EMC Information

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

CE Warning: This is a 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.

Suggestion: Shielded twisted pair (STP) cables must be used with the unit to ensure compliance with FCC & CE standards.

KCC Statement: 유선 제품용 / A급 기기 (업무용 방송 통신 기기) 이 기기는 업무용 (A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

RoHS

This product is RoHS compliant.
User Information

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

| International | http://eservice.aten.com |

Telephone Support
For telephone support, call this number:

<table>
<thead>
<tr>
<th>International</th>
<th>886-2-8692-6959</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>86-400-810-0-810</td>
</tr>
<tr>
<td>Japan</td>
<td>81-3-5615-5811</td>
</tr>
<tr>
<td>Korea</td>
<td>82-2-467-6789</td>
</tr>
<tr>
<td>North America</td>
<td>1-888-999-ATEN ext 4988</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>44-8-4481-58923</td>
</tr>
</tbody>
</table>

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 CN8000A package consists of:

- 1 CN8000A Single Port KVM over IP Switch
- 1 Custom KVM Cable
- 1 Custom Console Cable
- 1 Laptop USB Cable
- 1 Power Adapter
- 1 Mounting Kit
- 1 User Instructions*

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 CN8000A since this manual was published. Please visit our website to download the most up-to-date version of the manual.
# Contents

EMC Information .................................................. ii
RoHS .......................................................... ii
User Information ................................................... iii
  Online Registration ......................................... iii
  Telephone Support ........................................... iii
  User Notice ................................................... iii
Package Contents ............................................... iv
About this Manual ............................................. xi
  Overview ....................................................... xi
  Conventions .................................................... xii
  Terminology ................................................... xiii
Product Information ........................................... xiv

1. Introduction
   Overview ....................................................... 1
   Features and Benefits ....................................... 3
   System Requirements ......................................... 6
      Servers ....................................................... 6
      Cables ....................................................... 6
      Video ......................................................... 8
      Operating Systems ........................................ 8
      Browsers .................................................... 10
   Components .................................................... 11
      Front View .................................................. 11
      Rear View .................................................. 12
      Custom Console Cable .................................... 13

2. Hardware Setup
   Mounting ........................................................ 15
      Rack Mounting ............................................. 15
      DIN Rail Mounting ....................................... 16
   Installation ..................................................... 17

3. OSD Operation
   OSD Overview .................................................. 21
   OSD Navigation ................................................ 22
   Device Information ........................................... 23
   Set IP Address ................................................ 24
   Disable Dev Authentication ................................. 25
   Reset Default Values ....................................... 25
   Reset Certificate ............................................ 25
   Reboot ........................................................ 25

4. Browser Login
   Logging In ....................................................... 27
5. Administration

Introduction ........................................... 33
Basic Settings ......................................... 34
User Management ....................................... 34
Sessions ................................................. 37
Maintenance ............................................ 38
Upgrade Main Firmware ............................... 38
Backup ................................................. 39
Restore .................................................. 39
Advanced Settings .................................... 42
Device Information ................................... 42
Network .................................................. 43
IP Installer ............................................. 43
Service Ports ......................................... 44
IPv4 Settings .......................................... 45
IPv6 Settings .......................................... 46
Network Transfer Rate ................................. 47
Finishing Up ............................................ 47
ANMS - Event Destination ............................ 48
SMTP Settings ......................................... 48
Log Server .............................................. 49
SNMP Server ........................................... 49
Syslog Server .......................................... 50
ANMS - Authentication ................................ 51
Disable Local Authentication ....................... 51
RADIUS Settings ....................................... 51
CC Management Settings ............................. 54
Security .................................................. 55
Login Failures .......................................... 55
Filter ...................................................... 56
Encryption ............................................. 60
Private Certificate ...................................... 62
Certificate Signing Request ......................... 63
Console Management .................................. 65
OOBCC ................................................................ 65
Date/Time .................................................. 70
Time Zone ................................................ 70
Date ....................................................... 71
Time ....................................................... 71
Network Time ........................................... 71
Preferences ......................................................... 74
User Preferences ........................................... 74
Settings ......................................................... 74
Password ......................................................... 75
Log ................................................................. 75
Remote Console ............................................ 76
Exit Macro ................................................... 76
Telnet .............................................................. 76
Open Power Management ................................ 76
About ............................................................. 77

6. The WinClient Viewer
Starting Up ....................................................... 79
Navigation ......................................................... 80
The WinClient Control Panel ................................ 81
Control Panel Functions .................................... 82
Macros ............................................................. 85
  Hotkeys ......................................................... 85
  Running Macros ............................................ 89
  System Macros ............................................. 91
Video Settings .................................................. 94
The Message Board ......................................... 97
  The Button Bar ............................................ 97
  Message Display Panel .................................. 98
  Compose Panel ............................................ 98
User List Panel .................................................. 98
Virtual Media .................................................... 99
  Virtual Media Icons ...................................... 99
  Virtual Media Redirection ................................ 99
Zoom ............................................................... 103
The On-Screen Keyboard .................................. 104
Mouse Pointer Type .......................................... 106
Mouse DynaSync Mode ....................................... 106
  Automatic Mouse Synchronization (DynaSync) .... 106
  Manual Mouse Synchronization ....................... 107
Customize Control Panel .................................... 108
Power Management ........................................... 110
Admin Utility .................................................... 111

7. The JavaClient Viewer
Introduction .................................................... 113
Navigation ....................................................... 114
The JavaClient Control Panel ......................... 115
  Control Panel Functions .................................. 116
  Macros ......................................................... 118
    Hotkeys .................................................. 118
8. The Log Server
Installation. ................................................................. 127
Starting Up ................................................................. 128
The Menu Bar ............................................................... 129
Configure ................................................................. 129
Events ................................................................. 130
Search ................................................................. 130
Maintenance ............................................................... 131
Options ................................................................. 132
Help ................................................................. 132
The Log Server Main Screen ................................................................. 133
Overview ................................................................. 133
The List Panel ............................................................... 134
The Tick Panel ............................................................... 134

9. LDAP Server Configuration
Introduction ................................................................. 135
Install the Windows 2003 Support Tools ................................................................. 135
Install the Active Directory Schema Snap-in ................................................................. 136
Create a Start Menu Shortcut Entry ................................................................. 136
Extend and Update the Active Directory Schema ................................................................. 137
Creating a New Attribute ................................................................. 137
Extending the Object Class With the New Attribute ................................................................. 138
Editing Active Directory Users ................................................................. 141
Type 1 ................................................................. 141
Permission String Characters ................................................................. 145
OpenLDAP ................................................................. 148
OpenLDAP Server Installation ................................................................. 148
OpenLDAP Server Configuration ................................................................. 149
Starting the OpenLDAP Server ................................................................. 150
Customizing the OpenLDAP Schema ................................................................. 151
LDAP DIT Design and LDIF File ................................................................. 152
LDAP Data Structure ................................................................. 152
DIT Creation ................................................................. 153
Using the New Schema ................................................................. 155
Appendix

Safety Instructions ................................................................. 157
General ................................................................. 157
Rack Mounting ................................................................. 159
Consignes de sécurité ................................................................. 160
Général ................................................................. 160
Montage sur bâti ................................................................. 163
Technical Support ................................................................. 164
International ................................................................. 164
North America ................................................................. 164
IP Address Determination ................................................................. 165
First Time Browser Login ................................................................. 165
IP Installer ................................................................. 165
Network Device IP Installer ................................................................. 166
Device List ................................................................. 166
Protocol ................................................................. 166
Network Adapter ................................................................. 166
Set IP ................................................................. 166
About ................................................................. 167
Browser ................................................................. 167
AP Windows Client ................................................................. 167
IPv6 ................................................................. 168
Link Local IPv6 Address ................................................................. 168
IPv6 Stateless Autoconfiguration ................................................................. 169
Port Forwarding ................................................................. 170
Keyboard Emulation ................................................................. 171
PPP Modem Operation ................................................................. 172
Basic Setup ................................................................. 172
Connection Setup Example (Windows XP) ................................................................. 173
Trusted Certificates ................................................................. 174
Overview ................................................................. 174
Installing the Certificate ................................................................. 175
Certificate Trusted ................................................................. 176
Self-Signed Private Certificates ................................................................. 178
Examples ................................................................. 178
Importing the Files ................................................................. 178
Troubleshooting ................................................................. 179
General Operation ................................................................. 179
Windows ................................................................. 181
Java ................................................................. 182
Sun Systems ................................................................. 183
Mac Systems ................................................................. 184
The Log Server ................................................................. 184
Additional Mouse Synchronization Procedures ................................................................. 185
Windows ................................................................. 185
Sun / Linux ................................................................. 186
About this Manual

This User Manual is provided to help you get the most from your CN8000A. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Overview

Chapter 1, Introduction, introduces you to the CN8000A 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, OSD Operation, describes how to log into the CN8000A via the OSD, and explains the functions of each menu item on the screen.

Chapter 4, Browser Login, describes how to log into the CN8000A with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 5, Administration, explains the administrative procedures that are employed to configure the CN8000A’s working environment, as well as how to operate the CN8000A from the local console.

Chapter 6, The WinClient Viewer, explains how to connect to the CN8000A with the Windows Client software, and describes how to use the OSD to access and control the computers connected to the switch.

Chapter 7, The JavaClient Viewer, describes how to connect to the CN8000A with the Java Applet software, and explains how to use the OSD to access and control the computers connected to the switch.

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

Chapter 9, LDAP Server Configuration, explains how to configure the CN8000A for LDAP / LDAPS authentication and authorization with Active Directory or OpenLDAP.

An Appendix, provides specifications and other technical information regarding the CN8000A.
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.
Terminology
Throughout the manual we make reference to the terms *Local* and *Remote* in regard to the operators and equipment deployed in a CN8000A installation. Depending on the point of view, users and servers can be considered *Local* under some circumstances, and *Remote* under others:

- **Switch’s Point of View**
  - Remote users – We refer to a user as a *Remote* user when we think of him as someone who logs into the switch over the net from a location that is *remote from the switch*.
  - Local Console – The keyboard mouse and monitor connected directly to the switch.
  - Servers – The servers attached to the switch via custom KVM cables.

- **User’s Point of View**
  - Local client users – We refer to a user as a *Local client user* when we think of him as sitting at his computer performing operations on the servers connected to the switch that is *remote from him*.
  - Remote servers – We refer to the servers as *Remote servers* when we think of them from the Local Client User’s point of view – since, although they are locally attached to the switch, they are *remote from him*.

When we describe the overall system architecture we are usually speaking from the switch’s point of view – in which case the users are considered remote. When we speak about operations users perform via the browser, viewers, and AP programs over the net, we are usually speaking from the user’s point of view – in which case the switch and the servers connected to it are considered remote.
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 |
Chapter 1
Introduction

Overview

The CN8000A 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 CN8000A connects to the local area network using standard Cat 5e cable, then uses a custom KVM cable to connect to a local KVM switch or server.

