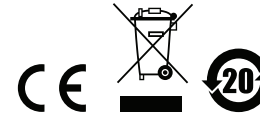
The following contains information that relates to China.

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 basic CN8000 package consists of:

- 1 CN8000 KVM On the NET™ Switch
- 2 Custom KVM Cable Sets
- 1 Custom Console Cable Set
- 1 USB 2.0 Virtual Media Cable
- 1 Power Adapter
- 1 Mounting Kit
- 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 CN8000 since this manual was printed. Please visit our website to download the most up-to-date version of the manual.

Manual Part No. PAPE-0288-100G
Manual Date: 2008-07-01

Contents

4. Administration

5. The Windows Client

6. The Java Applet

7. The Log File

8. The Log Server

9. AP Operation

10.LDAP Server Configuration

Appendix

About this Manual

This User Manual is provided to help you get the most from your c/c system. 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 CN8000 System. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup, provides step-by-step instructions for setting up your installation, and explains some basic operation procedures.

Chapter 3, Browser Login, describes how to log into the CN8000 with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 4, Administration, explains the administrative procedures that are employed to configure the CN8000's working environment, as well as how to operate the CN8000 from the local console.

Chapter 5, The Windows Client, explains how to connect to the CN8000 with the Windows Client software, and describes how to use the OSD to access and control the computers connected to the switch.

Chapter 6, The Java Applet, describes how to connect to the CN8000 with the Java Applet software, and explains how to use the OSD to access and control the computers connected to the switch.

Chapter 7, The Log File, shows how to use the log file utility to view the events that take place on the CN8000.

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

Chapter 9, AP Operation, describes how to operate the CN8000 using Windows and Java programs, rather than with the browser method.

Chapter 10, LDAP Server Configuration, explains how to configure the CN8000 for LDAP / LDAPS authentication and authorization with Active Directory or OpenLDAP.

An Appendix, provides specifications and other technical information regarding the CN8000.

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 same 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

This Page Intentionally Left Blank

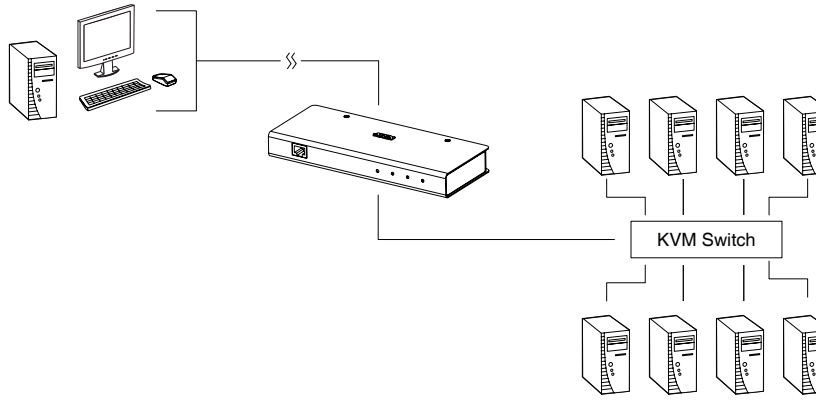
Chapter 1
Introduction

Overview

The CN8000 is a control unit that provides “over-IP” capability to KVM switches that do not have built in over-IP functionality. It allows operators to monitor and access their computers from remote locations using a standard Internet browser or Windows and Java based application programs. The CN8000 connects to the Internet, an Intranet, LAN, or WAN using industry standard Cat 5e cable, then uses a custom KVM cable to connect to a local KVM switch or server.

Because the CN8000 uses TCP/IP for its communications protocol, the server or KVM switch 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.

Operators at remote locations connect to the CN8000 via its IP address. Once a connection has been established and authorization granted, the remote computer can exchange keyboard, video and mouse signals with the server (or servers on a KVM switch installation), just as if they were physically present and working on the equipment directly.



The CN8000 expands on previous models by providing a dedicated RS-232 port for modem access, a PON port to attach a Power Over the NET™ device and USB 2.0 virtual media capability.

With its advanced security features, the CN8000 is the fastest, most reliable, most cost effective way to remotely access and manage widely distributed multiple computer installations.

The *Administrator* and *Client* software included with the CN8000 make it easy to install, maintain, and operate. System administrators can handle a multitude of tasks with ease - from installing and running GUI applications, to BIOS level troubleshooting, routine monitoring, concurrent maintenance, system administration, rebooting and even pre-booting functions.

The *Administrator Utility* is available in both a browser-based version and a Windows-based application version. It is used to configure the system; limit access from remote computers; manage users; and maintain the system with firmware and software module updates.

Both a *Windows GUI Client* and a *Java Applet* are also available in browser-based and Windows application versions. They are provided for IP connection and login from anywhere on the net. Inclusion of a Java-based client ensures that the CN8000 is platform independent, and is able to work with practically all operating systems.

The client software allows access to, and control of, the connected servers. Once an operator successfully connects and logs in, his screen displays what is running on the remote unit attached to the CN8000 (a KVM OSD display, a server's desktop, or a running program, for example) and he can control it from his console just as if he were there.

The *Log Server* records all the events that take place on selected CN8000 units for the administrator to analyze.

Your CN8000 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

- Provides over-IP capability to KVM switches that do not have built in over-IP functionality
- Virtual media via USB 2.0 data transmission
- PON (Power Over the NET™) support via Java
- 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; LDAP; LDAPS; MS Active Directory
- 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 – Java works with practically all operating systems
- Supports TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP, 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
- PPP mode (modem) dialup support for out-of-band, and low bandwidth operation
- Full-screen or sizable remote desktop window;
- In full-screen mode the remote desktop display scales to user's monitor display size
- On-screen keyboard
- Export/import user account and configuration settings
- Advanced security features include password protection and advanced encryption technologies
- Secure 128-bit SSL encryption
- Enable/disable browser operation
- Event logging
- Remote firmware upgrading

System Requirements

General

- For best results we recommend that the computers used to access the CN8000 control unit have at least a PIII 1 GHz processor, and that the screen resolution is set to 1024 x 768.
- Browsers must support 128 bit data encryption.
- For best results we recommend that the internet connection speed be at least 128 kbps.
- Browsers must support ActiveX in order to access the Win Client link.
- 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 the following **non-interlaced** video signals are supported:

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

Cables

- Two custom KVM cable sets (1 USB; 1 PS/2) to link the CN8000 to a server or KVM switch are provided with this package.
- Custom KVM cable sets are available in various lengths, as shown in the table below:

Cable Type	Length	CS Part Number
PS/2	1.2 m	2L-5201P
	1.8 m	2L-5202P
	3.0 m	2L-5203P
	6.0 m	2L-5206P
USB	1.2 m	2L-5201U
	1.8 m	2L-5202U
	3.0 m	2L-5203U
	5.0 m	2L-5205U

  To purchase additional cable sets, contact your dealer.

- One custom Console cable set to link the CN8000 to a local console is provided with this package.

  Note: This cable set has been designed to operate with either PS/2 or USB consoles.

- A USB 2.0 cable for use with the *Virtual Media* function (see *Virtual Media Port*, page 9) is provided with this package.
- Cat 5e or higher Ethernet cable (not provided with this package), should be used to connect the CN8000 to the LAN, WAN, or Internet.

Operating Systems

- Supported operating systems for servers that connect to the CN8000 are shown in the table, below:

OS		Version
Windows		2000 and higher
Linux	RedHat	7.1 and higher
	Fedora	Core 5 and higher
	SuSE	9.0 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	3.51 and higher
	Sun	Solaris 8 and higher
Novell	Netware	5.0 and higher
Mac		OS 9 and higher
DOS		6.2 and higher

- Supported operating systems for users that log into the CN8000 include Windows 2000 and higher, and those capable of running Sun's Java Runtime Environment (JRE) 6, Update 3, or higher.

Browsers

Supported browsers for users that log into the CN8000 include the following:

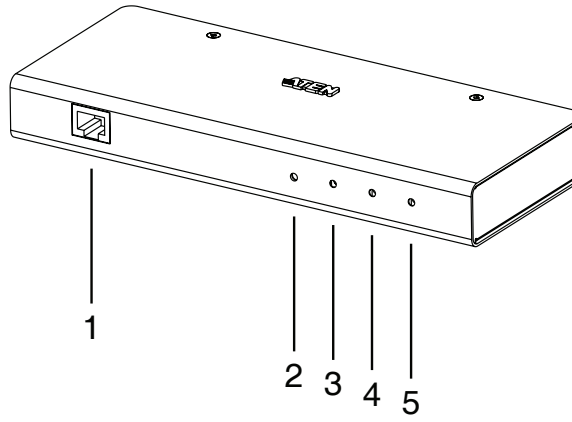
Browser	Version
IE	6 and higher
Firefox	1.5 and higher
Mozilla	1.7 and higher
Safari	2.0 and higher
Opera	9.0 and higher
Netscape	8.1 and higher

Virtual Media Support

- USB CDROM/DVD-ROM Drives
- USB Floppy Drives
- USB Flash Drives
- IDE CDROM/DVD-ROM Drives
- Image Files

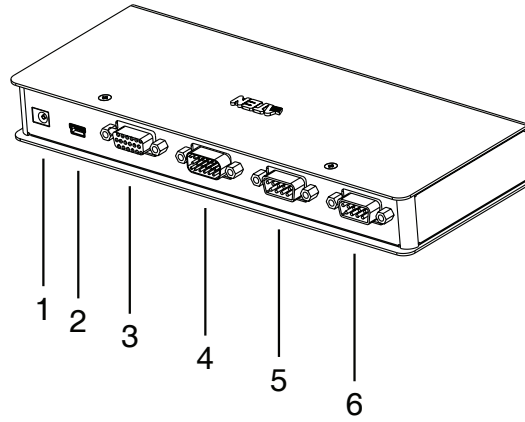
Components

Front View



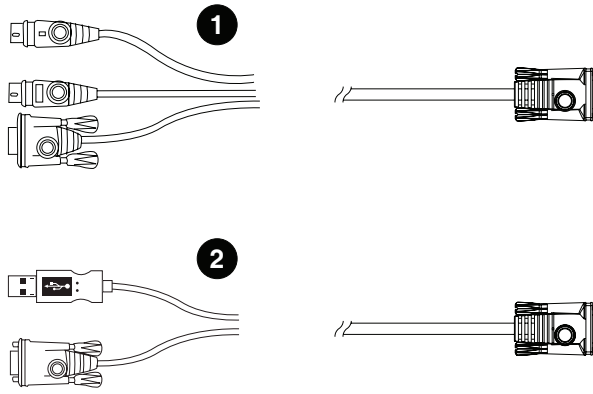
No.	Component	Description
1	LAN Port	The Cat 5e cable that connects the CN8000 to the LAN, WAN, or Internet plugs in here.
2	Firmware Upgrade/Reset Switch	1. Pressing and releasing this switch performs a CN8000 system reset. (See *Erratic operation*, page 116.) 2. Pressing and holding this switch for more than three seconds returns the CN8000 to its factory default configuration settings. 3. Pressing and holding this switch while powering on the switch returns the CN8000 to its factory default firmware level. This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. **Note:** This switch is recessed and must be pushed with a thin object - such as the end of a paper clip, or a ballpoint pen.
3	10/100 Mbps LED	The LED lights ORANGE to indicate 10 Mbps data transmission speed. It lights GREEN to indicate 100 Mbps data transmission speed.
4	Link LED	Flashes GREEN to indicate that a Client program is accessing the device.
5	Power LED	Lights ORANGE when the CN8000 is powered up and ready to operate.

Rear View



No.	Component	Description
1	Power Jack	The power adapter cable plugs in here.
2	Virtual Media Port	The cable that connects the CN8000 to a USB port on your server or KVM switch plugs in here. See *Virtual Media*, page 47, for virtual media details.
3	PC/KVM Port	The KVM cable (supplied with this package) that links the CN8000 to your server or KVM switch plugs in here.
4	Console Port	The CN8000 can be accessed via a local console as well as over the Net. The cable for the local console (keyboard, monitor, and mouse) plugs in here. The console can use either a PS/2 or USB keyboard and mouse. Each connector is color coded and marked with an appropriate icon to indicate itself.
5	PON Port	This port is made available for use with a Power over the NET™ remote power management module. If you connect a PON device, its cable plugs in here. Refer to the User Manual that came with the PON device for operation details.
6	RS-232 Port	This serial port is provided for out-of-band and low bandwidth modem and serial terminal connections.

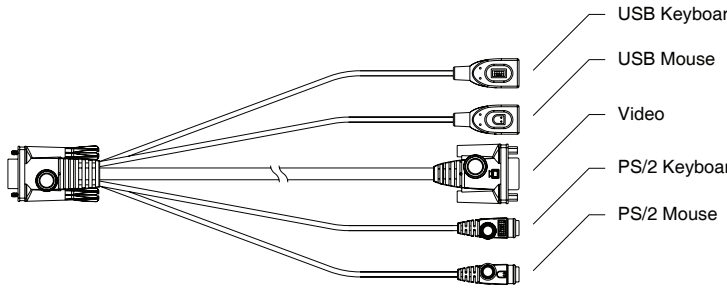
Custom KVM Cables



No.	Description
1	For use with PS/2 configuration servers or KVM switches.
2	For use with USB configuration servers or KVM switches.

Note: The advantage of using a USB cable is that it allows automatic *locked-in* mouse synchronization. See *Mouse Sync Mode*, page 36, for details.

Custom Console Cable



Note: You can use any combination of keyboard and mouse connections. For example, you can use a PS/2 keyboard with a USB mouse.

Chapter 2
Hardware Setup

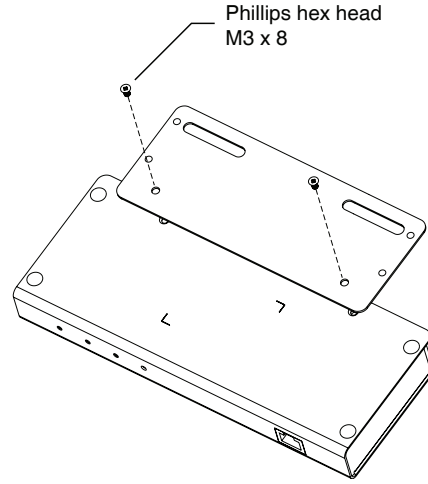
1. Important safety information regarding the placement of this device is provided on page 107. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.

Mounting

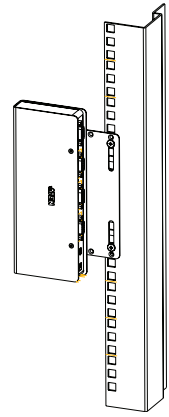
Rack Mounting

For convenience and flexibility, the CN8000 can be mounted on a system rack. To rack mount the unit do the following:

1. Remove the two original screws from the bottom of the unit (near the rear of the unit).
2. Using the screws provided with the rack mount kit, screw the mounting bracket into the CN8000 – as shown in the diagram below.