Because the CN8000A uses TCP/IP for its communications protocol, the server or KVM switch it is connected to can be accessed from any computer across the Internet – whether that computer is located down the hall, down the street, or half-way around the world.

Operators at remote locations connect to the CN8000A 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 CN8000A expands on previous models by providing a dedicated RS-232 port for modem access or serial console management, a PON port to attach a Power Over the NET™ device and a Laptop USB Console port for easy console access from a laptop.
With its advanced security features, the CN8000A is the fastest, most reliable, most cost effective way to remotely access and manage widely distributed multiple computer installations.

A mini USB port in the front panel serves as a Laptop USB Console (LUC) port. No additional monitor, keyboard or mouse is required – simply use a laptop that utilizes the LUC feature to access a remote computer for easy management.

The *Administrator* and *Client* software included with the CN8000A 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 a browser-based version as well as Windows-based and Java application versions. The utility is used to configure the system; limit access from remote computers; manage users; and maintain the system with firmware and software module updates.

A *Windows Client Viewer* and a *Java Applet Viewer* are available for browser access, while *Windows Client AP* and *Java Client AP* programs are provided for non-browser GUI access. They allow IP connection and login from anywhere on the Internet. Inclusion of a Java-based client ensures that the CN8000A 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 CN8000A (KVM OSD display or server's desktop) 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 CN8000A units for the administrator to analyze.

Your CN8000A investment is protected through the ability of its firmware to be upgraded over the Internet. 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 and Benefits

The features and benefits provided by a CN8000A deployment are described in the following table:

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over-IP Capability for Legacy KVM Switches</td>
<td>Protects your original KVM switch investment. No need to purchase new KVM switches to achieve the benefits of over-IP connectivity.</td>
</tr>
<tr>
<td>Configuration and Operation</td>
<td>An easy-to-navigate graphical user interface makes for convenient, intuitive configuration and operation. Web-based Windows and Java implementations allow the remote equipment to be controlled from a standard web browser. Windows and Java AP client software – using the same convenient GUI are also included to provide access where a browser environment is not desired.</td>
</tr>
<tr>
<td>Superior Video</td>
<td>With its enhanced fps throughput for crisp responsive video display, the CN8000A offers resolutions of up to 1920 x 1200 @ 60Hz; vibrant 24-bit color depth for rich remote session display. The remote desktop can appear full-screen, or in a window. In full-screen mode the remote desktop display scales to the user’s monitor display size.</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>USB 2.0 devices (Floppy drives, CDROMs, Flash drives, etc.), folders, and image files on a user’s local system, appear and act as if they were installed on the remote server, for ease and convenience when performing software installation and system updates across the entire installation. <strong>Note:</strong> Virtual Media only works with 2L-5301UP (1.2m), 2L-5302UP (1.8m), 2L-5201U (1.2m), and 2L-5202U (1.8m) KVM cables.</td>
</tr>
<tr>
<td>Virtual Remote Desktop</td>
<td>• On-screen keyboard with multilanguage support</td>
</tr>
<tr>
<td></td>
<td>• Exit Macros support</td>
</tr>
<tr>
<td></td>
<td>• BIOS-level access</td>
</tr>
<tr>
<td>Laptop USB Console (LUC)</td>
<td>A mini USB port in the front panel serves as a Laptop USB Console (LUC) port allowing a laptop to be used as a console for remote access.</td>
</tr>
<tr>
<td>Smart Card / CAC Reader Support</td>
<td>To meet advanced security requirements, the CN8000A’s Virtual Media function allows a Smart Card / CAC reader on a user’s local system to be mapped to a remote server.</td>
</tr>
<tr>
<td>Low Bandwidth Optimization</td>
<td>Bandwidth optimization via grayscaling and video quality settings allow maximum data throughput in low bandwidth situations. PPP modern dial-up support ensures reliable connectivity for out-of-band, and low bandwidth situations.</td>
</tr>
</tbody>
</table>
### Multi-Platform / Multi-Protocol Support

Windows and Java client software ensures that the CN8000A and the equipment that connects to it can be accessed from most of the operating systems in use today (Windows, Linux, Unix, Sun, Mac). The CN8000A also supports a broad range of communication protocols, such as TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP, 10Base-T, 100Base-T.

### Multi-Keyboard Language Support / On-Screen Keyboard

The CN8000A supports multiple keyboard language input – including English, French, German, Italian, Spanish, Japanese, Korean, and Traditional Chinese. There is no need to have a separate keyboard for each language – you can input key data in any of these languages with the CN8000A’s convenient on-screen keyboard.

### Multi-Users / Multi-Logins

The CN8000A supports up to 64 user accounts, and allows up to 32 concurrent user logins for single-bus access.

### Message Board

To alleviate the possibility of access conflicts that may result from multiple user logins, and facilitate communication among the logged-in users, a message board – similar to an Internet chat program – allows users to communicate with each other, and provides mechanisms for a user to take exclusive control of the KVM functions.

### Advanced Security

- Advanced security features include password protection – whereby a valid username and password must be given before the client software will run – and advanced encryption technologies, such as secure SSL and TLS 1.2.
- Supports SSL data encryption, TLS 1.2 and RSA 2048-bit certificates for secure users logging in from a browser.
- Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption.
- Support for IP/MAC Filter
- Supports strong password protection
- Private CA

### External Authentication Support

In addition to its own security protection, the CN8000A allows you to set up log in authentication and authorization management from an external sources such as RADIUS, LDAP, LDAPS, and MS Active Directory.

### Event Logging

The CN8000A can record all the events that take place on it and write them to a searchable database. Administrators and selected users can search for events containing specific words or strings and retrieve them according to date and order of significance.

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Platform / Multi-Protocol</td>
<td>Windows and Java client software ensures that the CN8000A and the equipment that connects to it can be accessed from most of the operating systems in use today (Windows, Linux, Unix, Sun, Mac). The CN8000A also supports a broad range of communication protocols, such as TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP, 10Base-T, 100Base-T.</td>
</tr>
<tr>
<td>Multi-Keyboard Language Support</td>
<td>The CN8000A supports multiple keyboard language input – including English, French, German, Italian, Spanish, Japanese, Korean, and Traditional Chinese. There is no need to have a separate keyboard for each language – you can input key data in any of these languages with the CN8000A’s convenient on-screen keyboard.</td>
</tr>
<tr>
<td>Message Board</td>
<td>To alleviate the possibility of access conflicts that may result from multiple user logins, and facilitate communication among the logged-in users, a message board – similar to an Internet chat program – allows users to communicate with each other, and provides mechanisms for a user to take exclusive control of the KVM functions.</td>
</tr>
<tr>
<td>Advanced Security</td>
<td>Advanced security features include password protection – whereby a valid username and password must be given before the client software will run – and advanced encryption technologies, such as secure SSL and TLS 1.2. Supports SSL data encryption, TLS 1.2 and RSA 2048-bit certificates for secure users logging in from a browser. Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption. Support for IP/MAC Filter. Supports strong password protection. Private CA.</td>
</tr>
<tr>
<td>External Authentication Support</td>
<td>In addition to its own security protection, the CN8000A allows you to set up log in authentication and authorization management from an external sources such as RADIUS, LDAP, LDAPS, and MS Active Directory.</td>
</tr>
<tr>
<td>Event Logging</td>
<td>The CN8000A can record all the events that take place on it and write them to a searchable database. Administrators and selected users can search for events containing specific words or strings and retrieve them according to date and order of significance.</td>
</tr>
</tbody>
</table>
1. Introduction

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Console Management        | • Serial console management – serial terminal access. Access the CN8000A via a built-in serial viewer, or via third party software (such as PuTTY) for Telnet and SSH sessions.  
                             • Out of Band Support – via dial up modem support. Access the CN8000A through its RS-232 port using a dial-up connection. |
| Upgradeable Firmware over the Internet | No need to add yet another cable to your installation – stay current with the latest functionality improvements and updates, all over the Internet. |
| Remote Power Control      | You can add a PON (Power Over the NET™) power management unit and remotely control the power status of devices on your installation, including monitoring their current status, as well as turning servers On, Off and Rebooting them. |
| Mouse DynaSync            | No need to re-sync your mouse – Mouse DynaSync provides automatic locked-in synching of the remote and local mouse pointers – eliminating the need to constantly resync the two movements. Your local console mouse movement becomes the remote unit’s mouse movement. |
| Full-Screen or Sizable Remote Desktop Window | Get a full screen even if your monitor’s resolution is lower than the remote computer’s resolution. In full-screen mode the remote desktop display scales to the user’s monitor display size. Supports up to 1920 x 1200 @ 60Hz; 24-bit color depth for remote sessions. |
| DDNS                      | Allows the mapping of a dynamic IP address assigned by a DHCP server to a hostname. |
| End session               | Administrators can terminate running sessions |
System Requirements

Servers
Servers are the computers connected to the switch via KVM Cables (see Terminology, page xiii). The following equipment must be installed on these servers:

- A VGA, SVGA or multisync port
- For USB KVM Cable Connections: Type A USB port and USB host controller
- For PS/2 KVM Cable Connections: 6-pin Mini-DIN keyboard and mouse ports

Cables

- A custom KVM cable set (USB; PS/2) to link the CN8000A 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:

<table>
<thead>
<tr>
<th>Cable Type</th>
<th>Length</th>
<th>CS Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS/2</td>
<td>1.2 m</td>
<td>2L-5201P</td>
</tr>
<tr>
<td></td>
<td>1.8 m</td>
<td>2L-5202P</td>
</tr>
<tr>
<td></td>
<td>1.8 m</td>
<td>2L-5702P</td>
</tr>
<tr>
<td></td>
<td>3.0 m</td>
<td>2L-5203P</td>
</tr>
<tr>
<td></td>
<td>6.0 m</td>
<td>2L-5206P</td>
</tr>
<tr>
<td>USB</td>
<td>1.2 m</td>
<td>2L-5201U</td>
</tr>
<tr>
<td></td>
<td>1.8 m</td>
<td>2L-5202U</td>
</tr>
<tr>
<td></td>
<td>3.0 m</td>
<td>2L-5203U</td>
</tr>
<tr>
<td></td>
<td>5.0 m</td>
<td>2L-5205U</td>
</tr>
<tr>
<td>PS/2-USB</td>
<td>1.2 m</td>
<td>2L-5301UP</td>
</tr>
<tr>
<td></td>
<td>1.8 m</td>
<td>2L-5302UP</td>
</tr>
<tr>
<td></td>
<td>3.0 m</td>
<td>2L-5303UP</td>
</tr>
</tbody>
</table>

To purchase additional cable sets, contact your dealer.

- One custom Console cable set to link the CN8000A to a local console is provided with this package.
1. Introduction

**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 *Laptop USB Console (LUC)* (see *Laptop USB Console (LUC)*, page 3) is provided with this package.
- Cat 5e or higher Ethernet cable (not provided with this package), should be used to connect the CN8000A to the LAN, WAN, or Internet.
Video

Only the following *non-interlaced* video signals are supported:

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Refresh Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>640 x 480</td>
<td>60, 72, 75, 85, 90, 100, 120</td>
</tr>
<tr>
<td>720 x 400</td>
<td>70</td>
</tr>
<tr>
<td>800 x 600</td>
<td>56, 60, 72, 75, 85, 90, 100, 120</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>60, 70, 75, 85, 90, 100</td>
</tr>
<tr>
<td>1152 x 864</td>
<td>60, 70, 75, 85</td>
</tr>
<tr>
<td>1280 x 720</td>
<td>60</td>
</tr>
<tr>
<td>1280 x 1024</td>
<td>60, 70, 75, 85</td>
</tr>
<tr>
<td>1600 x 1050</td>
<td>60</td>
</tr>
<tr>
<td>1600 x 1200</td>
<td>60</td>
</tr>
<tr>
<td>1920 x 1080</td>
<td>60</td>
</tr>
<tr>
<td>1920 x 1200</td>
<td>60</td>
</tr>
</tbody>
</table>

Operating Systems

- Supported operating systems for remote user computers that log into the CN8000A include Windows XP and higher, and other systems capable of running Sun's Java Runtime Environment (JRE) 6, Update 3, or higher (Linux, Mac, Sun, etc.).
- Supported operating systems for servers that connect to the CN8000A are shown in the table, below:

<table>
<thead>
<tr>
<th>OS</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>XP and higher</td>
</tr>
<tr>
<td>Linux</td>
<td>RedHat 7.1 and higher</td>
</tr>
<tr>
<td></td>
<td>Fedora Core12 and higher</td>
</tr>
<tr>
<td></td>
<td>SuSE 11.1 and higher</td>
</tr>
<tr>
<td></td>
<td>Mandriva (Mandrake) 9.0 and higher</td>
</tr>
<tr>
<td>UNIX</td>
<td>AIX 7.1 and higher</td>
</tr>
<tr>
<td></td>
<td>FreeBSD 10.1 and higher</td>
</tr>
<tr>
<td></td>
<td>Sun Solaris 10 and higher</td>
</tr>
<tr>
<td>Novell</td>
<td>Netware 6.5 and higher</td>
</tr>
<tr>
<td>Mac</td>
<td>OS X 10.7 and higher</td>
</tr>
<tr>
<td>OS</td>
<td>Version</td>
</tr>
<tr>
<td>-----</td>
<td>----------------</td>
</tr>
<tr>
<td>DOS</td>
<td>6.2 and higher</td>
</tr>
</tbody>
</table>
Browsers

Supported browsers for users that log into the CN8000A include the following:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE</td>
<td>10 and higher</td>
</tr>
<tr>
<td>Firefox</td>
<td>3.5 and higher</td>
</tr>
<tr>
<td>Mozilla</td>
<td>3.5 and higher</td>
</tr>
<tr>
<td>Safari*</td>
<td>2.0 and higher</td>
</tr>
<tr>
<td>Opera</td>
<td>9.0 and higher</td>
</tr>
<tr>
<td>Netscape</td>
<td>8.1 and higher</td>
</tr>
</tbody>
</table>

* See Mac Systems, page 184, for further information regarding Safari.
1. Introduction

## Components

### Front View

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LAN Port</td>
<td>The Cat 5e/6 cable that connects the CN8000A to the LAN plugs in here.</td>
</tr>
<tr>
<td>2</td>
<td>Laptop USB Console (LUC)</td>
<td>Use the USB cable provide with this package to connect a laptop to this port for console access.</td>
</tr>
</tbody>
</table>
| 3   | Firmware Upgrade/Reset Switch          | 1. Pressing and releasing this switch performs a CN8000A system reset. (See Erratic operation, page 179.)                                       
|     |                                        | 2. Pressing and holding this switch for more than three seconds returns the CN8000A to its factory default configuration settings.             |
|     |                                        | 3. Pressing and holding this switch while powering on the switch returns the CN8000A 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.                  |
| 4   | 10/100/1000 Mbps LED                   | The LED lights ORANGE to indicate 10 Mbps data transmission speed. It lights ORANGE+GREEN to indicate 100 Mbps data transmission speed. It lights GREEN to indicate 1000 Mbps data transmission speed. |
| 5   | Link LED                               | Flashes GREEN to indicate that a Client program is accessing the device.                                                                      |
| 6   | Power LED                              | Lights ORANGE when the CN8000A is powered up and ready to operate.                                                                           |
Rear View

<table>
<thead>
<tr>
<th>No.</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power Jack</td>
<td>The power adapter cable plugs in here.</td>
</tr>
<tr>
<td>2</td>
<td>PC/KVM Port</td>
<td>The KVM cable (supplied with this package) that links the CN8000A to your server or KVM switch plugs in here.</td>
</tr>
<tr>
<td>3</td>
<td>PS/2 - USB Console Port</td>
<td>The CN8000A 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.</td>
</tr>
<tr>
<td>4</td>
<td>PON Port</td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>RS-232 Port</td>
<td>This serial port is provided for: 1. Serial console management (see Console Management, page 65 for details); or 2. Out-of-band modem operation (see OOBC, page 65 for details).</td>
</tr>
</tbody>
</table>
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 157. 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 CN8000A 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 CN8000A – 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 CN8000A on a DIN rail:

1. Screw the mounting bracket to the back of the CN8000A 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.
2. Hardware Setup

Installation

To install the CN8000A, refer to the installation diagrams on the next two pages (the numbers correspond to the numbers of the steps), and do the following:

1. Use the Custom Console Cable provided with this package to connect the CN8000A’s PS/2-USB Console Port, to the local console keyboard, monitor and mouse.

   **Note:**
   1. The Custom 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 Custom KVM Cable provided with this package to connect the CN8000A’s PC/KVM Port, to the keyboard, video and mouse ports of the server, or KVM switch’s port or KVM cable that you are installing.

   **Note:**
   1. The diagram shows a connection to a KVM switch with PS/2 mouse and keyboard ports using a PS/2 KVM cable set. The CN8000A can also connect to a server or KVM switch that uses a USB connection by using a USB KVM cable set. See Cables, page 6, for cable option information.
   2. If you are using a PS/2 configuration KVM cable, refer to page 185 for mouse pointer synchronization information. When PS/2 cables are used (without USB) the virtual media functions will not work.
   3. If you are using a USB configuration KVM cable, see Mouse DynaSync Mode, page 106, for mouse pointer synchronization information.
   4. The CN8000A’s virtual media features may not be supported, depending on the functionality of the cascaded KVM switch (see Supported KVM Switches, page 187).

3. (Optional) If you want to connect a PON device for remote power management, plug its cable into the PON Port.
4. (Optional) If you want to connect a serial console device or modem, plug its cable into the \textit{RS-232 Port}.

5. (Optional) If you want to use a laptop as a console, use the Laptop USB Cable included with this package to connect the laptop’s USB port to the CN8000A’s \textit{Laptop USB Console Port}.

6. Plug a Cat 5e/6 Ethernet cable into the CN8000A’s \textit{LAN Port}.

7. Plug the power adapter cable into the CN8000A’s \textit{Power Jack}, then plug the power adapter into an AC power source.

This completes the hardware installation, and you are ready to start up.

\textbf{Note:} When starting up, be sure to first power on the CN8000A, then power on the server or KVM switch.
2. Hardware Setup

- KVM Switch
- Modem
- PN0108
- Serial Console Device (Router, Switch, Sunfire V100, ...)

Diagram:

1. KVM Switch
2. Modem
3. PN0108
4. Serial Console Device
5. Laptop
6. Monitor
7. Keyboard
Chapter 3
OSD Operation

OSD Overview

The On Screen Display (OSD) is a menu driven method to view and configure
the CN8000A’s basic settings. To display the Main Screen, tap the OSD hotkey
twice.

The default hotkey is [Scroll Lock]. You can change the hotkey to the Ctrl key
or the Alt key if you like (see User Preferences, page 74).

Note: 1. If you use the Ctrl or Alt key method you must press the same Ctrl or
Alt key both times.

2. Once you start the OSD, the keyboard lock will be controlled by the
device. The number lock and caps lock will always be on when the
OSD is being accessed.

Before the OSD Main Screen comes up, a login dialog box appears requesting
a username and password. You must provide a valid username and password
to continue.

The first time that the OSD is accessed, you must use the default username and
password. The default username is administrator; the default password is
password. For security purposes, we strongly recommend changing these to
something unique after you log in for the first time.

After logging in with the default username and password, the OSD Main
Screen opens in Administrator mode. In this mode, you have administrator
privileges, with access to all administrator and user functions, and can set up
operations (including password authorization for the future), as you prefer.
When you log in to the OSD, the CN8000A’s main menu appears:

<table>
<thead>
<tr>
<th>Device Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set IP Address</td>
</tr>
<tr>
<td>Disable Device Authentication</td>
</tr>
<tr>
<td>Reset Default Values</td>
</tr>
<tr>
<td>Reset Certificate</td>
</tr>
</tbody>
</table>

**OSD Navigation**

- The OSD uses a menu that is navigated using the keyboard or mouse.
- To logout of the OSD menu, click the X at the upper right corner of the OSD Window or press Esc.
- To move up or down through the list one line at a time, use the up and down arrow keys.
- To exit a screen and return to the main menu, press Esc.
Device Information

The Device Information page provides information about the CN8000A's status.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Display the name given to the CN8000A.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The CN8000A's MAC Address is displayed here.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Indicates the CN8000A's current firmware version level. New versions of the CN8000A's firmware can be downloaded from our website as they become available (see Upgrade Main Firmware, page 38). You can reference this number to see if there are newer versions available on the website.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the CN8000A's Internet Protocol Version 4 (32 bit) address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the CN8000A's Subnet Mask address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the CN8000A's Default Gateway address.</td>
</tr>
<tr>
<td>DNS Server 1/2</td>
<td>Displays the DNS Server configured for the CN8000A.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Displays the CN8000A's Internet Protocol Version 6 (128 bit) address (Appears only when an IPv6 address is assigned).</td>
</tr>
<tr>
<td>IPv6 Subnet Prefix Length</td>
<td>Displays the prefix length of the IPv6 Subnet address (Appears only when an IPv6 address is assigned).</td>
</tr>
</tbody>
</table>
Set IP Address

The Set IP Address screen is used to specify the CN8000A’s network environment.

The CN800A can have its IPv4 address assigned dynamically (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the *Obtain IP address automatically (DHCP)*, radio button. (This is the default setting.)

- To specify a fixed IP address, select the *Set IP address manually [Fixed IP]*, radio button and fill in the IP Address, Subnet Mask and Default Gateway. When you select this option the following screen appears:

```
Set IP Address

1. [ ] Obtain an IP address automatically (DHCP)
2. [ ] Use the following IP address
   - IP Address: 10.3.41.132
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 10.3.41.254

[Close]
```

Note: 1. If you choose *Obtain IP address automatically (DHCP)*, when the switch starts up it waits to get its IP address from the DHCP server. If
it hasn’t obtained the address after one minute, it automatically reverts to its factory default IP address (192.168.0.60.)