3. Screw the bracket into any convenient location on the rack.

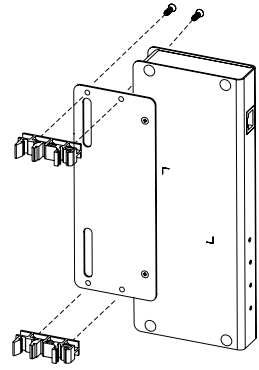


Note: Rack screws are not provided. Use screws that are appropriate for your rack.

DIN Rail Mounting

To mount the CN8000 on a DIN rail:

1. Screw the mounting bracket to the back of the CN8000 as described in steps 1 and 2 of the wall mounting procedure.
2. Use the larger screws supplied with the Rack Mount Kit to screw the DIN rail brackets to the mounting bracket – as shown in the diagram, below:



3. Hang the unit on the DIN rail.

Installation

Cabling Up

To install the CN8000, refer to the installation diagrams on the next page (the numbers correspond to the numbers of the steps), and do the following:

1. Use the Console cable provided with this package to connect the CN8000's *Console* port, to the local console keyboard, monitor and mouse.

   Note: 1. The Console cable comes with connectors for both PS/2 and USB mice and keyboards – use the ones appropriate for your installation.

   2. You can use any combination of keyboard and mouse connections. For example, you can use a PS/2 keyboard with a USB mouse.

2. Use the KVM cable provided with this package to connect the CN8000's *PC/KVM* port, to the keyboard, video and mouse ports of the server or KVM switch that you are installing.

   Note: The diagram shows a connection to a KVM switch with PS/2 mouse and keyboard ports using a PS/2 KVM cable set. The CN8000 can also connect to a server or KVM switch that uses a USB connection by using a USB KVM cable set. See *Cables*, page 5, for cable option information.

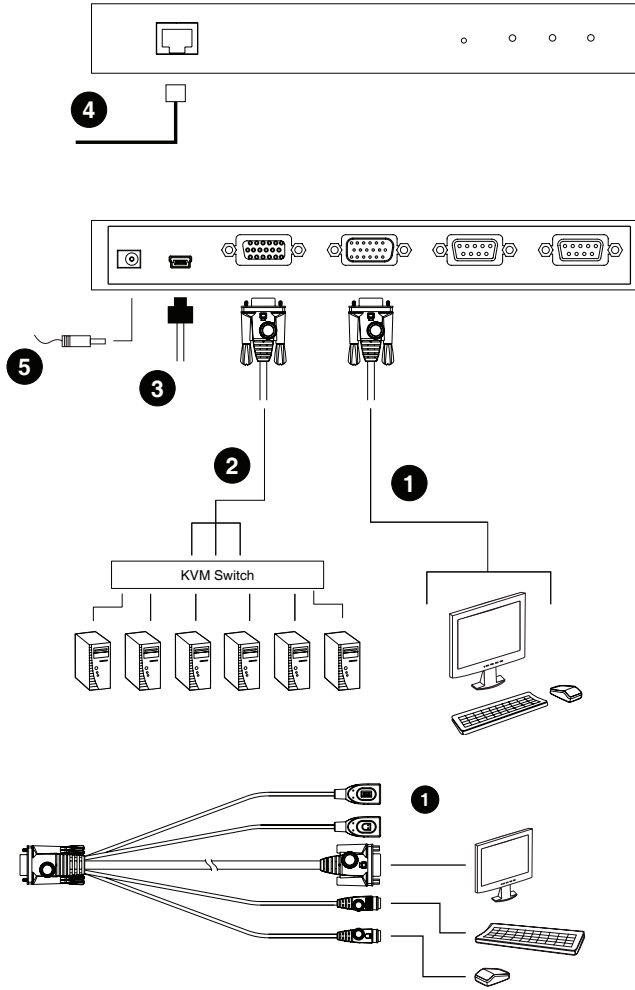
3. If you want to use the virtual media function (see *Virtual Media*, page 47), plug the USB 2.0 *Virtual Media Cable* provided with this package from the server's USB port into the CN8000's Virtual Media port.

   Note: This step is optional.

4. Plug the LAN or WAN cable into the CN8000's LAN port.
5. Plug the power adapter cable into the CN8000's power jack, then plug the power adapter into an AC power source.

Starting Up

Installation is complete, and you are ready to start up. When starting up, be sure to first power on the CN8000, then power on the server or KVM switch.


4
5
3
2
1
KVM Switch
1
2

Chapter 3
Browser Login

The CN8000 can be accessed either from an internet type browser, via Windows and Java application (AP) program, or by PPP modem dial-in. The next several chapters describe browser-based operations; AP access is discussed in Chapter 9; PPP modem login is discussed on page 114.

Logging In

To operate the CN8000 from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the CN8000 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/CN8000
```

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 CN8000's IP address are described in the Appendix on page 111.

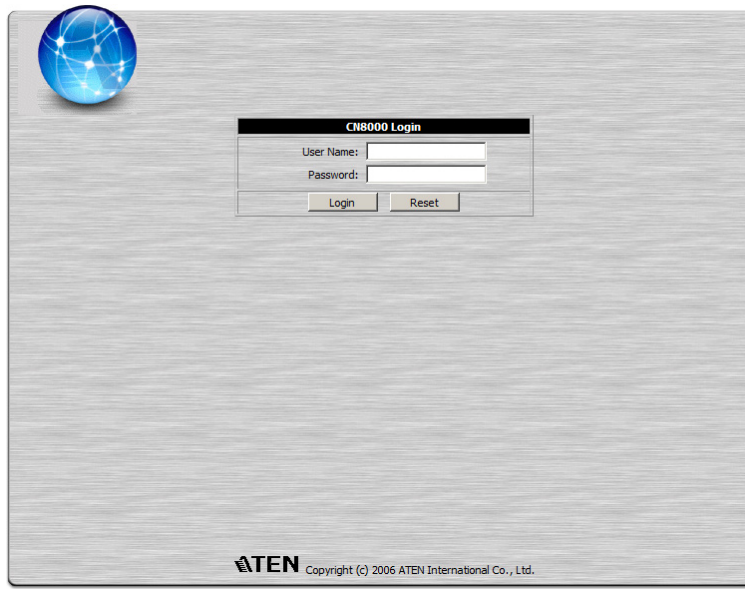
(Continues on next page.)

(Continued from previous page.)

2. A *Security Alert* dialog box appears.

Accept the certificate – it can be trusted. (See *Trusted Certificates*, page 122, for details.) If a second certificate appears, accept it as well.

The CN8000 login page appears:



3. Provide a valid Username and Password (set by the CN8000 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 33).

2. If you supplied an invalid login, the authentication routine will return this message: *Invalid Username or Password. Please try again.* If you see this message, log in again being careful with the Username and Password.

After you have successfully logged in, the CN8000 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 33, 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 a Power over the NET™ module is connected to your installation, and if you have the proper permission (see *User Management*, page 33), clicking this icon will bring up its interface.
	**Log:** All the events that take place on the CN8000 are recorded in a log file. If you have the proper permission (see *User Management*, page 33), clicking this icon displays the contents of the log file. The Log File is discussed in Chapter 7.
	**Logout:** Click this icon to log out and end your CN8000 session. It is important to log out when you end your session. Otherwise, you must wait until the timeout setting has expired before the CN8000 can be accessed again. (See *Timeout*, page 35.)

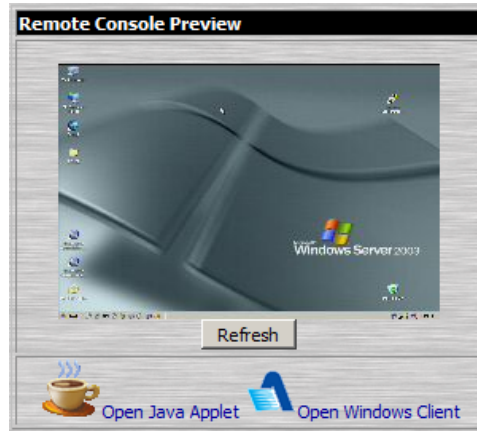
Administration Icons

The icons arranged horizontally across the top of the page are linked to the administration utilities, which are used to configure the CN8000. The ability to make configuration changes depends on the permissions associated with a user's login information (see *User Management*, page 33). The administrative functions are discussed in Chapter 4.

Note: The *General* icon is non-configurable and is available to all users.

Remote Console Preview

The main portion of the screen shows a snapshot of the server's 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	Clicking *Open Java Applet* uses a Java applet to open the remote server's display on your desktop. The Java Applet provides multi-platform access to the CN8000. **Note:** To use the Java Applet, Sun's Java Runtime Environment (JRE) 6, Update 3, or higher must be installed on your computer.
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.

CN8000 operation using the Java applet is discussed in Chapter 6; CN8000 operation using the Windows client is discussed in Chapter 5.

Chapter 4
Administration

Introduction

The administration utilities, represented by the icons located across the top of the CN8000 web page, are used to configure the CN8000's operating environment.

This chapter discusses each of them in turn.

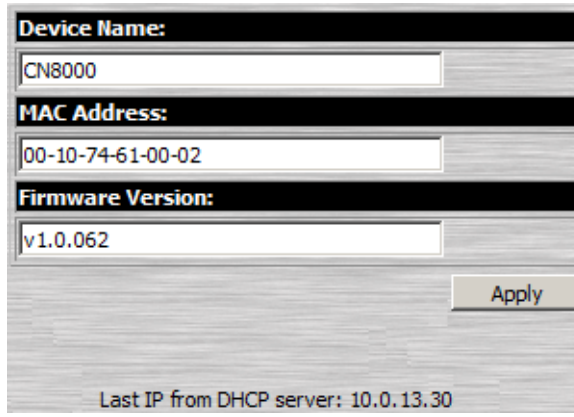
Note: 1. As you make your configuration changes in each dialog box, click **Apply** to save them.

2. Some configuration changes only take effect after an CN8000 reset. For those changes, a check is automatically put in the *Reset on Exit* box (see *Customization*, page 35). 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 33), the Administration configuration dialogs are not available.

General

The *General* page is the first of the Administration pages, and provides information about the CN8000's status.

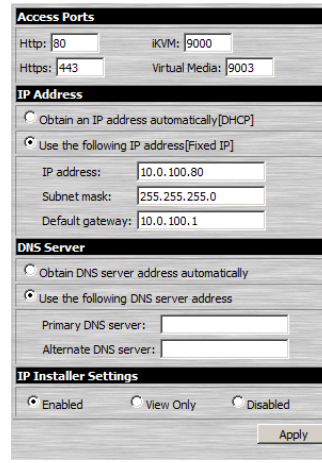


An explanation of each of the fields is given in the table below:

Field	Explanation
Device Name:	To make it easier to manage installations that have more than one CN8000, each one can be given a name. To assign a name for the CN8000, key in one of your choosing here (16 characters max.).
MAC Address:	The CN8000's MAC Address displays here.
Firmware Version:	Indicates the CN8000's current firmware version level. New versions of the CN8000's firmware can be downloaded from our website as they become available (see *Firmware Upgrade*, page 38). You can reference this number to see if there are newer versions available on the website.
Last IP from DHCP Server	If the CN8000 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 CN8000's network environment.



Access Ports

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). Users must specify the port number as part of the IP address when they connect to the CN8000. If an invalid port number (or no port number) is specified, the CN8000 will not be found. An explanation of the fields is given in the table below:

Field	Explanation
iKVM:	This is the port number that must be specified when connecting to the CN8000 from the stand-alone Windows software program. Valid entries are from 1024–65535. The default is 9000.
Virtual Media:	This is the port number used for data transfer using the CN8000'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: 1. If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.

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

IP Address

The CN8000 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 CN8000 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 111, 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 CN8000 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.

(Continues on next page.)

(Continued from previous page.)

IP Installer Settings

An IP Installer utility (IPInstaller.exe) is provided on the software CD that came with this package. It offers a simple method to ascertain and configure IP related settings for the CN8000. When the IP Installer is invoked, it scans the network for CN8000 devices and displays the ones it finds.

- Selecting *Enabled*, allows you to see the IP settings of the devices that were found, and to use the utility to set new IP addresses.
- Selecting *View Only*, allows you to see the IP settings of the devices that were found, but you cannot make any changes to the settings.
- Selecting *Disabled*, means that the CN8000 will not show up in the IP Installer's list of found devices.

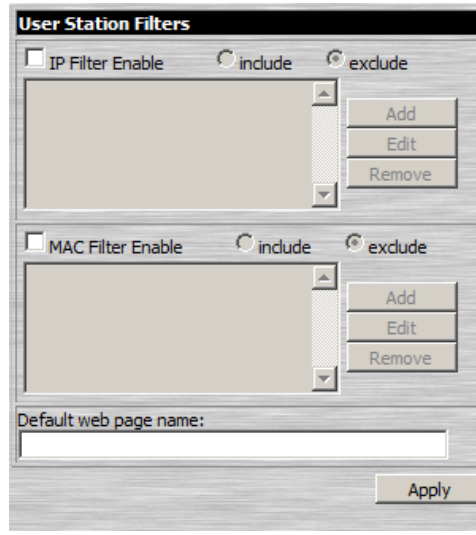
See *IP Installer*, page 111, for operation details.

Finishing Up

After making any network changes, be sure *Reset on exit* on the *Customization* page (see *Customization*, page 35) 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 CN8000 off and on.

Security

The Security page is used to control access to the CN8000.



Overview

- *IP* and *MAC Filters* control access to the CN8000 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 CN8000 with a browser. For example:

  ```
  192.168.0.126/CN8000
  ```

  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 CN8000 with a Web browser using the IP address alone. This makes the installation less secure.

Filtering

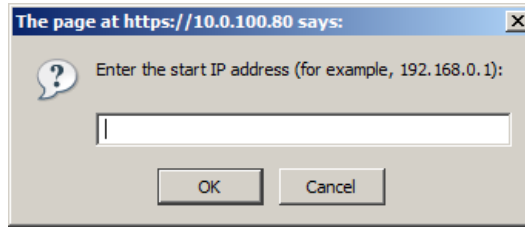
To enable IP and/or MAC filtering, **Click** to put a check mark in the *IP Filter Enable* and/or *MAC Filter Enable* checkbox. There are a maximum of 100 filters allowed for each.

- If the *include* button is checked, all the addresses within the filter range are allowed access to the CN8000; all other addresses are denied access.
- If the *exclude* button is checked, all the addresses within the filter range are denied access to the CN8000; all other addresses are allowed access.

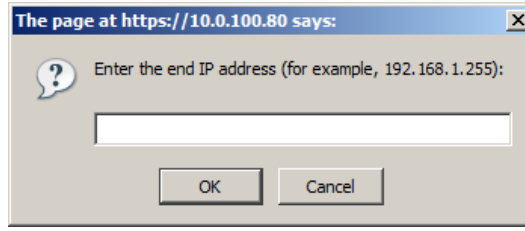
IP Filtering

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.

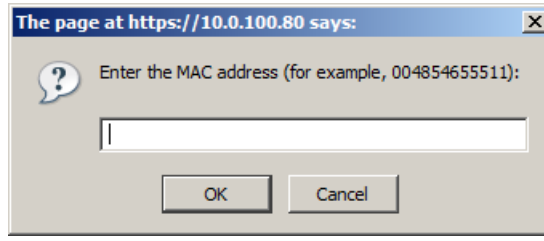
To delete a filter, select it and click **Remove**.

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.

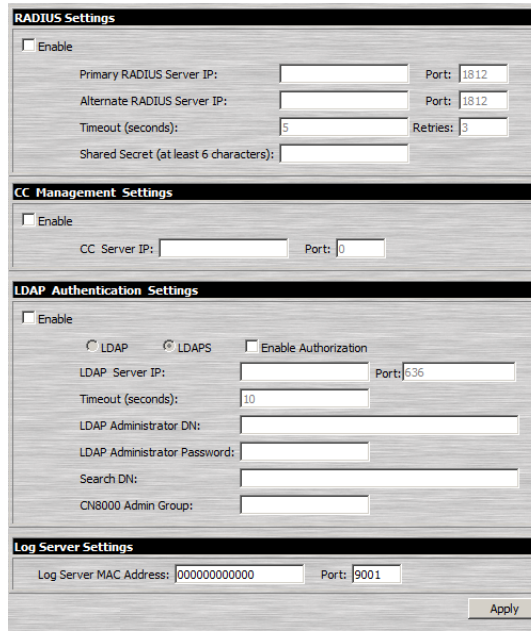
IP Filter / MAC Filter Conflict

If there is a conflict between an IP filter and a MAC filter – for example, where a computer's IP address is allowed by the IP filter but it's MAC address is excluded by the MAC filter – then that computer's access is blocked.

In other word's, if either filter blocks a computer, then the computer is blocked, no matter what the other filter is set to.

ANMS

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



RADIUS Settings

To allow authentication and authorization for the CN8000 through a RADIUS server, do the following:

1. Check **Enable**.
2. Fill in the IP addresses and port numbers for the Primary and Alternate RADIUS servers.
3. In the *Timeout* field, set the time in seconds that the CN8000 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 CN8000 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 the Java applet.
P	Allows the user to Power On/Off, Reset devices via an attached PN0108.
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. Capitals or lower case work equally well.

2. Characters are comma delimited.

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 access the attached PN0108
w,j,l	User can access the system via the Windows Client; user can access the system via the Java Applet; user can access log information via the user's browser.

CC Management Settings

To allow authorization for the CN8000 through a CC (Control Center) server, check *Enable* and fill in the CC Server's IP address and the port that it listens on in the appropriate fields.

LDAP / LDAPS Authentication and Authorization Settings

To allow authentication and authorization for the CN8000 via LDAP / LDAPS, refer to the information in the table, below:

Item	Action
Enable	Put a check in the *Enable* checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click a radio button to specify whether to use LDAP or LDAPS.
Enable Authorization	Select whether to enable *Enable Authorization*, or not. 1. If enabled (the box is checked), the LDAP / LDAPS server directly returns a 'permission' attribute and authorization for the user that is logging in. With this selection the LDAP schema must be extended. See *LDAP Server Configuration*, page 87, for details. 2. If not enabled (no check in the box), the result the server returns indicates whether the user that is logging in belongs to the 'CN8000 Admin Group'. If the result is 'yes' the user has full access rights; if the result is 'no', the user only has limited access rights. **Note:** Consult the LDAP / LDAPS administrator to ascertain whether to enable the *Enable Authorization* function, or not.
LDAP Server IP and Port	Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Timeout	Set the time in seconds that the CN8000 waits for an LDAP or LDAPS server reply before it times out.
LDAP Administrator DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: cn=LDAPAdmin,ou=cn8000,dc=aten,dc=com
LDAP Administrator Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. **Note:** If *Enable Authorization* is not checked, this field must include the entry where the *CN8000 Admin Group* is created. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.
CN8000 Admin Group	Key in the Group Name for CN8000 administrator users. **Note:** If *Enable Authorization* is not checked, this field is used to authorize users that are logging in. If a user is in this group, the user receives full access rights. If a user is not in this group, the user only receives limited access rights. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.

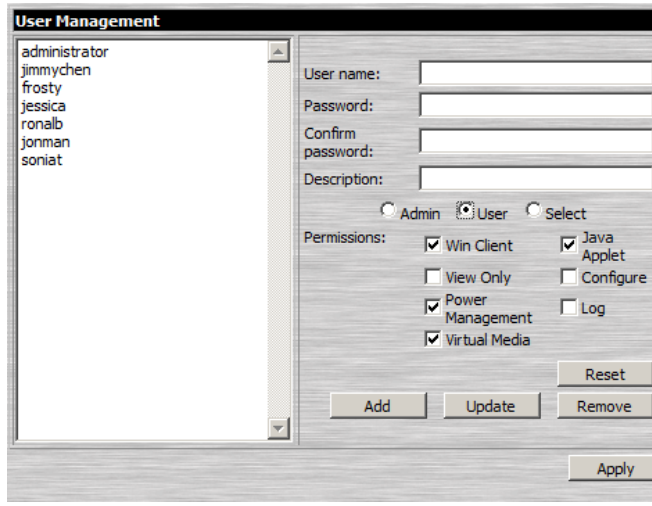
Log Server Settings

Important transactions that occur on the CN8000, 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 1024—65535. The default port number is 9001.

User Management

The User Management page 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 right panel, then click **Add**. The new user's name appears in the left panel.
- To delete a user profile, select it from the names displayed in the left panel, and click **Remove**. The user's name is removed from the panel.
- To modify a user profile, first select it from the list in the left panel; change the information that appears in the right panel; then click **Update**.

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 as is. If you do want to change the user's password, key the new password in the *Password* and *Confirm password* fields.

- The *Admin* and *User* radio buttons select automatically configured permissions. If you wish to modify these permissions, choose the *Select* radio button, then specify the permissions individually.

(Continues on next page.)

(Continued from previous page.)

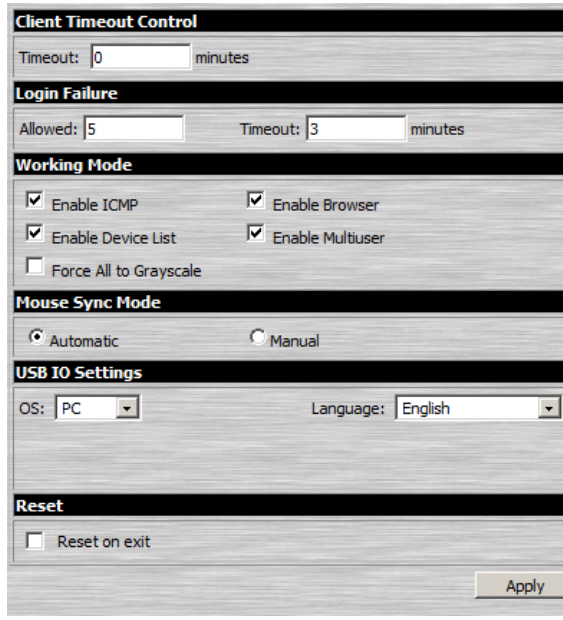
An explanation of the profile items is given in the table below:

Item	Explanation
Username	A minimum of 6 and a maximum of 16 characters is allowed.
Password	A minimum of 6 and a maximum of 16 characters 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 CN8000's operation. **Win Client:** Checking *Win client* allows a user to access the CN8000 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 CN8000, 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 devices via an attached Power Over the NET™ unit. **Virtual Media:** Checking *Virtual Media* allows a user to utilize the CN8000's Virtual Media capabilities (see *Virtual Media*, page 47 for details). **Java Applet:** Checking *Java Applet* allows a user to access the CN8000 via the Java Applet software. **Configure:** Checking *Configure* gives a user Administrator privileges, and allows the user to set up and modify the CN8000's operating environment. **Log:** Checking *Log* allows a user to view the contents of the log file.

- The **Reset** button clears all the information shown in the right panel.
- When you have made all your changes, click **Apply**.

Customization

The *Customization* page 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 CN8000 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. The default is 3 minutes.
Login failures	Allowed	Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 minutes.
	Timeout	Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.

(Continues on next page.)

(Continued from previous page.)

Item		Explanation
Working Mode	Enable ICMP	If *ICMP* is **enabled**, the CN8000 can be pinged and an IP address can be assigned with the ARP command. If it is not enabled, the device cannot be pinged, nor can it be assigned an IP address with the ARP command. The default is Enabled,
	Enable device list	If this item is **enabled**, the device will show up in the list of local CN8000 units on the AP Windows Client Connection screen (see *The Windows Client Connection Screen*, page 75). If it is not enabled, it will not show up. The default is Enabled,
	Force All to Grayscale	If *Force All to Grayscale* is enabled, the remote display for all users is changed to grayscale. This can speed up I/O transfer in low bandwidth situations. The default is Disabled,
	Enable browser	Placing a check in this box allows the user to access the CN8000 from a browser. If this function is not enabled, users will not be able to log into the unit via their browsers. The default is Enabled,
	Enable multiuser	Enabling *Multiuser* operation permits more than one user to log into the CN8000 at the same time. The default is Enabled,
Mouse Sync Mode	Automatic	This is the default. Selecting *Automatic* allows an automatic *locked-in* synching of the remote and local mouse pointers. **Note:** This feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you 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 46, and page 58. **Note:** 1. Sun systems must use the Manual setting. 2. If you use the Manual setting it may also be necessary to make additional mouse movement settings. See *Additional Mouse Synchronization Procedures*, page 120, for further help, if necessary.

(Continues on next page.)

(Continued from previous page.)

Parameter		Explanation
USB IO Settings	OS	When connecting to a computer or KVM switch with the USB connector for keyboard and mouse I/O, drop down the list to select the platform it uses. Choices are PC, Mac1, Mac2, and Sun. Default is PC. **Note:** In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.
	Language	When connecting to a computer or KVM switch with the USB connector for keyboard and mouse I/O, drop down the list to select the keyboard language it uses.
Reset		Some configuration changes only take effect after a CN8000 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 CN8000's performance degrades, reset it by putting a check in the *Reset on Exit* box, and then log out / log in.

Maintenance

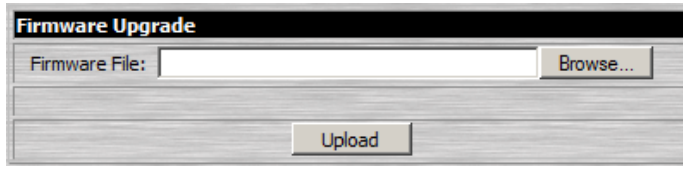
The *Maintenance* page allows the Administrator to upgrade the CN8000's firmware, and to backup and restore the CN8000's configuration settings and user profile information.

Firmware Upgrade

As new versions of the CN8000 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 your computer.
2. Open your browser; log in to the CN8000; 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, a message appears on the screen to inform you that the operations succeeded. Click **Logout** at the bottom left of the Main web page.
6. In the screen that comes up click **Yes** to confirm that you want to exit and reset the CN8000.

Note: You will need to wait a bit before logging back in.

Backup Configuration / User Accounts

The *Backup Configuration / User Accounts* section of the page gives you the ability to back up the CN8000's configuration and/or user profile information.

To perform a backup, do the following:

1. In the *Password* field, key in a password for the file.

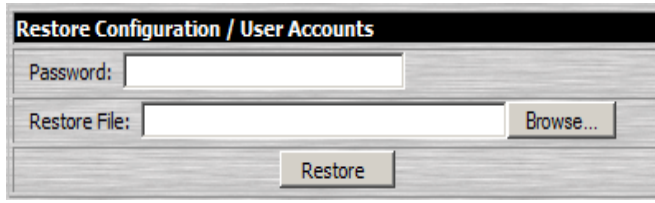
   Note: Make a note of the password, since you will need it to be able to restore the file.

2. Click a radio button to select which information to backup: the configuration information; the user profile information; or both.
3. Click **Save**.
4. When the browser asks what you want to do with the file, select *Save to disk*; then save it in a convenient location.

   Note: The CN8000 saves all its backup files as *CN8000BKUP.conf*. If you want to save more than one backup file, simply rename the file to something convenient when you save it.

Restore Configuration / User Accounts

Saved Configuration / User Accounts information can be restored with the *Restore Configuration / User Accounts* section of the page.



To restore a previous backup, do the following:

1. In the *Password* field, key in the same password that you used to save the file.
2. Click **Browse**; navigate to the file and select it.

   Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

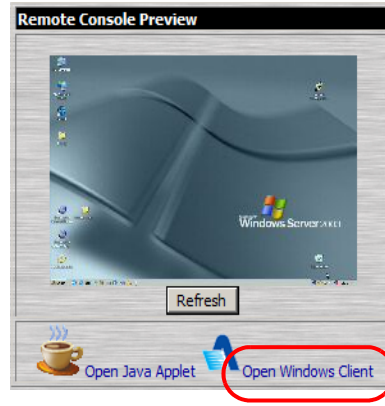
3. Click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.

Chapter 5
The Windows Client

Starting Up

To start the Windows client, after you log in (see *Logging In*, page 15), click the *Open Windows Client* link on the *Remote Console Preview* panel.



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.

- You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.
- To switch between your local and remote programs, minimize the Windows Client window and use [Alt + Tab] as you normally would.

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 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 functions that the icons perform are explained on the following page.
- The text bar performs two functions: normally it displays the remote server's video resolution; however, if you receive a message via the message board and your message board is not open, the message scrolls in this bar. See *The Message Board*, page 49, for more information about the message board.

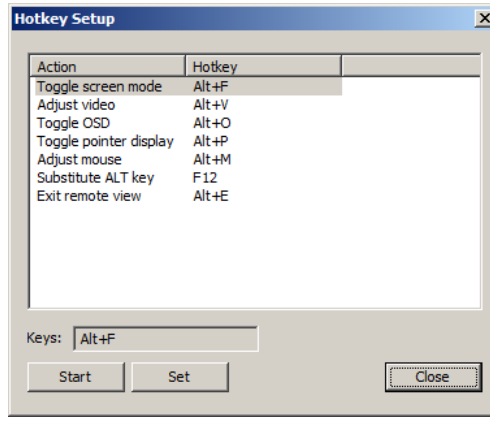
Note: You can move the control panel to any convenient location on the screen by moving the mouse pointer over one of its borders and dragging.

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 44 for details).
	Click to bring up the Video Settings dialog box.
	Click to toggle the remote display between grayscale and color.
	Click to bring up the *Virtual Media* dialog box. The red *X* indicates that the function has not been started. The icon changes when a virtual media device is started to indicate the type of device being used. See *Virtual Media*, page 47, for specific details.
	Click to open the Message Board.
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to enable an on-screen keyboard. Click the arrow to drop down a list of available language keyboards to select from.
	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.
	Click to display information about the Widnows Client version.

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 CN8000, [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 CN8000 and returns to local operation.

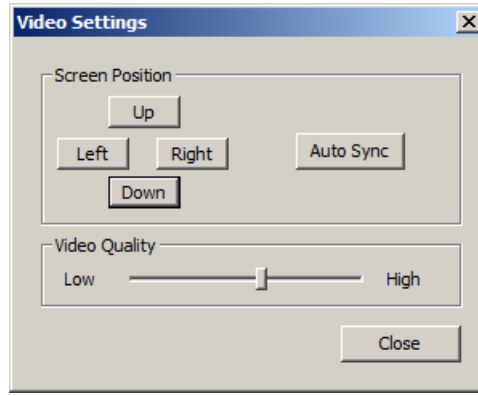
Configuring the Hotkeys

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.

Grayscale

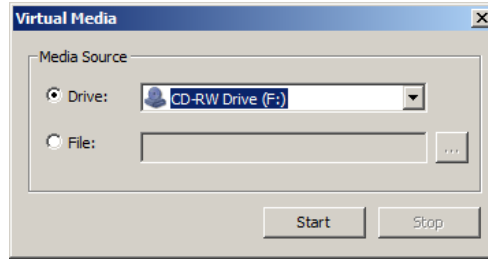
Click this button to toggle the remote display between grayscale and color.

Virtual Media

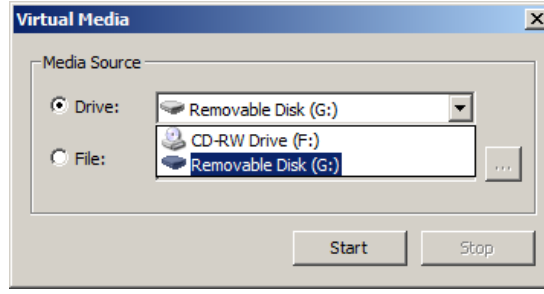
The CN8000's virtual media feature allows a USB 1.1 or 2.0 device (Floppy drive, CDROM, Flash Drive, etc.), or an image file, on a user's system, to appear, and act, as if it were installed on the remote server.

To implement this redirection feature, do the following:

1. Bring up the *Virtual Media* dialog box:

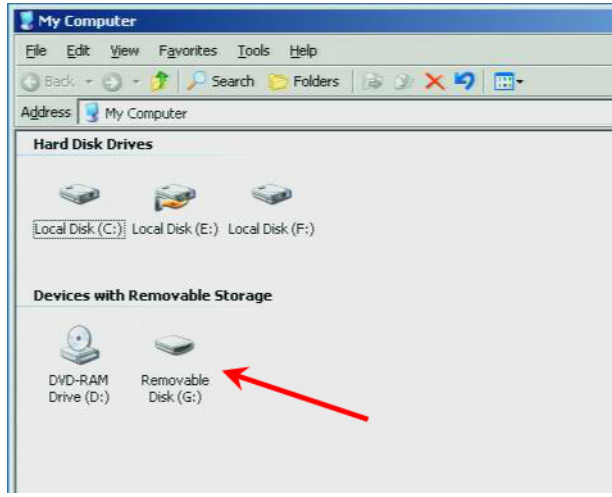


2. Select the media source.
   a) If you select *Drive*, drop down the drive list to select the appropriate drive:



   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 or folder 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 folder, 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**.

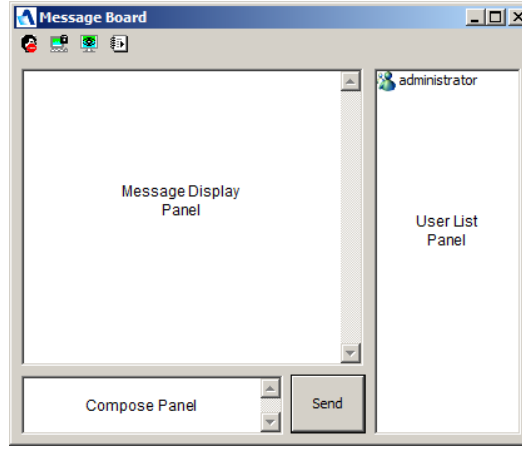
Virtual Media Icons

The Virtual Media icon on the Windows Client Control Panel changes, depending on the type of drive used, as shown in the table below:

Icon	Function
	Indicates a DVD-ROM or CDROM drive.
	Indicates a flash (pen) drive.
	Indicates a floppy drive.

The Message Board

The CN8000 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 button is shadowed when Chat is disabled. 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 button is shadowed when the KVM is occupied. 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 button is shadowed when the KM is occupied. 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. The button is shadowed when the User List is open.

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.

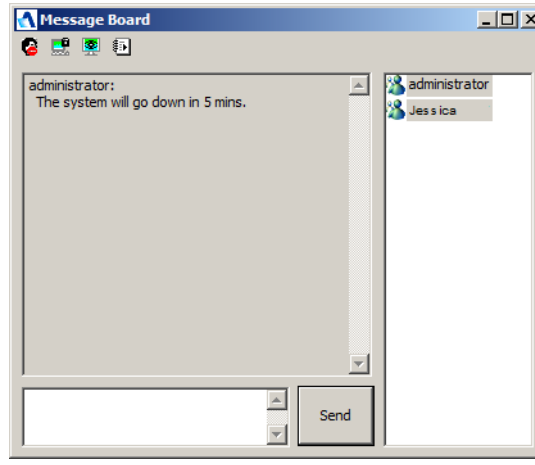
Message Display Panel

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

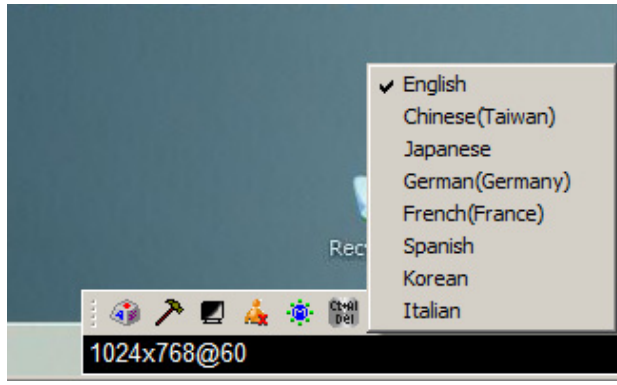
The names of all the logged in users are listed in this panel.

- 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.



On-Screen Keyboard

The CN8000 supports an on-screen keyboard, available in multiple languages. Click on the arrow to the right of the icon to display the list of available languages:



After selecting your language, click the icon to bring up the keyboard. In the future, having selected the language, you only need to click the icon.

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.

About

Click this button to see information about the Windows Client version.

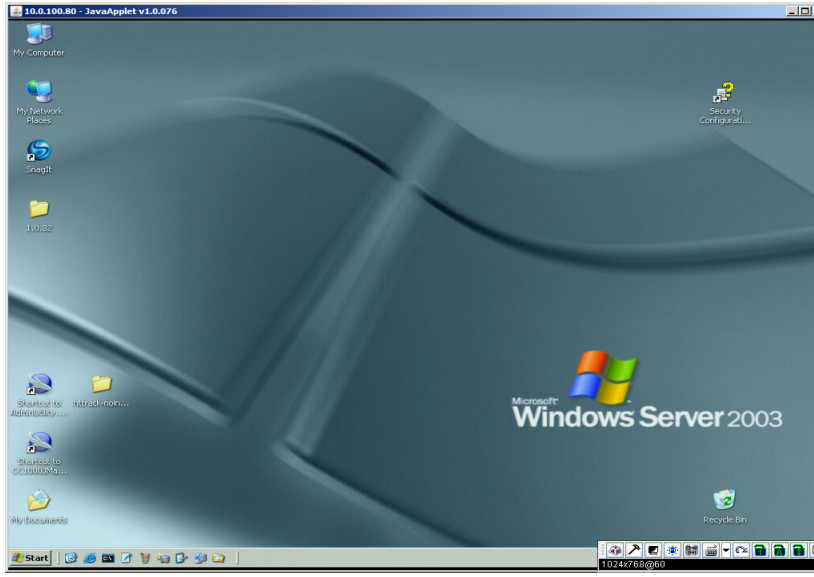
Chapter 6
The Java Applet

Introduction

The Java Applet makes the CN8000 accessible to all platforms that have the Java Runtime Environment (JRE) installed. (See *System Requirements*, page 4, for the required JRE version.) The JRE is available for free download from the Java web site (http://java.com).

To run the Java Applet, after you log in (see *Logging In*, page 15), Click the *Open Java Applet* link. After a second or two, the remote server's display appears as a window on your desktop.

Note: If a security dialog box appears, accept the certificate.



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 functions that the icons perform are explained on the following page.