2. If the CN8000A is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 165, for information.

**Disable Dev Authentication**
Selecting *Disable Dev Authentication* will disable local login authentication on the CN8000A. The switch can only be accessed using LDAP, LDAPS, MS Active Directory, RADIUS or CC Management authentication. For more information, see *ANMS - Authentication*, page 51.

**Reset Default Values**
Click *Reset Default Values* to use the default factory settings of the CN8000A.

**Reset Certificate**
Click *Reset Certificate* to use the Private Certificate settings of the CN8000A. For more information, see *Private Certificate*, page 62.

**Reboot**
Click *Reboot* to power down and restart the CN8000A.
Chapter 4
Browser Login

The CN8000A can be accessed either from an Internet 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 172.

Logging In

To operate the CN8000A from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the CN8000A 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/CN8000A

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

2. If a Security Alert appears, click Continue to this website.

   The security certificate can be trusted (See Trusted Certificates, page 174, for details).
3. The CN8000A login page appears:

![Login Page](image)

4. Provide a valid Username and Password (set by the CN8000A 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 34).

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.

5. After you have successfully logged in, the CN8000A Main Screen appears:
Main Webpage Elements

The Main page consists of two sections the Sidebar and Interactive Display Panel, as shown below. Each section of the web browser is explained in detail in Chapter 5, Administration.

Sidebar

The Sidebar to the left provides a tree view menu of links to the Basic Settings, Advanced Settings, and Preferences, that relate to the various options. A lower bar provides two icons allowing you to Logout or launch the Viewer. The next page provides a basic overview of each submenu.

Interactive Display Panel

The screen to the right of the sidebar is your main work area. The screens that appear reflect your sidebar menu choices, and allow you to make changes to the CN8000A.

Note: If a user doesn’t have permission to perform a particular activity, the menu for that activity doesn’t appear. See User Management, page 34, for permission details.
### Sidebar Submenu

<table>
<thead>
<tr>
<th>Sidebar Menu</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Basic Settings** | - **User Management**- Create, Manage and set Permissions for User Accounts.  
- **Session**- View and End current CN8000A user sessions.  
- **Maintenance**- Perform Backups, Restores, and Firmware upgrades. |
| **Advanced Settings** | - **Device Information**- View the CN8000A’s system information.  
- **Network**- Manage network settings.  
- **ANMS**- Manage Advanced Network Management Settings.  
- **Security**- Manage filters, policies, encryption, virtual Media, and private certificate information.  
- **Console Management**- Configure serial port settings.  
- **Date/Time**- Set date and time information for the CN8000A.  
- **Customization**- Customize the CN8000A system settings. |
| **Preferences** | - **User Preferences**- Set the current users default settings and password.  
- **Log**- View event information logged for the CN8000A.  
- **Remote Console**- Provides a Remote Console Preview, Exit Macro setup, and Power Management.  
- **Download**- Provides a link to install the Windows Client AP, Java Client AP and Log Server AP. |
| **About** | Click this link to display the CN8000A’s firmware version, and copyright information. |
| **Viewer** | Launches the Java or WinClient Viewer application for remote server access. |
| **Logout** | Click this icon to log out and end your CN8000A session. For security reasons, it is important to log out when your session ends. Otherwise, if Disable Duplicate Login is checked, other users must wait until the timeout setting has expired, and the system logs you out, before the CN8000A can be accessed (see Disable Duplicate Login, page 59). |
4. Browser Login

**Viewer**

You can connect to the remote server by clicking the *Viewer* icon from the lower section of the sidebar.

After clicking the *Viewer* icon:

- If you are logged in with a browser other than Windows Internet Explorer, a *Java Applet Viewer* application will open your remote server session.
- If you are logged in with IE as your browser, and you chose *Auto* as your Default Viewer, a WinClient Viewer application will open your remote server session.
- If you are logging in with IE as your browser, and you chose *Java* as your Default Viewer, a *Java Applet Viewer* application will open your remote server session.

Clicking the *Viewer* icon opens the remote server’s display on your desktop. Information on Java Applet Viewer operation is discussed in Chapter 7; WinClient Viewer operation is discussed in Chapter 6.
This Page Intentionally Left Blank
Chapter 5
Administration

Introduction

Administration of the CN8000A using a web browser is divided into 3 sections: Basic Settings, Advanced Settings, and Preferences. Each section is listed on the sidebar with sub-menus that are used to configure the CN8000A’s operating environment. This chapter discusses each of them in turn.

Note:
1. As you make your configuration changes in each section, click Apply to save them.
2. Some configuration changes only take effect after the CN8000A is reset. When those changes are made, a check is automatically put in the Reset on Exit box (see Customization, page 72). 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 34), the Administration configuration dialogs are not available.
Basic Settings

This section provides 3 sub-menus: User Management, Sessions, and Maintenance, used to manage user accounts and perform system maintenance on the CN8000A.

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 under User Information, Role and Permissions, then click Add. The new user’s name appears in the left panel. The fields in the right panel are explained in the table on the next page.

- 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 password fields are filled with round bullets. If you do not want to change the user’s password, simply leave the two fields as is.

- 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, as described in the table on the next page.
An explanation of the profile items is given in the table below:

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>From 1 to 16 characters are allowed depending on the Account Policy settings. See Account Policy, page 59.</td>
</tr>
<tr>
<td>Password</td>
<td>From 0 to 16 characters are allowed depending on the Account Policy settings. See Account Policy, page 59.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>To be sure there is no mistake in the password you are asked to enter it again. The two entries must match.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the user that you may wish to include.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Gives the user Administrator level access to the CN8000A. All permissions (except View Only) are granted (see Permissions below).</td>
</tr>
<tr>
<td>User</td>
<td>Gives the user User level access to the CN8000A. Windows Client, Power Manager, and Java Client permissions are granted (see Permissions below).</td>
</tr>
<tr>
<td>Select</td>
<td>Select is the default account type. It allows the administrator to select which permissions the user will be allowed.</td>
</tr>
</tbody>
</table>
The **Reset** button clears all the information shown in the right panel.

- When you have made all your changes, click **Apply**.
Sessions

The Sessions page lets the administrator see at a glance all the users currently logged into the CN8000A, and provides information about each of their sessions.

<table>
<thead>
<tr>
<th>Username</th>
<th>IP</th>
<th>Login Time</th>
<th>Client</th>
<th>Category</th>
<th>Devices</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.1.41.57</td>
<td>2016/07/26 10:41:54</td>
<td>Browser</td>
<td>Administrator</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.1.41.57</td>
<td>2016/07/26 14:04:57</td>
<td>WinClient</td>
<td>Administrator</td>
<td>CN8000A_Neogan [01] KVM Port</td>
<td></td>
</tr>
<tr>
<td>user01</td>
<td>10.1.41.57</td>
<td>2016/07/26 14:04:57</td>
<td>Browser</td>
<td>Xor</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

The meanings of the headings at the top of the page are fairly straightforward.

- **Username** refers to the account that the user logged in with.
- **IP** refers to the IP address that the user has logged in from.
- **Login Time** refers to the date and time that the account logged in.
- **Client** refers to the means the user employed to connect to the CN8000A (Browser, WinClient AP, JavaClient AP, etc.).
- **Category** lists the type of user who has logged in: Admin (Administrator), User, or Select. (See User Management, page 34 for details about user types.)
- **Devices** lists the device name given to the CN8000A.
- **Ports** lists the name of the name of the KVM port that is being accessed by the user.

This page also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session**; or refreshing the Sessions page by clicking **Refresh**.
Maintenance

The Maintenance page allows Administrators to upgrade the firmware, backup/restore the CN8000A’s settings and user information, and ping devices.

Upgrade Main Firmware

As new versions of the CN8000A 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 CN8000A; and click the Maintenance link 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 Upgrade Firmware.

   If Check Main Firmware Version is enabled, when you perform an upgrade the current firmware level is compared with that of the upgrade file. If the current version is higher than or equal to the upgrade version, a message appears informing you of the fact and the procedure stops.

   **Note:** If you want to install an older firmware version, you must uncheck the Check Firmware Version checkbox before clicking Upgrade Firmware.

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.
5. Administration

6. In the screen that comes up click **Yes** to confirm that you want to exit and reset the CN8000A.

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

**Backup**

The *Backup* section of the Backup/Restore page gives you the ability to back up the CN8000A’s configuration and user profile information.

To perform a backup, do the following:

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

   **Note:** If you set a password, make a note of it, since you will need it to be able to perform restore operations with the file.

2. Click **Backup**.

3. When the browser asks what you want to do with the file, select *Save*; then save it in a convenient location.

   **Note:** The CN8000A saves all its backup files as *Sysconfig.cfg*. If you want to save more than one backup file, simply rename the file to something convenient when you save it.

**Restore**

Backed up User Account and Configuration information can be restored in the *Restore* section of the page. Information currently configured on the CN8000A will be replaced with the information that you choose to restore.
To restore a previous backup, do the following:

1. If a password was set when the backup was made, key the same password that you used to save the backup file in the **Password** field. If a password wasn’t set, you can leave this field blank.

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. Select which parts of the backup you wish to restore:
   - Click the **Select All** radio button to restore both User Account and all CN8000A configuration information
   - Click the **User Account** radio button to only restore User Account information
   - Select the **User Select** radio button to choose which parts of the backed up information you wish to restore, then click the checkboxes below the **Options** heading to select/deselect the restore elements.

4. When you have made your selections, click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.
Ping Host
The Ping Host page allows you to ping the IP address of a device to see if it’s responding on the network. To ping a device, enter the IP address and click Ping.

<table>
<thead>
<tr>
<th>IP address/Host Name</th>
<th>10.3.41.100</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Result</strong></td>
<td></td>
</tr>
<tr>
<td>Ping 10.3.41.100 with 32 bytes of data:</td>
<td></td>
</tr>
<tr>
<td>Reply from 10.3.41.100: bytes=32 time = 1 ms</td>
<td></td>
</tr>
<tr>
<td>Reply from 10.3.41.100: bytes=32 time = 1 ms</td>
<td></td>
</tr>
<tr>
<td>Reply from 10.3.41.100: bytes=32 time = 1 ms</td>
<td></td>
</tr>
<tr>
<td>Reply from 10.3.41.100: bytes=32 time = 1 ms</td>
<td></td>
</tr>
</tbody>
</table>
Advanced Settings

This section provides 7 sub-menus: Device Information, Network, ANMS, Security, Console Management, Date/Time, and Customization, used to configure device settings for the CN8000A.

Device Information

The *Device Information* page is the first of the Advanced Settings pages, and provides information about the CN8000A’s status.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>To make it easier to manage installations that have more than one CN8000A, each one can be given a name. To assign a name for the CN8000A, key in one of your choosing (50 characters max.), then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The CN8000A's MAC Address is displayed here.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Indicates the CN8000A's current firmware version level. New versions of the CN8000A's firmware can be downloaded from our website as they become available (see [Upgrade Main Firmware], page 38). You can reference this number to see if there are newer versions available on the website.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the CN8000A's Internet Protocol Version 4 (32 bit) address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the CN8000A's Subnet Mask address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Displays the CN8000A's Default Gateway address.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Displays the CN8000A's Internet Protocol Version 6 (128 bit) address (Appears only when an IPv6 address is assigned).</td>
</tr>
<tr>
<td>IPv6 Subnet Prefix Length</td>
<td>Displays the prefix length of the IPv6 Subnet address (Appears only when an IPv6 address is assigned).</td>
</tr>
</tbody>
</table>
Network
The Network page is used to specify the CN8000A’s network environment.

IP Installer
The IP Installer is an external Windows-based utility for assigning IP addresses.

Click one of the radio buttons to select Enabled, View Only, or Disable for the IP Installer utility. See page 165 for IP Installer details.

Note: 1. If you select View Only, you will be able to see the CN8000A in the IP Installer’s Device List, but you will not be able to change the IP address.

2. For security, we strongly recommend that you set this to View Only or Disabled after using it.
Service Ports

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). If a port other than the default is set, users must specify the port number as part of the IP address when they login from a WinClient or Java Client AP program. If not, an invalid port number (or no port number) is specified, the CN8000A will not be found.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>This is the port number for connecting to the CN8000A from the Windows Client and Java Applet Viewers, and from the Windows and Java AP programs. The default is 9000.</td>
</tr>
<tr>
<td>HTTP</td>
<td>The port number for a browser login. The default is 80.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>The port number for a secure browser login. The default is 443.</td>
</tr>
<tr>
<td>SSH</td>
<td>The port for SSH access. The default is 22.</td>
</tr>
<tr>
<td>Telnet</td>
<td>The port for Telnet access. The default is 23.</td>
</tr>
</tbody>
</table>

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

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

3. If port numbers are not set to the default value, any user trying to access the CN8000A from a Windows Client AP, Java Client AP, third party SSH or Telnet viewer, or via web browser will need to specify the new port number for access.
IPv4 Settings

The CN8000A can have its IPv4 address assigned dynamically at boot-up (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the Obtain IP address automatically [DHCP], radio button. (This is the default setting.)
- To specify a fixed IP address, select the Set IP address manually [Fixed IP], radio button and fill in the IP Address, Subnet Mask and Default Gateway.

**Note:**
1. If you choose Obtain IP address automatically [DHCP], when the switch starts up it waits to get its IP address from the DHCP server. If it hasn’t obtained the address after one minute, it automatically reverts to its factory default IP address (192.168.0.60.)
2. If the CN8000A is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see IP Address Determination, page 165, for information.

**DNS Server**

The CN8000A can have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the Obtain DNS server address automatically, radio button.
- To specify a fixed address, select the Set DNS server address manually, radio button and fill in the required information.

**Note:** Specifying an alternate DNS Server address is optional.
IPv6 Settings

The CN8000A can have its IPv6 address assigned dynamically at boot-up (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the Obtain IPv6 address automatically [DHCP], radio button. (This is the default setting.)
- To specify a fixed IP address, select the Set IPv6 address manually [Fixed IP], radio button and fill in the IPv6 Address, Subnet Prefix Length and Default Gateway.

Note: If the CN8000A is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see IP Address Determination, page 165, for information.

DNS Server

The CN8000A can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the Obtain DNS server address automatically, radio button.
- To specify a fixed address, select the Set DNS server address manually, radio button and fill in the required information.

Note: Specifying an alternate DNS Server address is optional.
DDNS

DDNS maps the dynamic IP address assigned by a DHCP server to a host name. The CN8000A can update the DDNS server with its IP address whenever the IP address is changed.

To enable the DDNS capability for the CN8000A, do the following:

1. Check Enable.
2. Enter the Host Name that you registered with your DDNS service provider.
3. Drop down the DDNS list to select the DDNS service you are registered with.
4. Key in the Username and Password that authenticates you with your DDNS service.
5. In the DDNS Retry Time field, key in how many hours the CN8000A waits before it tries to reconnect to the DDNS server, when the CN8000A fails to connect.

Network Transfer Rate

This setting allows you to tailor the size of the data transfer stream to match network traffic conditions by setting the rate at which the CN8000A transfers data to remote computers. The range is from 4–99999 Kilobytes per second (KBps).

Finishing Up

After making any network changes, be sure Reset on exit on the Customization page (see Customization, page 72) 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 CN8000A off and on.
ANMS - Event Destination

The Advanced Network Management Settings Event Destination page allows you to set up login authentication and authorization management from external sources. It is divided into several sections, described in the sections that follow.

SMTP Settings

To have the CN8000A email reports from the SMTP server to you, do the following:

1. Enable the Enable report from the following SMTP Server, and key in the SMTP Server IP address and Service Port.
   - If you select My server requires secure connection (SSL) the Service Port entry is changed to 465.

2. If your server requires authentication, put a check in the Server requires authentication checkbox, and key in the appropriate account information in the Account Name and Password fields.

3. Key in the email address of where the report is being sent from in the From field.

   Note: 1. Only one email address is allowed in the From field, and it cannot exceed 64 Bytes.

2. 1 Byte = 1 English alphanumeric character.
4. Key in the email address (addresses) of where you want the SMTP reports sent to in the To field.

**Note:** 1. If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 Bytes.
2. 1 Byte = 1 English alphanumerical character.

5. Select the report options you would like sent. Choices include: Report IP Address, Report system reboot, Report user login and Report user logout.

**Log Server**

Important transactions that occur on the CN8000A, 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 Service Port field. The valid port range is 1–65535. The default port number is 9001.

**Note:** The port number must be different than the one used for the Program port (see Program, page 44).

**SNMP Server**

To be notified of SNMP trap events, do the following:
1. Check *Enable SNMP Agent*.

2. Key in the *Server IP* address and *Service Port* number of the computer to be notified of SNMP trap events. The valid port range is 1-65535.

**Note:** The following SNMP trap events are sent: System Power On, Login Failure, and System Reset.

## Syslog Server

![Syslog Server](image)

To record all the events that take place on the CN8000A and write them to a Syslog server, do the following:

1. Check *Enable*.

2. Key in the *Server IP* address and *Service Port* number of the Syslog server. The valid port range is 1-65535.
ANMS - Authentication
The Advanced Network Management Settings Authentication page allows you to set up login authentication and authorization management from external sources. It is divided into several sections, which are described in the sections that follow.

Disable Local Authentication
Selecting this option will disable local login authentication on the CN8000A. The switch can only be accessed using LDAP, LDAPS, MS Active Directory, RADIUS or CC Management authentication.

RADIUS Settings

<table>
<thead>
<tr>
<th>RADIUS Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>[ ]</td>
</tr>
<tr>
<td>Preferred RADIUS Server IP:</td>
<td></td>
</tr>
<tr>
<td>Preferred RADIUS Service Port:</td>
<td>0</td>
</tr>
<tr>
<td>Alternate RADIUS Server IP:</td>
<td></td>
</tr>
<tr>
<td>Alternate RADIUS Service Port:</td>
<td>0</td>
</tr>
<tr>
<td>Timeout:</td>
<td>0 sec</td>
</tr>
<tr>
<td>Retries:</td>
<td>0</td>
</tr>
<tr>
<td>Shared Secret (at least 6 characters):</td>
<td></td>
</tr>
</tbody>
</table>

To allow authentication and authorization for the CN8000A through a RADIUS server, do the following:

1. Check Enable.
2. Fill in the IP addresses and port numbers for the Preferred and Alternate RADIUS servers.
3. In the Timeout field, set the time in seconds that the CN8000A 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 CN8000A and the RADIUS Server.

(Continues on next page.)
6. On the RADIUS server, set the access rights for each user according to the information in the table, below:

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Grants the user administrator privileges, allowing the user to configure the system.</td>
</tr>
<tr>
<td>w</td>
<td>Allows the user to access the system via the Windows Client program.</td>
</tr>
<tr>
<td>j</td>
<td>Allows the user to access the system via the Java applet.</td>
</tr>
<tr>
<td>p</td>
<td>Allows the user to Power On/Off, Reset devices via an attached PN0108.</td>
</tr>
<tr>
<td>l</td>
<td>Allows the user to access log information via the user’s browser.</td>
</tr>
<tr>
<td>v</td>
<td>Limits the user’s access to only viewing the video display.</td>
</tr>
<tr>
<td>s</td>
<td>Allows the user to use the Virtual Media function in Read Only mode.</td>
</tr>
<tr>
<td>m</td>
<td>Allows the user to use the Virtual Media function in Read/Write mode.</td>
</tr>
<tr>
<td>t</td>
<td>Allows the user to access the system via a Telnet session.</td>
</tr>
<tr>
<td>h</td>
<td>Allows the user to access the system via an SSH session.</td>
</tr>
<tr>
<td>a</td>
<td>Allows the user to access the system via a Telnet or SSH session su/user</td>
</tr>
<tr>
<td></td>
<td>Where user represents the Username of a CN8000A user whose permissions reflect the permissions you want the RADIUS authorized user to have.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>String</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>c,w,p</td>
<td>User has administrator privileges; user can access the system via the Windows Client; user can access the attached PN0108</td>
</tr>
<tr>
<td>w,j,l</td>
<td>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.</td>
</tr>
</tbody>
</table>
To allow authentication and authorization for the CN8000A via LDAP / LDAPS, refer to the information in the table, below:

<table>
<thead>
<tr>
<th>Item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Put a check in the Enable checkbox to allow LDAP / LDAPS authentication and authorization.</td>
</tr>
<tr>
<td>LDAP / LDAPS</td>
<td>Click a radio button to specify whether to use LDAP or LDAPS.</td>
</tr>
<tr>
<td>Enable Authorization</td>
<td>Select whether to enable Enable Authorization, or not.</td>
</tr>
<tr>
<td>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 135, for details.</td>
<td></td>
</tr>
<tr>
<td>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 'CN8000A 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.</td>
<td></td>
</tr>
<tr>
<td>Note: Consult the LDAP / LDAPS administrator to ascertain whether to enable the Enable Authorization function, or not.</td>
<td></td>
</tr>
<tr>
<td>LDAP Server and Port</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Set the time in seconds that the CN8000A waits for an LDAP or LDAPS server reply before it times out.</td>
</tr>
<tr>
<td>Admin DN / Name</td>
<td>Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: cn=LDAPAdmin,ou=CN8000A,dc=aten,dc=com</td>
</tr>
<tr>
<td>Password</td>
<td>Key in the LDAP administrator’s password.</td>
</tr>
</tbody>
</table>
CC Management Settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search DN</td>
<td>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 CN8000A Admin Group is created. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.</td>
</tr>
</tbody>
</table>

To allow authorization for the CN8000A 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.
Security
The Security page controls access to the CN8000A.