- The text bar performs two functions: normally it displays the remote server's video resolution; however, if you receive a message via the message board and your message board is not open, the message scrolls in this bar. See *Message Board*, page 59, for more information about the message board.

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.)

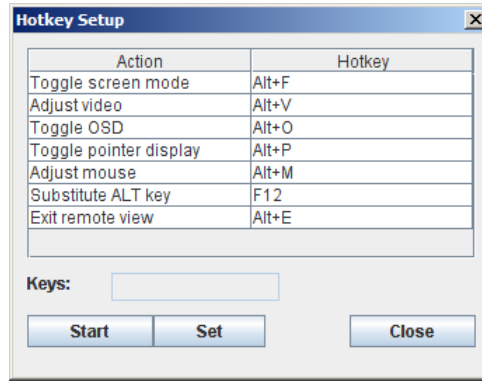
The functions that the icons perform is described in the table below:

Icon	Function
	Click to bring up the *Hotkey setup* dialog box (see *Hotkey Setup*, page 56 for details).
	Click to bring up the *Video settings* dialog box.
	Click to toggle the remote display between grayscale and color.
	Click to bring up the *Message board* (see page 59).
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to enable an on-screen keyboard. Click the arrow to drop down a list of available language keyboards to select from.
	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.
	Click to display information about the Java Applet version.

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 CN8000, [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 CN8000 and returns to local operation.

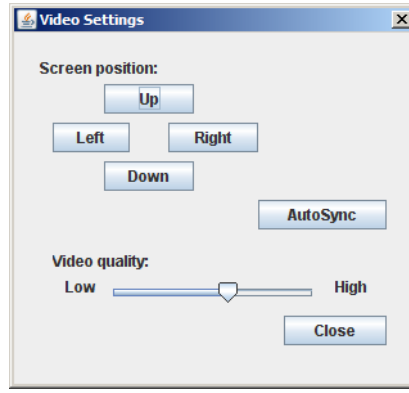
Configuring the Hotkeys

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:

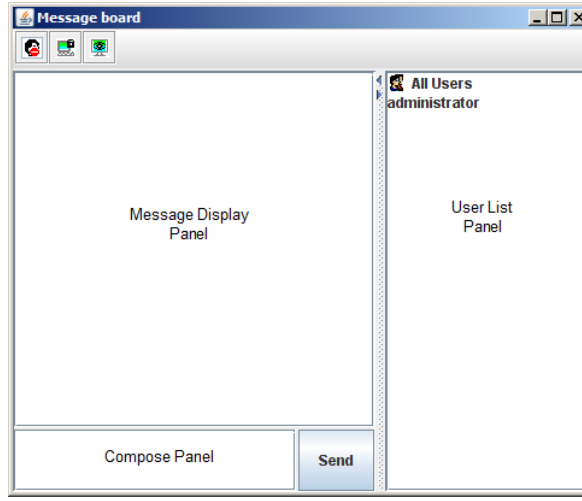
Option	Usage
Screen position	Adjust the horizontal and vertical position of the remote computer window by Clicking the Arrow buttons.
AutoSync	Click Auto-Sync to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen. 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.

Grayscale

Click this button to toggle the remote display between grayscale and color.

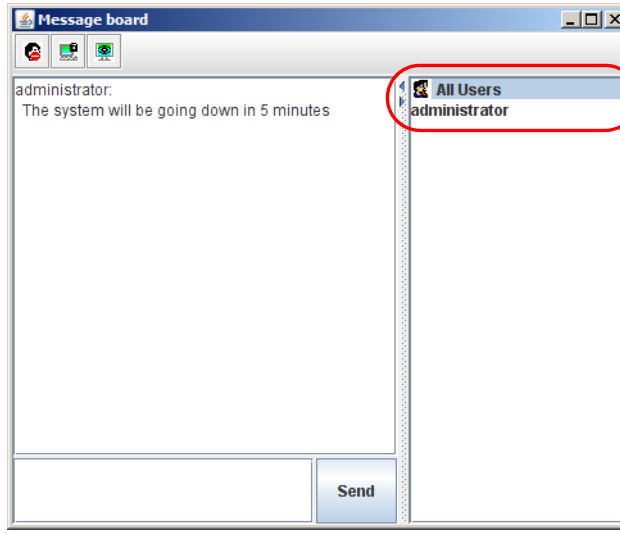
Message Board

The CN8000 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 button is shadowed when Chat is disabled. 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 button is shadowed when the KVM is occupied. 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 button is shadowed when the KM is occupied. 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.

On-Screen Keyboard

The CN8000 supports an on-screen keyboard, available in multiple languages. Click on the arrow to the right of the icon to display the list of available languages:

After selecting your language, click the icon to bring up the keyboard. In the future, having selected the language, you only need to click the icon.

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.

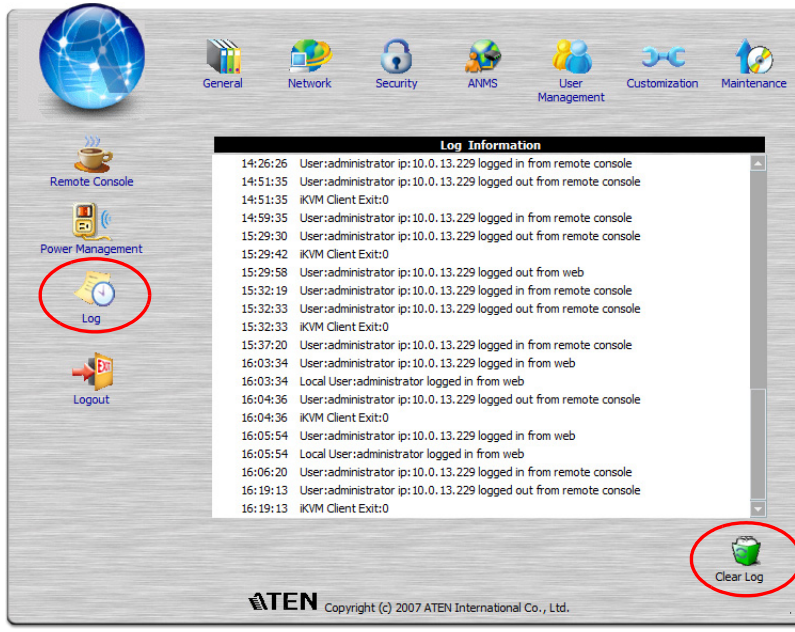
About

Click this button to see information about the Java Applet version.

Chapter 7
The Log File

The Log File Screen

The CN8000 logs all the events that take place on it. Following a reset, it writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the lower left of the page. A screen similar to the one below appears:



(Continues on next page.)

(Continued from previous page.)

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.

Note: To maintain and view a record of all the events that take place (not just the most recent 512), set up the Log Server AP program. see *The Log Server*, page 65.

To clear the log file, click on the *Clear Log* icon at the lower right of the page.

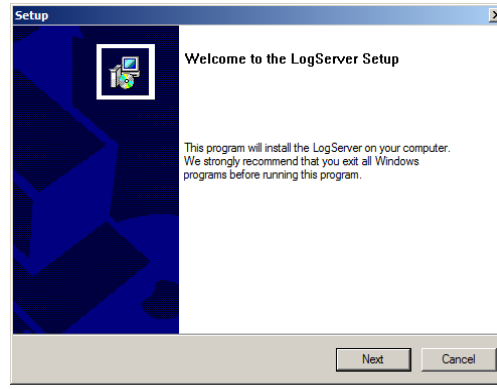
Chapter 8
The Log Server

The Windows-based Log Server is an administrative utility that records all the events that take place on selected CN8000 units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. From the computer that you want to use as the Log Server, open your browser and log into the CN8000 (see page 15).
2. Click the *Log Server* button at the left of the Webpage to start the Log Server installation program.
3. If any security warning dialog boxes appear, ignore them and click **Run** or **Open**.

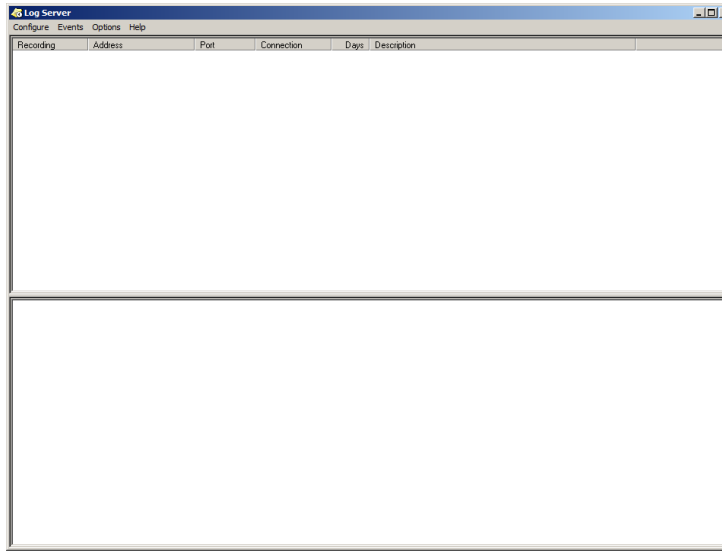
Note: If the browser cannot run the file, save it to disk, instead, and run the file from your disk.



4. Click **Next**. Then follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.

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 29 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 CN8000 units in the middle (see *The Log Server Main Screen*, page 71, 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.

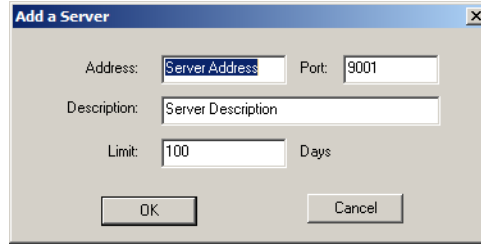
Note: If the Menu Bar appears to be disabled, click in the CN8000 List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new CN8000 units to the CN8000 List, edit the information for units already on the list, or delete CN8000 units from the list.

- To add a CN8000 to the CN8000 List, click **Add**.
- To edit or delete a listed CN8000, first select the one you want in the CN8000 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:



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

Field	Explanation
Address	This can either be the IP address of the CN8000 or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the CN8000 in the *ANMS* settings (see *ANMS*, page 29).
Port	Key in the port number that was specified for the CN8000 in the *ANMS* settings (see *ANMS*, page 29).
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.

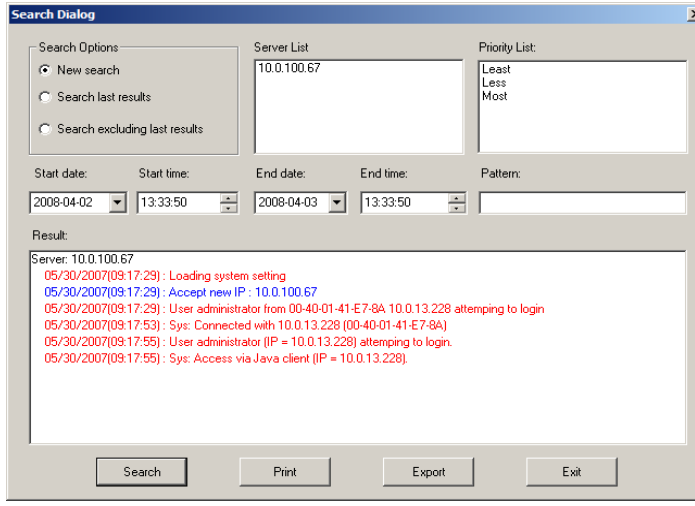
Fill in or modify the fields, then click **OK** to finish.

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:

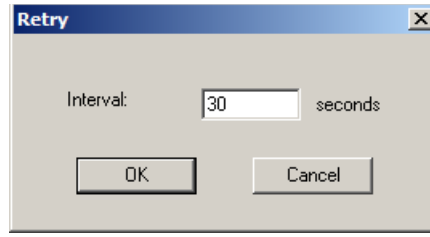
Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected CN8000.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected CN8000 *excluding* the events that resulted from the last search.
Server List	CN8000 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.
Export	Click this button to write the search results to a .txt file.
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 68).

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

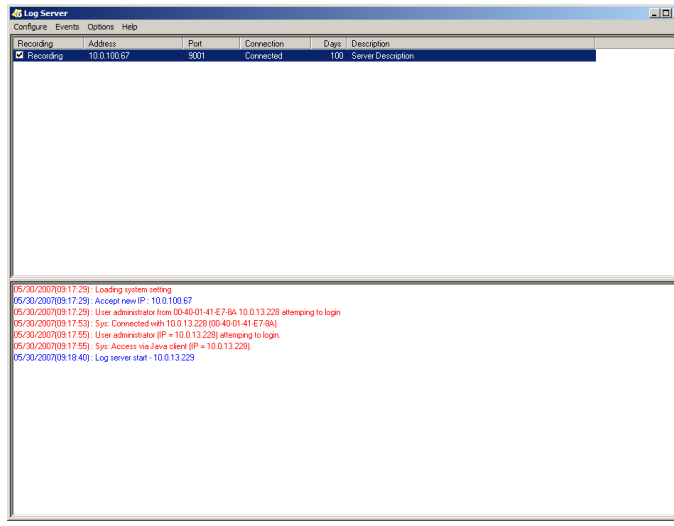
From the Help Menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

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

- The upper (List) panel lists the CN8000 units that have been selected for the Log Server to track (see *Configure*, page 67).
- The lower (Event) panel displays the log events for the currently selected CN8000 (the highlighted one - if there are more than one). To select a CN8000 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 CN8000 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 CN8000 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 CN8000 when it was added to the Log Server (see *Configure*, page 67).
Port	This is the port number that was assigned to the CN8000 when it was added to the Log Server (see *Configure*, page 67).
Connection	If the Log Server is connected to the CN8000, 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 29) and specified in the *Configure* dialog box (see *Configure*, page 67).
Days	This field displays the number of days that the CN8000's log events are to be kept in the Log Server's database before expiration (see *Configure*, page 67).
Description	This field displays the descriptive information given for the CN8000 when it was added to the Log Server (see *Configure*, page 67).

The Tick Panel

The lower panel displays tick information for the currently selected CN8000. 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.

Chapter 9
AP Operation

Introduction

In addition to the browser based client utilities, the CN8000 also provides stand-alone Windows and Java applications that can be used without a browser. The applications can be found on the CN8000 software CD. The Windows Client program is called *CN8000winclient.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 *CN8000winclient.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 – *CN8000 iClient* – is placed on your desktop and a program entry is made in the Windows *Start* menu:
(Start → All Programs → CN8000 → iClient).

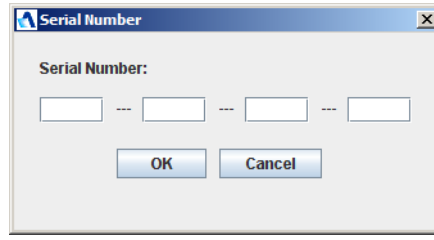
(Continues on next page.)

(Continued from previous page.)

Starting Up

To connect to the CN8000, 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.

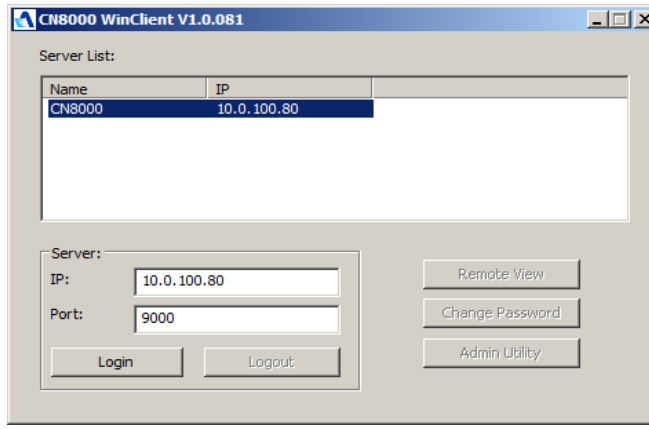


The serial number can be found on the CN8000's CD case. Key in the serial number - 5 characters per box - then click **OK** to bring up the CN8000 Connection Screen.

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

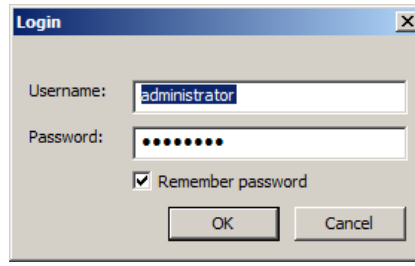


A description of the Connection Screen is given in the following table:

Item	Description
Server List	Each time the CN8000 iClient program is run, it searches the user's local LAN segment for CN8000 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 CN8000 at a remote location. If the IP address that appears isn't the one you want, or if there is no entry at all, key in the IP address you want. Next, 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 CN8000.
Logout	These buttons become active once you log into the CN8000. See page 77 for details.
Remote View	
Change Password	
Admin Utility	

Logging In

Once the CN8000 connects to the unit you specified, a login window appears:



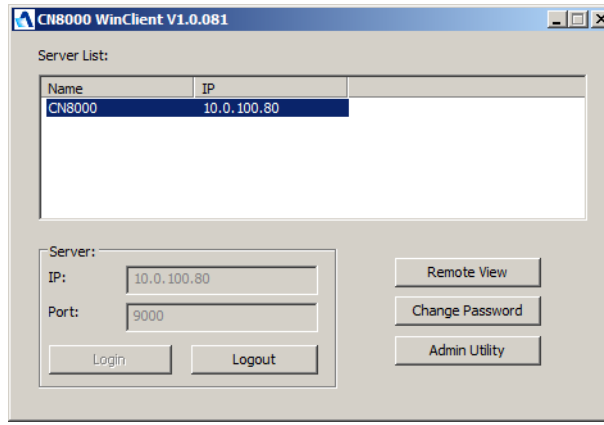
Provide a valid Username and Password, then Click **OK** to continue.

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 82, 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:

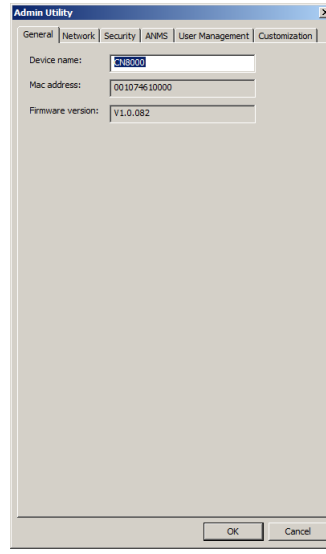
Button	Action
Logout	Breaks the connection to the CN8000.
Remote View	In some cases, administrator's do not wish to have users connect to the CN8000 with a browser. *Remote View* solves this problem. It opens a window on the user's desktop containing the remote server's display that is the same as the 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 CN8000 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:

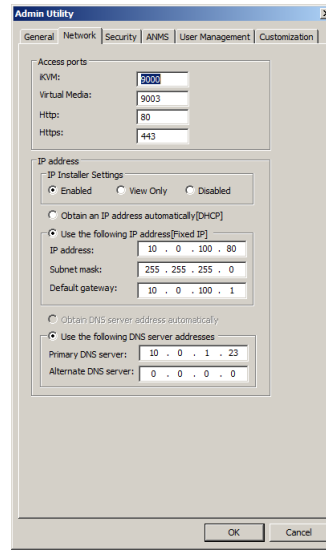


The General page provides information about the CN8000's status, as explained in the table, below:

Item	Description
Device Name:	To make it easier to manage installations that have more than one CN8000, each one can be given a name. To assign a name for the CN8000, erase the current name and key in one of your choosing (16 characters max.).
MAC Address	The CN8000's MAC Address displays here.
Main Firmware Version:	Indicates the mainboard's current firmware version level. New versions of the CN8000's firmware and authentication software can be downloaded from our web site as they become available (see *Upgrading the Firmware*, page 84, for details).

Network

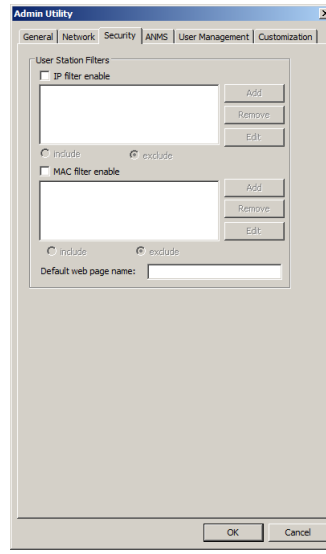
This page is used to specify the CN8000's network environment.



The settings on this page are essentially the same as that of the browser-based version. See *Network*, page 23, for details.

Security

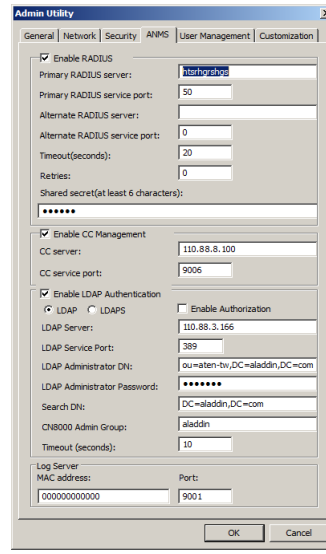
The Security page is used to control access to the CN8000.



The settings on this page are essentially the same as that of the browser-based version. See *Security*, page 26, for details.

ANMS

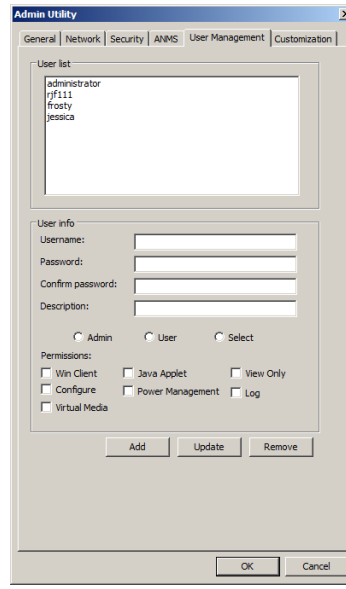
The Advanced Network Management Settings dialog box allows you to set up login authorization management from a external sources.



The settings on this page are essentially the same as that of the browser-based version. See *ANMS*, page 29, for details.

User Management

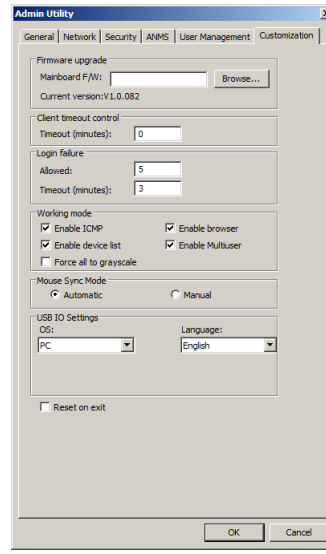
This page is used to set up and manage user profiles. It defines the access rights of each user. Up to 64 user profiles can be established



The settings on this page are essentially the same as that of the browser-based version. See *User Management*, page 33, for details.

Customization

This page allows the Administrator to upgrade the firmware and to set to set *Timeout*, *Login failure*, and *Working mode* parameters.



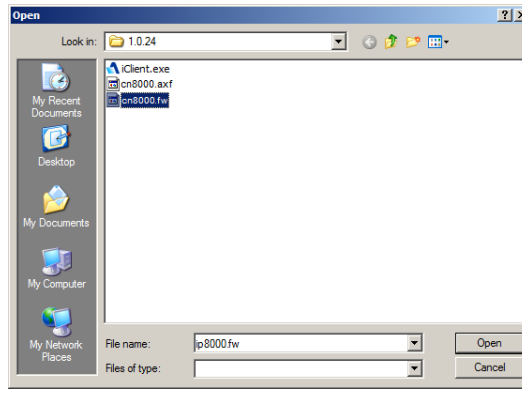
The settings on this page are essentially the same as that of the browser-based version. See *Customization*, page 35, for details on setting the parameters, and use of the *Reset on Exit* checkbox.

Note: The *Firmware Upgrade* section is used when upgrading the CN8000'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 83) 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**.



When you return to the Customization page, the file appears in the *Mainboard F/W* field.

3. Click OK to begin the upgrade.

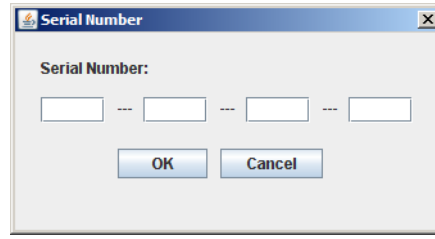
The AP Java Client

The Java Client is provided to make the CN8000 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://java.sun.com).

Starting Up

To connect to the CN8000 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.

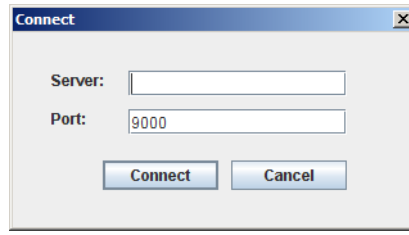
Note: If this is the first time that you are running the program a dialog box appears requesting you to input your serial number.



The serial number can be found on the CN8000's CD case. Key in the serial number - 5 characters per box - then click **OK** to bring up the CN8000 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

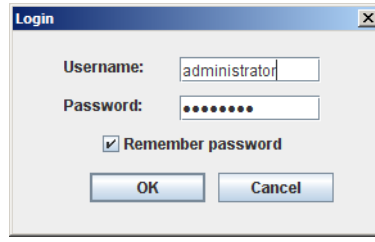


To connect to the CN8000

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 CN8000 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 82, 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.

Chapter 10
LDAP Server Configuration

Introduction

The CN8000 allows log in authentication and authorization through external programs. This chapter describes how to configure Active Directory and OpenLDAP for CN8000 authentication and authorization.

Active Directory

To allow authentication and authorization for the CN8000 via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the CN8000 – ***permission*** – is added as an optional attribute to the *person* class.

Note: *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.

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

The following section provides an example of configuring LDAP under Windows 2003 Server.

Install the Windows 2003 Support Tools

To install the Windows 2003 Support Tools, do the following:

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

Install the Active Directory Schema Snap-in

To install the Active Directory Schema Snap-in, do the following:

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

Create a Start Menu Shortcut Entry

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

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

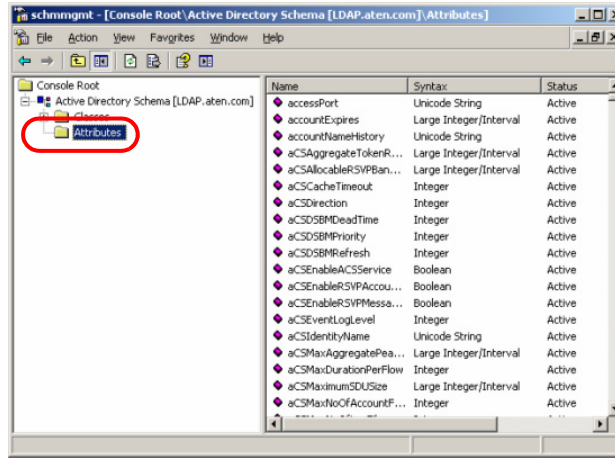
Extend and Update the Active Directory Schema

To extend and update the Active Directory Schema, do the following 3 procedures:

1. Create a New Attribute:

   a) Start → Administrative Tools → Active Directory Schema.

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



   c) Select New → Attribute.

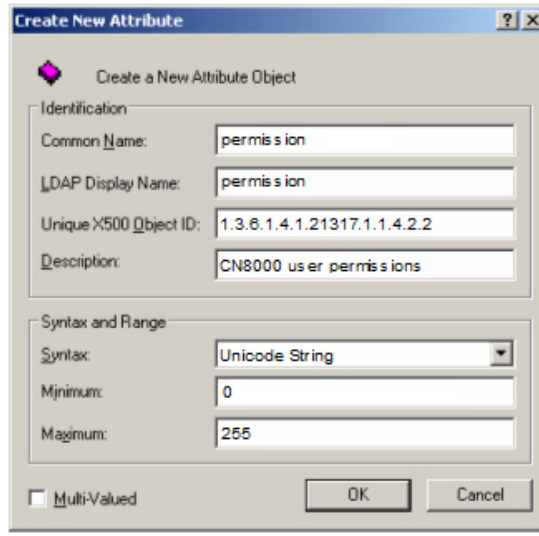
   d) In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

(Continues on next page.)

(Continued from previous page.)

e) Fill in the dialog box to match the entries shown below, then click **OK** to complete step 1 of the procedure.

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



2. Extend the Object Class With the New Attribute:

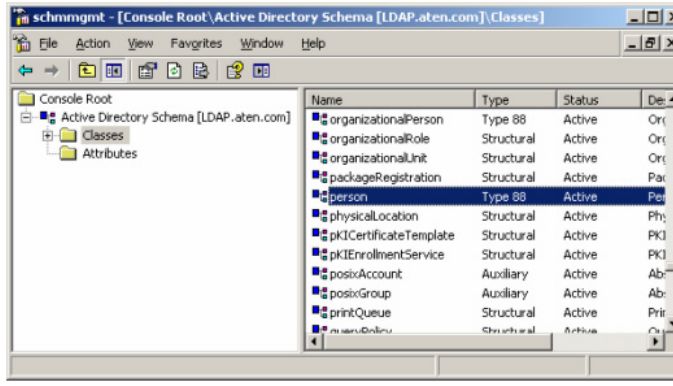
   a) Control Panel → Administrative Tools → Active Directory Schema.

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

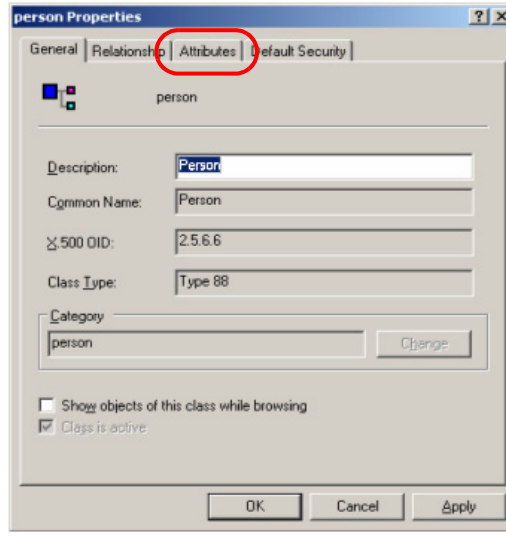
(Continues on next page.)

(Continued from previous page.)

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



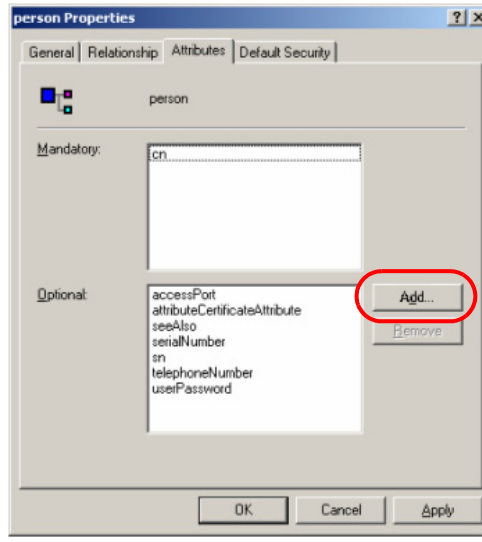
d) Select **Properties**; the *person Properties* dialog box comes up with the *General* page displayed. Click the *Attributes* tab.



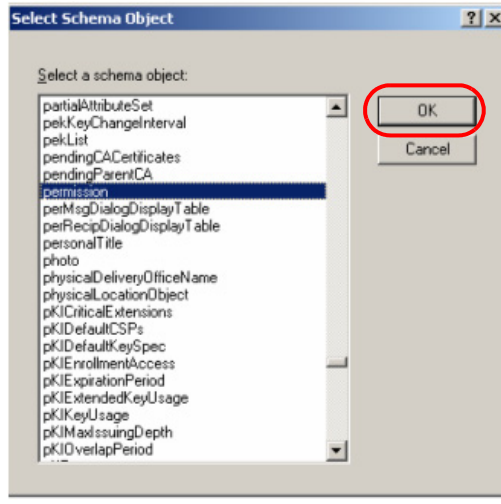
(Continues on next page.)

(Continued from previous page.)

e) On the *Attributes* page, click **Add**:



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

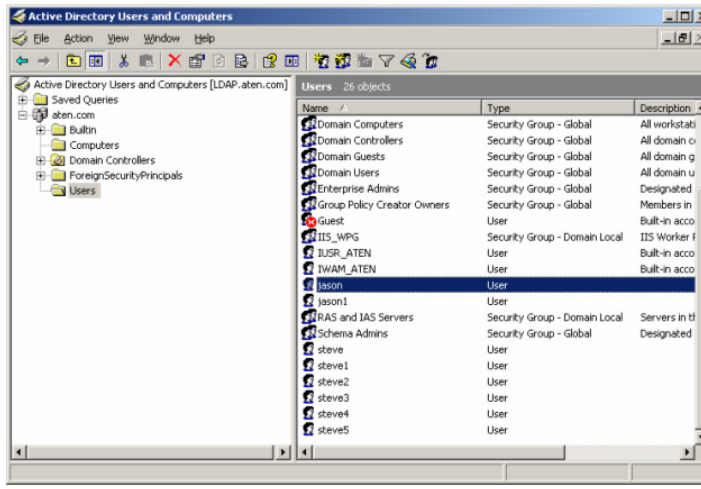


3. Edit Active Directory Users With the Extended Schema:

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

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

   c) Locate the user you wish to edit. (Our example uses *jason*.)

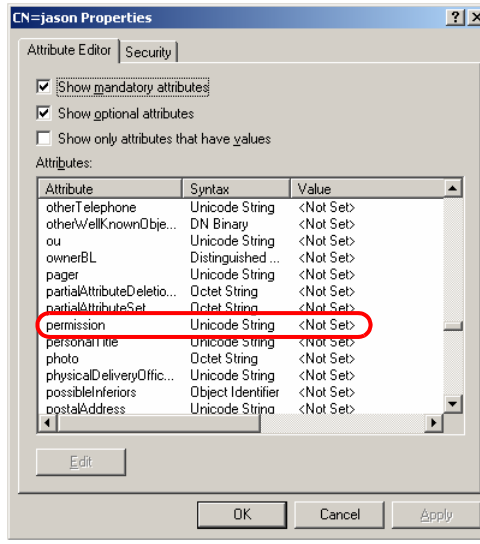


   d) Right-click on the user's name and select **properties.**

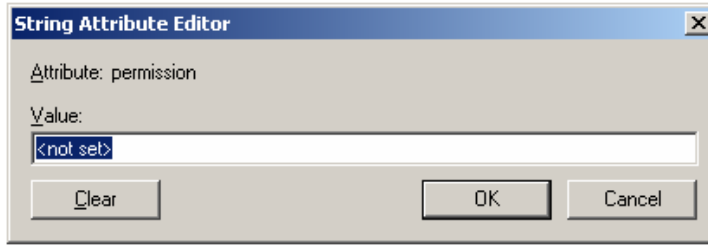
(Continues on next page.)

(Continued from previous page.)

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



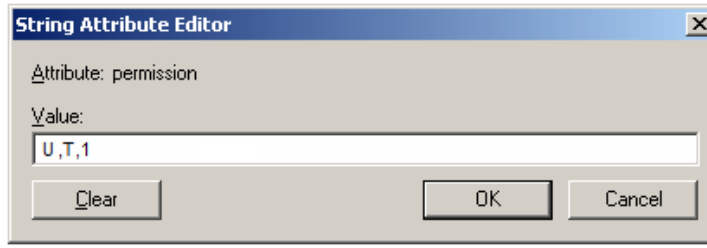
f) Click **Edit** to bring up the *String Attribute Editor*:



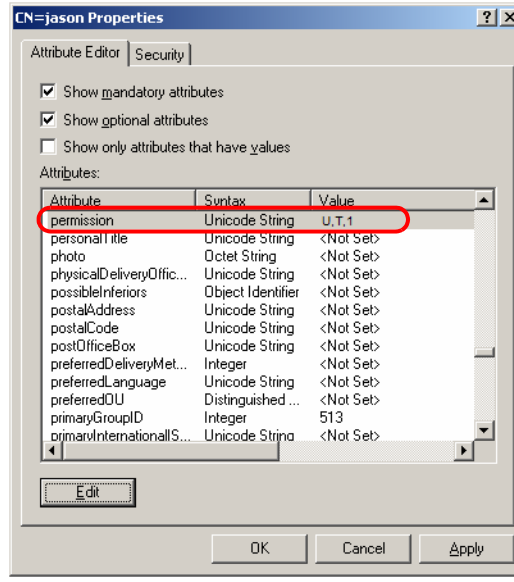
(Continues on next page.)

(Continued from previous page.)

g) Key in the desired CN8000 permission attribute values (see *The Permission Attribute Value*, page 96 for details). For example:



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



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

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

The Permission Attribute Value

The attribute value for *permission* is made up of two parts: 1) the IP address of the CN8000 a user will access; and 2) a string that indicates the access rights the user has on the CN8000 at that IP address. For example:

```
192.168.0.80&c,w,j;192.168.0.188&v,l
```

The makeup of the permission entry is as follows:

- An ampersand (&) connects the CN8000's IP with the access rights string.
- The access rights string is made up of various combinations of the following characters: c w j p l v s. The characters can be entered in upper or lower case. The meanings of the characters is provided in the *Permission String Characters* table, below.
- The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- If a user has access rights to more than one CN8000, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Permission String Characters

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 the Java applet.
P	Allows the user to Power On/Off, Reset devices via an attached PN0108.
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.

Permission Examples

Access rights examples are given in the table, below:

User	String	Meaning
User1	10.0.0.166&w,v	1. User has *Windows Client* and *View Only* rights on a CN8000 with an IP address of 10.0.0.166. 2. User has no rights on any other CN8000 units administered by the LDAP server.
User2	10.0.0.164&p,s;10.0.0.166&j,c	1. User has *PON* and *Virtual Media* rights on a CN8000 with an IP address of 10.0.0.164. 2. User has *Java Applet* and *Administrator* rights on a CN8000 with an IP address of 10.0.0.166. 3. User has no rights on any other CN8000 units administered by the LDAP server.
User3	v,l;10.0.0.164&p,j	1. User has *View Only* and *Log Information* rights on all CN8000 units administered by the LDAP server, except for the one with an IP address of 10.0.0.164. 2. User has *PON* and *Java Applet* rights on a CN8000 with an IP address of 10.0.0.164.
User4		User has no access rights to any CN8000 units administered by the LDAP server.
User5	v,w	User has *View Only* and *Windows Client* rights on all CN8000 units administered by the LDAP server.
User6	v;10.0.0.166&;10.0.0.164&c,j	1. User has *View Only* rights on all CN8000 units administered by the LDAP server, except for the ones with IP addresses of 10.0.0.166 and 10.0.0.164. 2. User has no access rights on the CN8000 with an IP address of 10.0.0.166. 3. User has *Administrator* and *Java Applet* rights on the CN8000 with an IP address of 10.0.0.164.

OpenLDAP

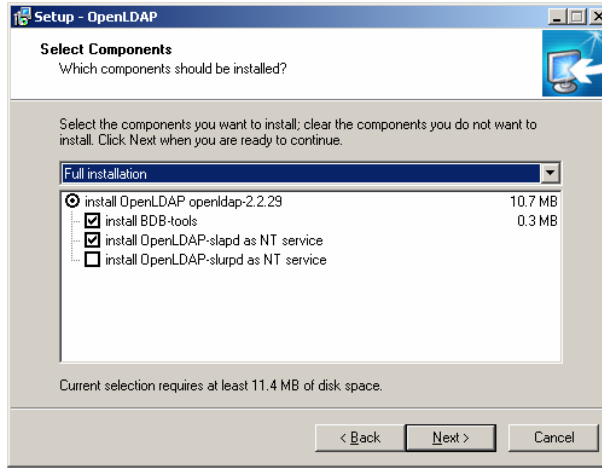
OpenLDAP is an Open source LDAP server designed for Unix platforms. A Windows version can be downloaded from:

```
http://download.bergmans.us/openldap/openldap-2.2.29/
openldap-2.2.29-db-4.3.29-openssl-0.9.8a-
win32_Setup.exe.
```

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is: *c:\Program Files\OpenLDAP*.

When the *Select Components* dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service*, as shown in the diagram, below:



OpenLDAP Server Configuration

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

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

An example configuration file is provided in the figure, below:

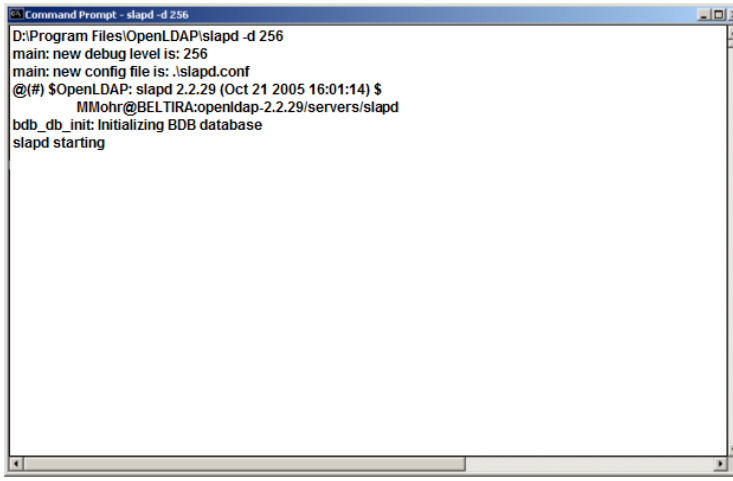
```
ucdata-path ./ucdata
include ./schema/core.schema