Login Failures
For increased security, the Login Failures section allows administrators to set policies governing what happens when a user fails to log in successfully.

To set the Login Failures policies, check the Enable checkbox (the default is for Login Failures to be enabled). The meanings of the entries are explained in the table below:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed</td>
<td>Sets the number of consecutive failed log in attempts that are permitted from a remote computer. The default is 5 times.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Sets the amount of time a remote computer must wait before attempting to log in again after it has exceeded the number of allowed failures. The default is 3 minutes.</td>
</tr>
<tr>
<td>Lock Client PC</td>
<td>If this is enabled, after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No log ins from that computer will be accepted. The default is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This function relates to the client computer’s IP. If the IP is changed, the computer will no longer be locked out.</td>
</tr>
<tr>
<td>Lock Account</td>
<td>If this is enabled, after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is enabled.</td>
</tr>
</tbody>
</table>

**Note:** If you don’t enable Login Failures, users can attempt to login an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.
Filter
If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.

IP and MAC Filters control access to the CN8000A based on the IP and/or MAC addresses of the computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed.

To enable IP and/or MAC filtering, Click to put a check mark in the Enable IP Filter and/or Enable MAC Filter checkbox.

- If the Include button is checked, all the addresses within the filter range are allowed access; all other addresses are denied access.
- If the Exclude button is checked, all the addresses within the filter range are denied access; all other addresses are allowed access.
Adding Filters
To add an IP filter, do the following:

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

```
IP Filter

From: [ ]
To: [ ]

[OK] [Cancel]
```

2. Key the address you want to filter in the *From*: field.
   - To filter a single IP address, key the same address in the *To*: field.
   - To filter a continuous range of addresses, key in the end number of the range in the *To*: field.

3. After filling in the address, click **OK**.
4. Repeat these steps for any additional IP addresses you want to filter.

To add a MAC filter, do the following:

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

```
MAC Filter

MAC Address: [ ]

[OK] [Cancel]
```

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.

**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.
Modifying Filters
To modify a filter, select it in the IP Filter or MAC Filter list box and click Modify. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

Deleting Filters
To delete a filter, select it in the IP Filter or MAC Filter list box and click Delete.

Login String
The Login String lets the Administrator specify a login string that users must include (in addition to the IP address) when they access the CN8000A with a browser. For example:

192.168.0.126/CN8000A

- The following characters are allowed:
  0–9 a–z A–Z ~ ! @ $ ^ & * ( ) _ + = \ } { ; ' < > , . |

- The following characters are not allowed:
  ♦ % " : / ? # \ [Space]
  ♦ Compound characters (É Ç ñ ... etc.)

Note: 1. There must be a forward slash between the IP address and the string.

2. If no login string is specified here, anyone will be able to access the CN8000A login page using the IP address alone. This makes your installation less secure.

For security purposes, we recommend that you change this string occasionally.
Account Policy

In the Account Policy section, system administrators can set policies governing usernames and passwords.

The meanings of the Account Policy entries are explained in the table below:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Username Length</td>
<td>Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>Sets the minimum number of characters required for a password. Acceptable values are from 0–16. A setting of 0 means that no password is required, and users can login with only a Username. The default is 6.</td>
</tr>
<tr>
<td>Password Must Contain At Least</td>
<td>Checking any of these items requires users to include at least one uppercase letter, one lowercase letter or one number in their password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This policy does not affect existing user accounts. Only new user accounts created after this policy has been enabled, and users required to change their passwords are affected.</td>
</tr>
<tr>
<td>Disable Duplicate Login</td>
<td>Check this to prevent users from logging in with the same account at the same time.</td>
</tr>
<tr>
<td>Enforce Password History</td>
<td>Check this box and enter the number of times a unique password must be created before an old password can be used again. The number represents the number of passwords that the system will remember to enforce the password history requirement.</td>
</tr>
</tbody>
</table>
Encryption

These flexible encryption alternatives for keyboard/mouse, video, and virtual media data let you choose any combination of DES; 3DES; AES; RC4; or a Random cycle of any or all of them.

Enabling encryption will affect system performance – no encryption offers the best performance; the greater the encryption the greater the adverse effect. If you enable encryption, the performance considerations (going from best to worst) are as follows:

- RC4 offers the least performance impact; DES is next; then 3DES or AES
- The RC4 + DES combination offers the least impact of any combination
Working Mode
Use this section to set the working mode parameters.

- **Enable ICMP** so that the CN8000A can be pinged. If it is not enabled, the device cannot be pinged. The default is **Enabled**.
- **Enable Multiuser Operation** to permit more than one user to log into the CN8000A at the same time. The default is **Enabled**.
- **Enable Virtual Media Write** allows redirected virtual media devices on a user’s system to send data to a remote server, as well as being able to have data from the remote server written to them. The default is **Enabled**.
- **Browser Service** allows the administrator to limit the scope of browser access to the CN8000A. Put a check in the checkbox to enable this function, then select the browser limitation in the drop down list box. Choices are explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Browser</td>
<td>If this is selected, the CN8000A cannot be accessed via a browser. It can only be accessed from the AP programs (see AP Operation, page 133).</td>
</tr>
<tr>
<td>Disable HTTP</td>
<td>If this is selected, the CN8000A can be accessed via a browser, but not from an ordinary (HTTP) login connection – it can only be accessed over a secure HTTPS (SSL) connection.</td>
</tr>
<tr>
<td>Disable HTTPS (SSL)</td>
<td>If this is selected, the CN8000A can be accessed via a browser over an ordinary (HTTP) login connection, but not via a secure HTTPS (SSL) connection.</td>
</tr>
</tbody>
</table>

- **If Disable Authentication** is checked, no authentication procedures are used to check users attempting to log in. Users gain Administrator access to the CN8000A switch simply by entering combination of username and password.

**Note:** Enabling this setting creates an extremely dangerous result as far as security goes, and should only be used under very special circumstances.
Private Certificate
When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the Private Certificate section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.

There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

- **Generating a Self-Signed Certificate**
  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See Self-Signed Private Certificates, page 178 for details about using OpenSSL to generate your own private key and SSL certificate.

- **Obtaining a CA Signed SSL Server Certificate**
  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After the CA sends you the certificate, save it to a convenient location on your computer.

- **Importing the Private Certificate**
  To import the private certificate, do the following:

  1. Click **Browse** to the right of **Private Key**; browse to where your private encryption key file is located; and select it.

  2. Click **Browse** to the right of **Certificate**; browse to where your certificate file is located; and select it.

  3. Click **Upload** to complete the procedure.

**Note:** Both the private encryption key and the signed certificate must be imported at the same time.
Certificate Signing Request
The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.

To perform this operation do the following:

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

2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

<table>
<thead>
<tr>
<th>Information</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country (2 letter code)</td>
<td>TW</td>
</tr>
<tr>
<td>State or Province</td>
<td>Taiwan</td>
</tr>
<tr>
<td>Locality</td>
<td>Taipei</td>
</tr>
<tr>
<td>Organization</td>
<td>Your Company, Ltd.</td>
</tr>
<tr>
<td>Unit</td>
<td>Techdoc Department</td>
</tr>
<tr>
<td>Common Name</td>
<td>mycompany.com This must be the exact domain name of the site that you want the certificate to be valid for. If the site’s domain name is <a href="http://www.mycompany.com">www.mycompany.com</a>, and you only specify mycompany.com, the certificate will not be valid.</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:administrator@yourcompany.com">administrator@yourcompany.com</a></td>
</tr>
</tbody>
</table>
3. After filling in the form (all fields are required), click **Create**.
   A self-signed certificate based on the information you just provided is now stored on the CN8000A.

4. Click **Get CSR**, and save the certificate file (*csr.cer*) to a convenient location on your computer
   This is the file that you give to the third party CA to apply for their signed SSL certificate.

5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Browse** to locate the file; then click **Upload** to store it on the CN8000A.

   **Note:** When you upload the file, the CN8000A checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Remove CSR**.
Console Management

This section discusses methods of opening the CN8000A console via OOBC or serial connection.

OOBC

In case the CN8000A cannot be accessed with the usual LAN-based methods, it can be accessed via the switch’s modem port. To enable support for PPP (modem) operation, click to put a checkmark in the Enable Out of Band Access checkbox.

**PPP Settings**

When you enable Out of Band Access, the Enable Dial Back, and Enable Dial Out functions become available, as described in the sections that follow.

Dial Back

As an added security feature, if this function is enabled, the switch disconnects the calls that dial in to it, and dials back to one of the entries specified below:

- **Enable Fixed Number Dial Back**: If Fixed Number Dial Back is enabled, when there is an incoming call, the CN8000A hangs up the modem and dials back to the modem whose phone number is specified in the Phone Number field.

  Key the phone number of the modem that you want the CN8000A to dial back to in the Phone Number field.

- **Enable Flexible Dial Back**: If Flexible Dial Back is enabled, the modem that the CN8000A dials back to doesn’t have to be fixed. It can dial back to any modem that is convenient for the user, as follows:

  1. Key the password that the users must specify in the Password field.

  2. When connecting to the CN8000A’s modem, users specify the phone number of the modem that they want the CN8000A to dial back to as their Username, and specify the password set in the Password field for their password.
Dial Out
For the dial out function, you must establish an account with an Internet Service Provider, and use a modem to dial up to your ISP account. An explanation of the Enable Dial Out items is given in the table below:

- **ISP Settings**: Specify the telephone number, account name (username), and password that you use to connect to your ISP.
- **Dial Out Schedule**: This entry sets up the times you want the CN8000A to dial out over the ISP connection. *Every* provides a listing of fixed times from every hour to every four hours.
  - If you select *Every two hours* (for example), the CN8000A will start dialing out every two hours beginning at 00:00.
  - If you don't want the CN8000A to dial out on a fixed schedule, select *Never* from the list.
- **Daily at** will dial out once a day at a specified time. Use the hh:mm format to specify the time.
5. Administration

- **PPP online time** specifies how long you want the ISP connection to last before terminating the session and hanging up the modem. A setting of zero means it is always on line.

- **Emergency Dial Out**: If the CN8000A gets disconnected from the network, or the network goes down, this function puts the switch on line via the ISP dial up connection.
  - If you choose **PPP stays online until network recovery**, the PPP connection to the ISP will last until the network comes back up or the switch reconnects to it.
  - If you choose **PPP online time**, the connection to the ISP will terminate after the amount of time that you specify is up. A setting of zero means it is always on line.

- **Dial Out Mail Configuration**: This section provides email notification of problems that occur on the devices connected to the CN8000A’s ports.

  **Note:** This email notification differs from the one configured under **SMTP Settings** in that it uses the ISP mail server rather than the internal company’s mail server.