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

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

Starting the OpenLDAP Server

To start the OpenLDAP Server, run **slapd** (the OpenLDAP Server executable file) from the command line. slapd supports a number of command line options, the most important option is the **d** switch that triggers debug information. For example, a command of:

```
slapd -d 256
```

would start OpenLDAP with a debug level of 256, as shown in the following screenshot:



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

Customizing the OpenLDAP Schema

The schema that slapd uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes.

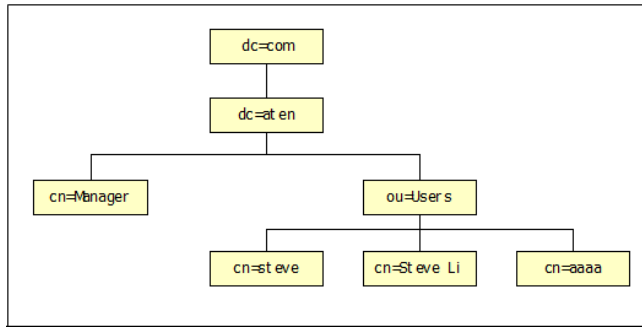
In the case of the CN8000, the CN8000*User* class and the *permission* attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the CN8000 is shown in the figure, below:

```
##########################################################################
##
##
##      Copyright (C) 2005-2006  ATEN CANADA TECHNOLOGIES INC.
##      All Rights Reserved.
##      Author:  Judy Liu
##      Date:    Aprl 7, 2008
##      Summary: Define the LDAP schema used in CN8000.
##
##
##########################################################################
#
#   ATEN OID::={1.3.6.1.4.1.21317}
#

attributetype ( 1.3.6.1.4.1. 21317.1.1.4.2.2
        NAME 'permission'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

objectclass (1.3.6.1.4.1. 21317.1.1.4.1.2
        NAME 'cn8000User'
        SUP organizationalPerson
        STRUCTURAL
        MAY ('permission'$ userCertificate ))
```

LDAP DIT Design and LDIF File

LDAP Data Structure

An LDAP Directory stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree for the CN8000 is shown in the figure, below:



(Continues on next page.)

(Continued from previous page.)

DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the CN8000 directory tree (shown in the figure, above).

```
##########################################################################
##
##
##      Copyright (C) 2005-2006  ATEN CANADA TECHNOLOGIES INC.
##      All Rights Reserved.
##      Author:  Judy Liu
##      Date:    April 7, 2008
##      Summary: Define the OpenLDAP users for CN8000
##
##
##########################################################################

dn: dc=aten,dc=com
objectclass: top
objectClass: dcObject
objectClass: organization

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

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

dn: cn=steve,ou=Users,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: cn8000User
cn: steve
sn: steve
permission: w,v,p,j,c,l
userPassword: password
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the CN8000.

```
##############################################################################
##
##
##       Copyright (C) 2005-2006  ATEN CANADA TECHNOLOGIES INC.
##       All Rights Reserved.
##       Author:  Judy Liu
##       Date:     April 7, 2008
##       Summary: Define the OpenLDAP group  for CN8000
##
##
##############################################################################

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

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

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

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

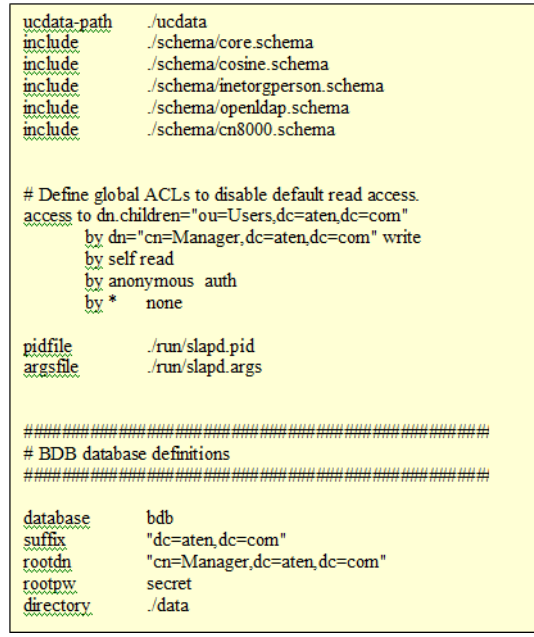
(Continues on next page.)

(Continued from previous page.)

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., cn8000.schema) in the /OpenLDAP/ schema/ directory.
2. Add the new schema to the slapd.conf file, as shown in the figure, below:



3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in init.ldif with the *ldapadd* command, as shown in the following example:

```
ldapadd -f init.ldif -x -D "cn=Manager,dc=aten,dc=com"
-w secret
```

This Page Intentionally Left Blank

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.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- 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.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors – is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer
- Do not step on or stand on any device when servicing other devices in a rack.

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.

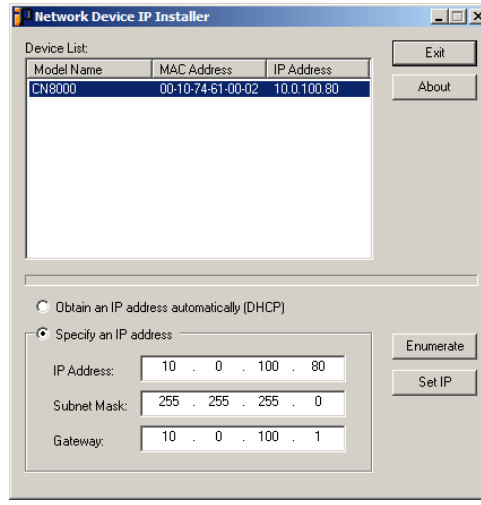
IP Address Determination

If you are an administrator logging in for the first time, you need to access the CN8000 in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your computer must be on the same network segment as the CN8000.After you have connected and logged in you can give the CN8000 its fixed network address. (See *Network*, page 23.)

IP Installer

For computers running Windows, an IP address can be assigned with the IP Installer utility:

1. Unzip the contents of *IPInstaller.zip* (found on the Software CD that came with your CN8000 package) to a directory on your hard drive.
2. Go to the directory that you unzipped the IPInstaller program to and run *IPInstaller.exe*. A dialog box similar to the one below appears:



3. Select the CN8000 in the *Device List*.

Note: 1. If the list is empty, or your device doesn't appear, click **Enumerate** to refresh the Device List.

2. If there is more than one device in the list, use the MAC address to pick the one you want. The CN8000's MAC address is located on its bottom panel.

4. Select either *Obtain an IP address automatically (DHCP)*, or *Specify an IP address*. If you chose the latter, fill the IP Address, Subnet Mask, and Gateway fields with the information appropriate to your network.
5. Click **Set IP**.
6. After the IP address shows up in the Device List, click **Exit**.

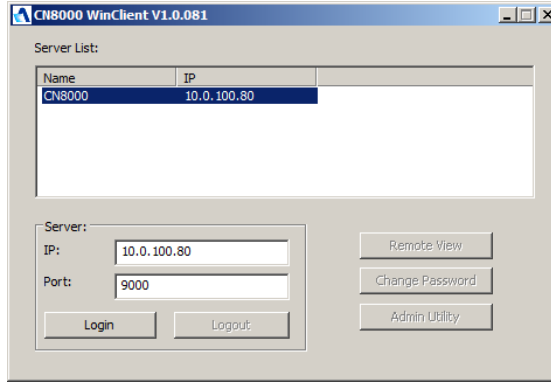
Browser

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

   Where *XXX* represents any number or numbers except 60. (192.168.0.60 is the default address of the CN8000.)
2. Specify the switch's default IP address (192.168.0.60) in your browser, and you will be able to connect.
3. Assign a fixed IP address for the CN8000 that is suitable for the network segment that it resides on.
4. After you log out, reset your computer's IP address to its original value.

AP Windows Client

For computers running Windows, the CN8000's IP address can be determined with the Windows AP program (see *The AP Windows Client*, page 73). When you run the program it searches the network segment for CN8000 devices, and displays the results in a dialog box similar to the one below:



You can now use this network address, or you can change it by clicking **Login**, logging in, clicking **Admin Utility**, and clicking the *Network* tab. See *Network*, page 79, for details.