- Key in the IPv4 address, IPv6 address, or domain name of your SMTP server in the **SMTP Server IP Address** field, and enter the corresponding port in the **Service Port** field.
- If your server requires a secure SSL connection, put a check in the **SMTP server requires secure connection (SSL)** checkbox.
- If your server requires authentication, put a check in the **SMTP server requires authentication** checkbox, then key in the appropriate account name and password in the fields, below.
- Key in the email address of the person responsible for the SMTP server (or some other equally responsible administrator), in the **Email From** field.
- Key in the email address (addresses) of where you want the report sent to in the **To** field. If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon.

When you have finished making your settings on this page, click **Save**.
Serial Console
To configure the CN8000A to interact with the connected serial device, you need to set its parameters to match the parameters of the device in the Port Property Settings.

| Port Property/Settings |  |  |  |
|------------------------|------------------|------------------|
| Baud Rate:             | 9600             | Data Bits:       | 8 |
| Parity:                | None             | Stop Bits:       | 1 |
| Flow Control:          | None             |                  |   |

Select the values that match the ones used by the connected serial console device. The port property settings that the CN8000A supports are as follows:

- **Baud Rate**: This sets the port’s data transfer speed. Choices are from 300–115200 (drop down the list to see them all). Set this to match the baud rate setting of the serial console device. Default is 9600 (which is a basic setting for many serial console devices).

- **Data Bits**: This sets the number of bits used to transmit one character of data. Choices are: 7 and 8. Set this to match the data bit setting of the serial console device. Default is 8 (which is the default for the majority of serial console devices).

- **Parity**: This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even. Set this to match the parity setting of the serial console device. Default is None.

- **Stop Bits**: This indicates that a character has been transmitted. Set this to match the stop bit setting of the serial console device. Choices are: 1 and 2. Default is 1 (which is the default for the majority of serial console devices).

- **Flow Control**: This allows you to choose how the data flow will be controlled. Choices are: None, Hardware, and XON/XOFF. Set this to
match the flow control setting of the serial console device. Default is None.

**Note:** None is only supported for baud rates of 9600 and lower. For baud rates greater than 9600, you must choose Hardware or XON/XOFF.

- **Port Alert Properties:** You can specify up to 10 types of events (e.g., Power On). Enter them in the provided Alert String (1 - 10) fields.

When you have finished making your selections, click **Save**.
Date/Time

The Date/Time dialog page sets the CN8000A time parameters:

- **Time Zone**: To establish the time zone that the CN8000A is located in, drop down the Time Zone list and choose the city that most closely corresponds to where it is at.
- **Daylight Savings Time**: If your country or region employs Daylight Saving Time (Summer Time), check the corresponding checkbox.

Set the parameters according to the information below.

**Time Zone**

- To establish the time zone that the CN8000A is located in, drop down the Time Zone list and choose the city that most closely corresponds to where it is at.
- If your country or region employs Daylight Saving Time (Summer Time), check the corresponding checkbox.
Date
- Select the month from the drop-down list box.
- Click < or > to move backward or forward by one year increments.
- In the calendar, click on the day.

Time
- To set the time, key in the numbers using the 24 hour HH:MM:SS format.
- Click Set to save your settings.

Network Time
To have the time automatically synchronized to a network time server, do the following:
1. Check the Enable auto adjustment checkbox.
2. Drop down the time server list to select your preferred time server
   - or –
   Check the Preferred custom server IP checkbox, and key in the IP address
   of the time server of your choice.
3. If you want to configure an alternate time server, check the Alternate time
   server checkbox, and repeat step 2 for the alternate time server entries.
4. Key in your choice for the number of days between synchronization
   procedures.
5. If you want to synchronize immediately, click Adjust Time Now.

Note: After checking the Enable auto adjustment checkbox, you must click
Adjust Time Now or Set to save the change. Otherwise, the setting will
be lost.
Customization
Use this section to edit the device settings.

<table>
<thead>
<tr>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Force All to Grayscale</td>
</tr>
<tr>
<td>☑ Enable Client AP Device List</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB IO Settings</th>
<th>OS:</th>
<th>Language:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiuser Mode</th>
<th>Multiuser Mode:</th>
<th>Occupy Timeout:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Share</td>
<td>sec (0-255)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Default Values</td>
</tr>
</tbody>
</table>

- If **Force All to Grayscale** is enabled, the remote displays of all devices connected to the CN8000A are changed to grayscale. This can speed up I/O transfer in low bandwidth situations.

- If **Enable Client AP Device List** is enabled, the switch appears in the Server List when using the WinClient or Java Client AP (see The WinClient Viewer, page 79, and The JavaClient Viewer, page 113). If this option is not enabled, the switch can still be connected to, but its name will not appear in the Server List.

- **OS**: Specifies the operating system that the server on the connected port is using. Choices are Win, Mac, Sun, and Other. The default is Win.

- **Language**: Specifies the OS language being used by the server on the connected port. Drop down the list to see the available choices. The default is English US.

(Continues on next page.)
Multiuser Mode: Defines how a port is to be accessed when multiple users have logged on, as follows:

- **Exclusive:** The first user to switch to the port has exclusive control over the port. No other users can view the port.
- **Occupy:** The first user to switch to the port has control over the port. However, additional users may view the port’s video display.
- **Share:** Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically. Under these circumstances, users can take advantage of the Message Board, which allows a user to take control of the keyboard and mouse or keyboard, mouse, and video of a Share port (see The Message Board, page 80).

- **Occupy Timeout:** If there is no user input for the amount of time specified here, the control privilege is released and transferred to the next user who moves the mouse or uses the keyboard.

- **Reset:** After making any network changes, be sure Reset on exit 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 switch off and on.

Click Reset Default Values to use the default factory settings of the CN8000A.
Preferences

The following sections describe the administration utilities covered in this section, including the User Preferences, Log, Remote Console and Download pages. You can find the links to these screens under Preferences in the left panel menu.

User Preferences

The User Preferences screen allows the user to set the device password, as well as device parameters including the Language, OSD Hotkey, Logout Timeout and the Viewer.

Settings

Set device parameters using the following fields:

- **Language**: Selects the language that the interface displays in. Drop down the list to make your selection.
  
  Selecting **Auto** causes the CN8000A to display the pages in the same language to which the browser is set.

  If your browser is set to a non-supported language, the CN8000A looks to what your server’s operating system is set to. If the operating system is set to a supported language it will use that language to display its pages. If the operating system is set to a non-supported language, the CN8000A defaults to English. After making your choice, click **Save**.

- **OSD Hotkey**: Select the keyboard combination to call the OSD function.

- **Logout Timeout**: Set how many minutes the CN8000A allows a user session to last before terminating the session.
5. Administration

- **Launch viewer after login**: Checking this box will automatically launch the Viewer application after a user logs in to the CN8000A.

- **Viewer**: Choose the viewer you would like to use when viewing the remote server’s display. This is set to **Auto Detect** by default, which opens the WinClient for Windows systems.

**Password**
Change your password using the following fields:
- **Old Password**: Key in the old password.
- **New Password**: Key in the new password.
- **Confirm Password**: Key in the exact same characters to verify you have entered the correct new password

Click **Change Password** to apply your settings.

**Log**
The CN8000A logs all the events that take place on it. Following a reset, it writes them to a log file, which can be used as a searchable database with a log server. To view the contents of the log file, click **Log** under the Preference menu. A screen similar to the one below appears:

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>User</th>
<th>Log Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/07/27 11:22:36</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/27 09:41:09</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/25 17:33:34</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/26 17:22:29</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) logging out via browser.</td>
</tr>
<tr>
<td>2016/07/25 17:35:18</td>
<td>Least</td>
<td>administrator</td>
<td>EM: user administrator modified security setting.</td>
</tr>
<tr>
<td>2016/07/25 17:37:40</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/26 16:19:18</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/26 16:19:13</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.57 (50-ES-49-EA-7-4A) attempting to login via browser.</td>
</tr>
<tr>
<td>2016/07/26 16:13:08</td>
<td>Most</td>
<td>System</td>
<td>OP: user administrator from 10.3.41.134 (74-0E-62-EF-AD-7-33) attempting to login via browser.</td>
</tr>
</tbody>
</table>

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 127.

To clear the log file, click on the **Clear Log** icon at the lower right of the page.
Remote Console
This section provides a preview screen that shows a snapshot of the server’s display, as follows:

Clicking *Refresh* updates the snapshot of the remote display.

Exit Macro
The *Exit Macro* panel contains a drop-down list box of user created System macros: Select the *Exit Macro* you would like to use and click *Save*. See *System Macros*, page 91, for details on creating exit macros.

Telnet
If the Serial Console is enabled and a user has telnet access rights, then the “Open Telnet Client” button will appear on the Remote Console page. Click this button to launch the built-in telnet client AP.

Open Power Management
To configure the PN0108 (a Power Over the NET™ device), click *Open Power Management*. When a connection between the devices is established, you can
use the CN8000A to access the configuration screens of the PN0108. Clicking this button opens the login page of the PN0108 device.

**Note:**
1. Connection to the PN0108 or a Power Over the NET™ (PON) device can be viewed and managed through the browser, Windows and/or Java application (AP) programs, with the latest firmware version.
2. Refer to ATEN’s PN0108 User Manual (or a compatible PON device’s manual) for details on editing the power management configuration screens.

**About**
Click About to view the CN8000A’s firmware version.
Chapter 6
The WinClient Viewer

Starting Up

The WinClient Viewer is available by logging in using Microsoft’s Internet Explorer, selecting Auto as the Default Viewer (under Preferences - User Preferences) and clicking launch from the sidebar, at which time the CN8000A WinClient application will install on your computer. You can also use the WinClient Viewer to log in directly to the server from your computer. For more information on installing this stand alone client based application, See AP Operation, page 133, for details.

Click the Viewer icon, shown above, to launch the WinClient Viewer AP.
A second or two after you click the Viewer icon, the remote server’s display appears as a window on your desktop:

**Navigation**

You can work on the remote computer via the screen display, 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 WinClient Control Panel

The WinClient control panel is hidden at the upper center of the screen. It becomes visible when you move the mouse pointer over it:

![Control Panel Image]

**Note:** 1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Customize Control Panel*, page 108, for details.

2. To move the Control Panel to a different location on the screen, place the mouse pointer over the text bar area, then click and drag.

- By default, the left of the text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, however, the information in the text row changes to describe the icon's function. In addition, if a message from another user is entered in the message board, and you have not opened the message board, the message will appear in the text row.

- If the *User Info* function has been enabled under *Customize Control Panel* (see *User Info*, page 109), the total number of users currently logged into the CN8000A displays to the right of the video resolution in the text row.

- Right clicking in the text row area brings up a menu that allows you to select options for the Screen Mode, Zoom, Mouse Pointer type, Mouse Sync Mode, Macro List, and Local/Remote Share Mode. These functions are discussed in the sections that follow.
Control Panel Functions

The Control Panel functions are described in the table below.