Port Forwarding

For devices located behind a router, port forwarding allows the router to pass data coming in over a specific port to a specific device. By setting the port forwarding parameters, you tell the router which device to send the data coming in over a particular port to.

For example, if the CN8000 connected to a particular router has an IP address of 192.168.1.180, you would log into your router's setup program and access the Port Forwarding (sometimes referred to as *Virtual Server*) configuration page. You would then specify 192.168.1.180 for the IP address and the port number you want opened for it (9000 for internet access, for example).

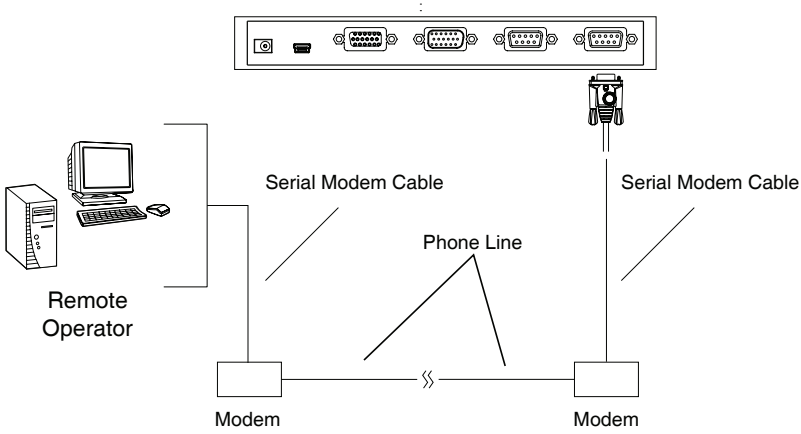
Since configuration setup can vary somewhat for each brand of router, refer to the router's User Manual for specific information on configuring port forwarding for it.

PPP Modem Operation

Basic Setup

In addition to the browser and AP methods, the CN8000 can also be accessed through its RS-232 port using a PPP dial-in connection, as follows:

1. Set up your hardware configuration to match the diagram, below:



2. From your computer, use your modem terminal program to dial into the CN8000's modem.

Note: 1. If you don't know the CN8000 modem's serial parameters, get them from the CN8000 administrator.

2. An example of setting up a modem terminal program under Windows XP is provided on the next page.

3. Once the connection is established, open your browser, and specify **192.168.192.1** in the URL box.

From here, operation is the same as if you had logged in from a browser or with the AP programs.

Connection Setup Example (Windows XP)

To set up a dial-in connection to the CN8000 under Windows XP, do the following:

1. From the *Start* menu, select Control Panel → Network Connections → Create a New Connection.
2. When the *Welcome to the New Connection Wizard* dialog box appears, click **Next** to move on.
3. In the *Network Connection Type* dialog box, select *Connect to the network at my workplace*, then click **Next**.
4. In the *Network Connection* dialog box, select *Dial-up connection*, then click **Next**.
5. In the *Connection Name* dialog box, key in a name for the connection (for example, TPE-CN8000-01), then click **Next**.
6. In the *Connection Availability* dialog box, you can select either *Anyone's use* or *My use only*, depending on your preferences, then click **Next**.

   Note: If you are the only user on this computer, this dialog box won't appear.

7. In the *Phone Number to dial* dialog box, key in the phone number of the modem connected to the CN8000 (be sure to include country and area codes, if necessary), then click **Next**.
8. In the *Completing the New Connection Wizard* dialog box, check **Add a shortcut to this connection on my desktop**, then click **Finish**.

This completes the connection setup. Double click the desktop shortcut icon to make a PPP connection to the CN8000.

Troubleshooting

General Operation

Problem	Resolution
Erratic operation	The CN8000 needs to be started before the KVM switch 1. If the CN8000 is connected to a KVM switch, make sure to power it on before powering on the switch. 2. If the KVM switch was started before the CN8000, reset or restart the KVM switch.
	The CN8000 needs to be reset (see *Firmware Upgrade/ Reset Switch*, page 8, point 1).
I can't access the CN8000, even though I have specified the IP address and port number correctly.	If the CN8000 is behind a router, the router's *Port Forwarding* (also referred to as *Virtual Server*) feature must be configured. See *Port Forwarding*, page 113, for details.
Mouse pointer confusion	If you find the display of two mouse pointers (local and remote) to be confusing or annoying, you can use the *Toggle Pointer Display* function to shrink the non-functioning pointer. See page 44 for details.
Mouse movement extremely slow	There is too much data being transferred for your connection to keep up with. Lower the video quality (see *Video Settings*, page 46) so that less video data is transmitted.
Changing Mouse Sync Mode to Manual makes the CN8000 crash.	The CN8000 hasn't crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the CN8000 to get it going right away (see *Firmware Upgrade/Reset Switch*, page 8, point 1).
I can't access my PN9108 when I click the *Power Management* icon.	Since the PN9108 already has over IP functionality, there is no need for the CN8000 to provide it. Therefore, only PON devices that don't have their own over IP functionality (such as the PN0108) are supported.
The Windows Client link doesn't appear in the *Remote Console Display* when I log in with Firefox.	The Windows Client link requires ActiveX. Since Firefox doesn't support ActiveX only the Java Applet is available.

Windows

Problem	Resolution
Windows Client won't connect to the CN8000.	DirectX 7.0 or higher must be installed on your computer.
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 122, for details.
Remote mouse pointer is out of step.	1. Check the status of the *Mouse Sync Mode* setting (see *Mouse Sync Mode*, page 36). If it is set to *Automatic*, change the setting to *Manual* and refer to the information provided. 2. If you are in Manual mode, use the *AutoSync* feature (see *Video Settings*, page 46), to sync the local and remote monitors. 3. If that doesn't resolve the problem, use the *Adjust Mouse* feature (see *Adjust Mouse*, page 44) to bring the pointers back in step. 4. If the above fails to resolve the problem, refer to *Additional Mouse Synchronization Procedures*, page 120, for further steps to take.
Part of remote window is off my monitor.	Use the *AutoSync* feature (see *Video Settings*, page 46), to sync the local and remote monitors.
Virtual Media doesn't work.	This problem sometimes arises on older computers. Get the latest firmware version for your mainboard from the manufacturer and upgrade your mainboard firmware.

Mac Systems

Problem	Resolution
The local and remote mouse pointers do not sync.	There are two USB I/O settings for the Mac: Mac 1, and Mac 2 (see *Customization*, page 35). In general, Mac 1 works with older operating system versions, whereas Mac 2 works with the newer ones. In some cases, however, the reverse is true. If you experience pointer sync problems, try selecting the other mode.

Java

For mouse synchronization problems, see *Hotkey Setup*, page 56, *AutoSync*, page 58, and *Sun / Linux*, page 121. For other problems, see the table below:

Problem	Resolution
Java Applet won't connect to the CN8000	1. Java 6 Update 3 or higher must be installed on your computer. 2. Make sure to include the correct login string when you specify the CN8000's IP address. 3. Close the Java Applet, reopen it, and try again.
I have installed the latest Java JRE, but I am having performance and stability problems.	There may be issues with the latest version because it is so new. Try using a Java version that is one or two updates earlier than the latest one.
Java Applet performance deteriorates.	Exit the program and start again.
National language characters don't appear.	Use the CN8000's *On-Screen Keyboard* and be sure that the local and remote computers are set to the same language. (See *On-Screen Keyboard*, page 61.)
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 122, for details.
There is no Virtual Media icon on my Control Panel.	The virtual media function only supports the Windows 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	The default configuration is for the local and remote mouse pointers to automatically sync when you connect. Automatic mouse sync only supports USB mice on Windows and Mac (G4 or higher) systems, however. You must select *Manual* as the *Mouse Sync Mode* choice, and sync the pointers manually. See *Mouse Sync Mode*, page 36 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.

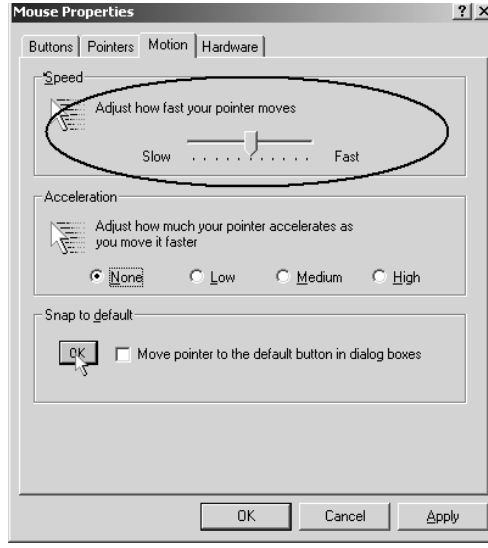
1. Windows 2000:

   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*



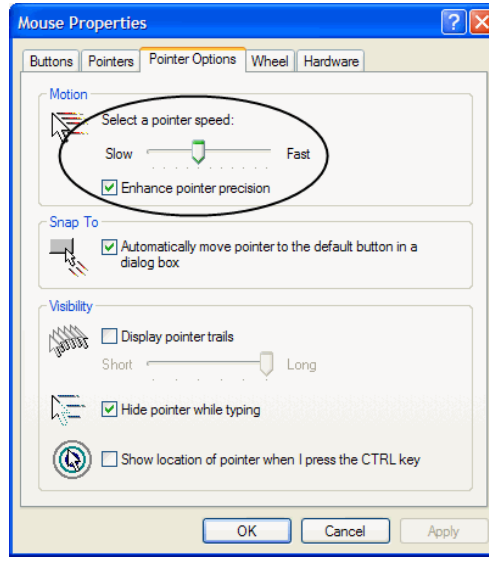
2. Windows XP / Windows Server 2003:

   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:

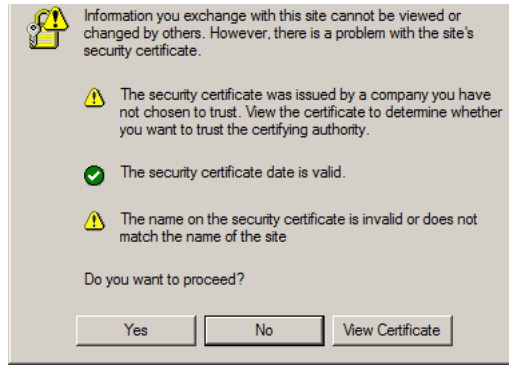
Sun: `xset m 1`

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.



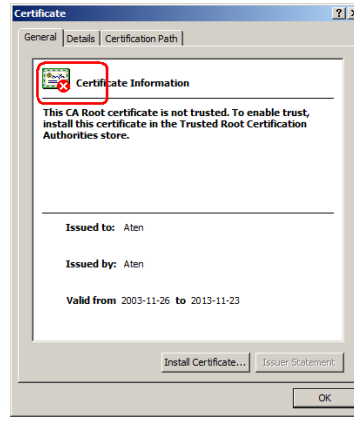
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- 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

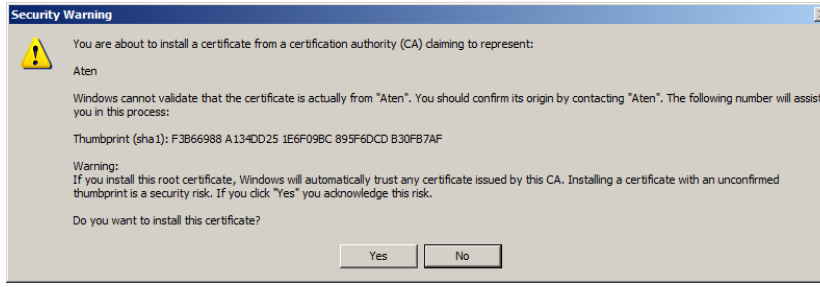
To install the certificate, do the following:

5. 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.

6. Click **Install Certificate.**
7. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
8. When the Wizard presents a caution screen:



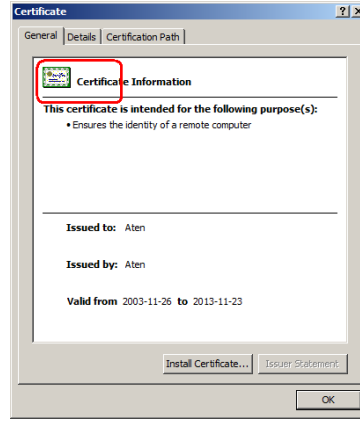
Click **Yes**.

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

Certificate Trusted

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:

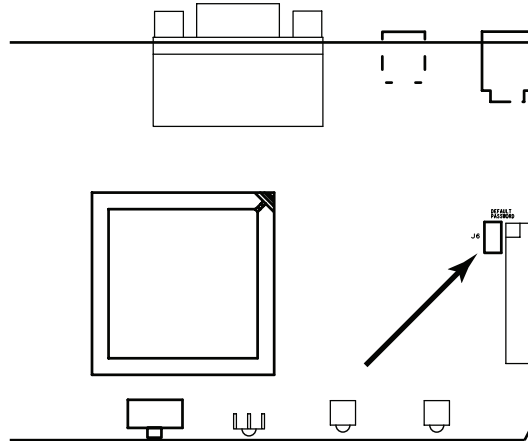


Administrator Login Failure

If you are unable to perform an Administrator login (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.

To clear the login information do the following:

1. Power off the CN8000 and remove its housing.
2. Use a jumper cap to short the jumper on the mainboard labeled J6.



3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from J6.
6. Close the housing and power on the CN8000.

   After you start back up, you can use the default Username and Password (see page 17, and page 76) to log in.

Specifications

Function		Specification
Connectors	Console	1 x SPHD-18 Male (Yellow)
	KVM (Computer)	1 x SPHD-15 Female (Yellow)
	PON[1]	1 x DB-9 Male (Black)
	Modem	1 x DB-9 Male (Black)
	LAN	1 x RJ-45 Female
	Power	1 x DC Jack
	Virtual Media	1 x USB Mini-B Female (Black)
Switches	Reset	1 x Semi-recessed pushbutton
LEDs	Power	1 (Orange)
	Link	1 (Green)
	10/100 Mbps	1 (Orange/Green)
Emulation	Keyboard/Mouse	USB; PS/2
Video		Up to 1600 x 1200 @ 60 Hz; DDC2B
Power Consumption		DC5.3V; 6.3W
Environment	Operating Temp.	0–50° C
	Storage Temp.	-20–60° C
	Humidity	0–80% RH Non-condensing
Physical Properties	Housing	Metal
	Weight	0.49 kg
	Dimensions (L x W x H)	20.00 x 8.15 x 2.50 cm

[1] Power Over the NET

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.

This Page Intentionally Left Blank

Index