Note: Clicking the T button at the top right of the windows that appear for the control panel functions brings up a slider bar to adjust the transparency of the dialog box. After making your adjustment, click anywhere in the dialog box to dismiss the slider.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="icon" /></td>
<td>This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>When you click this icon, the Control Panel collapses into 4 categories: Keyboard/Mouse, Video, Macro and Advanced. Hover your mouse over the categories to see the submenus. Click the icon again to revert to the original Control Panel format.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Click to bring up the Macros dialog box (see Macros, page 85, for details).</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Click to bring up the Video Options dialog box. Right-click to perform a quick Auto Sync (see Video Settings, page 94, for details).</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Click to perform a video and mouse autosync operation. It is the same as clicking the Auto-sync button in the Video Options dialog box (see Video Settings, page 94, for details).</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Toggles the display between Full Screen Mode and Windowed Mode.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Click to take a snapshot (screen capture) of the remote display. See Snapshot, page 109, for details on configuring the Snapshot parameters.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Click to bring up the Message Board (see The Message Board, page 97, for details).</td>
</tr>
</tbody>
</table>
6. The WinClient Viewer

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Click to send a Ctrl+Alt+Del signal to the remote system.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Click to toggle the remote display between color and grayscale.</td>
</tr>
</tbody>
</table>
| ![Icon](image3) | Click to bring up the Virtual Media dialog box. The icon changes when a virtual media device is started on the port (see Virtual Media, page 99, for details).  
**Note:** This icon displays in gray when the function is disabled or not available to the user. |
| ![Icon](image4) | Click to zoom the remote display window.  
**Note:** This feature is only available in windowed mode (Full Screen Mode is off). (See Zoom, page 103, for details). |
| ![Icon](image5) | Click to bring up the on-screen keyboard (see The On-Screen Keyboard, page 104, for details). |
| ![Icon](image6) | Click to select the mouse pointer type.  
**Note:** This icon changes depending on which mouse pointer type is selected (see Mouse Pointer Type, page 106, for details). |
| ![Icon](image7) | Click to toggle Automatic or Manual mouse sync.  
• When the selection is Automatic, the icon to the right appears.  
• When the selection is Manual, a / appears over the icon.  
(See Mouse DynaSync Mode, page 106, for details.) |
| ![Icon](image8) | Click to display a drop-down Macro List of User macros. Access and run macros more conveniently using this icon (see Macros, page 85, for details). |
| ![Icon](image9) | To configure the PN0108 (a Power Over the NET™ device), click Power Management. When a connection between the devices is established, you can use the CN8000A to access the configuration screens of the PN0108. Clicking this button opens the login page of the device. See Power Management, page 110, for details. |
| ![Icon](image10) | Click this icon to open a Viewer based GUI with the web browser administrative functionalities. See Admin Utility, page 111, for details. |
| ![Icon](image11) | Click to bring up the Customize Control Panel dialog box (see Customize Control Panel, page 108, for details). |
Exit

Click to exit the remote view and go back to the web browser Main Page.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Click on the icon to toggle the status.</td>
</tr>
</tbody>
</table>

These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer.

- When the lock state is On, the icon is highlighted in blue.
- When the lock state is Off, the icon is not highlighted.

**Note:** These icons and your local keyboard icons are in sync. Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.
Macros
The Macros icon provides access to three functions found in the Macros dialog box: Hotkeys, User Macros, and System Macros. Each of these functions is described in the following sections.

Hotkeys
Various actions, corresponding to clicking the Control Panel icons, can be accomplished directly from the keyboard with hotkeys. Selecting the Hotkeys radio button lets you configure which hotkeys perform the actions. The actions are listed to the left; their hotkeys are shown to the right. Use the checkbox to the left of an action’s name to enable or disable its hotkey.

If you find the default Hotkey combinations inconvenient, you can reconfigure them as follows:

1. Highlight an Action, then click Set Hotkey.
2. Press your selected Function keys (one at a time). The key names appear in the Hotkeys field as you press them.
   - You can use the same function keys for more than one action, as long as the key sequence is not the same.
   - To cancel setting a hotkey value, click Cancel; to clear an action’s Hotkeys field, click Clear.
3. When you have finished keying in your sequence, click Save.

To reset all the hotkeys to their default values, click Reset.
An explanation of the Hotkey actions is given in the table below:

<table>
<thead>
<tr>
<th>Action</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit remote location</td>
<td>Exits the remote view and goes back to the web browser Main Page. This is equivalent to clicking the Exit icon on the Control Panel. The default keys are F2, F3, F4.</td>
</tr>
<tr>
<td>Adjust Video</td>
<td>Brings up the Video Settings dialog box. This is equivalent to clicking the Video Settings icon on the Control Panel. The default keys are F5, F6, F7.</td>
</tr>
<tr>
<td>Toggle Control Panel</td>
<td>Toggles the Control Panel Off and On. The default keys are F3, F4, F5.</td>
</tr>
<tr>
<td>Toggle Mouse Display</td>
<td>If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely noticeable tiny circle, which can be ignored. Since this function is a toggle, use the hotkeys again to bring the mouse display back to its original configuration. This is equivalent to selecting the Dot pointer type from the Mouse Pointer icon on the Control Panel. The default keys are F7, F8, F9. Note: The Java Control Panel does not have this feature.</td>
</tr>
<tr>
<td>Adjust Mouse</td>
<td>This synchronizes the local and remote mouse movements. The default keys are F7, F8, F9.</td>
</tr>
<tr>
<td>Show/Hide Local Cursor</td>
<td>Toggles the display of your local mouse pointer off and on. This is equivalent to selecting the Null pointer type from the Mouse Pointer icon on the Control Panel. The default keys are F4,F5.</td>
</tr>
<tr>
<td>Substitute Ctrl key</td>
<td>If your local computer captures Ctrl key combinations, preventing them from being sent to the remote system, you can implement their effects on the remote system by specifying a function key to substitute for the Ctrl key. If you substitute the F11 key, for example, pressing [F11 + 5] would appear to the remote system as [Ctrl + 5]. The default key is F11. Note: When Keyboard Pass Through is enabled, [Alt + Tab] can be sent directly to the remote system (see Customize Control Panel, page 108, for details).</td>
</tr>
<tr>
<td>Substitute Alt key</td>
<td>Although all other keyboard input is captured and sent to the remote system, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F11. Note: When Keyboard Pass Through is enabled, [Alt + Tab] can be sent directly to the remote system (see Customize Control Panel, page 108, for details).</td>
</tr>
</tbody>
</table>
User Macros

User Macros are used to perform specific actions on the remote server. To create the macro, do the following:

1. Select the User Macros radio button, then click Add.

2. In the dialog box that comes up, replace “NewMacro” with a name of your choice for the macro:
3. Click **Record**.

   The dialog box disappears, and a small panel appears at the top left of the screen:

   ![Pause, Done, Cancel, Show buttons]

4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Record** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes:

   ![Macros dialog box with keystrokes and times]

   - Clicking **Cancel** cancels all keystrokes.
   - When you have finished, click **Stop**. This is the equivalent of clicking **Done** in Step 5.

**Note:**
1. Case is not considered – typing **A** or **a** has the same effect.
2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.
5. If you haven’t brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with the macro keys that you pressed displayed in the Macro column:

6. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.

7. Repeat the procedure for any other macros you wish to create.

**Running Macros**

After creating your macros, you can run them in any of three ways:

1. By using the hotkey (if one was assigned).
2. By opening the Macro List on the Control Panel and clicking the one you want (see *Macro List*, page 83).
3. By opening this dialog box and clicking **Play**.

If you run the macro from this dialog box, you have the option of specifying how the macro runs.

- If you choose **Play Without Wait**, the macro runs the keypresses one after another with no time delay between them.
If you choose *Play With Time Control*, the macro waits for the amount of time between key presses that you took when you created it. Click on the arrow next to *Play* to make your choice.

If you click *Play* without opening the list, the macro runs with the default choice. The default choice (*NoWait* or *TimeCtrl*), is shown in the *Playback* column.

You can change the default choice by clicking on the current choice (*NoWait* in the screenshot above), and selecting the alternative choice.

**Note:**
1. Information about the Search function is given on page 91.
2. User Macros are stored on the Local Client computer of each user. Therefore there is no limitation on the number of macros, the size of the macro names, or makeup of the hotkey combinations that invoke them.
Search
Search, at the bottom of the dialog box, lets you filter the list of macros that appear in the large upper panel for you to play or edit. Click a radio button to choose whether you want to search by name or by key; key in a string for the search; then click Search. All instances that match your search string appear in the upper panel.

System Macros
System Macros are used to create exit macros for when you close a session. For example, as an added measure of security, you could create a macro that sends the Winkey-L combination, which would cause the remote device’s log in page to come up the next time the device was accessed. To create the macro, do the following:

1. Select System Macros, then click Add.

2. In the dialog box that comes up, replace the “NewMacro” text with a name of your choice for the macro:
3. Click **Record**.
   The dialog box disappears, and a small panel appears at the top left of the screen:

```
Pause  Done  Cancel  Show
```

4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Record** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 88).

**Note:**
1. Case is not considered – typing `A` or `a` has the same effect.
2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is `A` the alternate Chinese character obtained via keyboard switching is not recorded.

5. If you haven’t brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with your system macro key presses displayed in the Macro column:

![Macro dialog box](image)

6. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.
7. Repeat the procedure for any other macros you wish to create.

Once the system macros have been created, you can choose to run any one of them upon logging out of the CN8000A. System macros will only execute when the last user has logged out of the viewer (see Exit Macro, page 76, for details).

Note: 1. Information about the Search function is given on page 91.

2. Systems macros are stored on the CN8000A, therefore macro names may not exceed 64 Bytes (1 Byte = 1 English alphanumeric character), and hotkey combinations may not exceed 256 Bytes (each key usually takes 3–5 Bytes).
The Video Settings dialog box allows you to adjust the placement and picture quality of the remote screen display on your monitor. Click Advanced to view all the video settings.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Position</td>
<td>Adjust the horizontal and vertical position of the remote computer window by clicking the Arrow buttons.</td>
</tr>
</tbody>
</table>
| Auto Sync       | Click Auto Sync to have the vertical and horizontal offset values of the remote screen detected and automatically synchronized with the local screen.  
Note: 1. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync.  
2. This function works best with a bright screen.  
3. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually. |
6. The WinClient Viewer

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGB</td>
<td>Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When an RGB value is increased, the RGB component of the image is correspondingly increased. If you enable Set to Grayscale, the remote video display is changed to grayscale.</td>
</tr>
<tr>
<td>Gamma</td>
<td>This section allows you to adjust the video display's gamma level. This function is discussed in detail in the next section, Gamma Adjustment.</td>
</tr>
<tr>
<td>Performance</td>
<td>Select the type of Internet connection that exists between the Local Client computer and the CN8000A. The CN8000A will use that selection to automatically adjust the Video Quality and Detect Tolerance settings to optimize the quality of the video display. Since network conditions vary, if none of the pre-set choices seem to work well, you can select Customize and use the Video Quality and Detect Tolerance slider bars to adjust the settings to suit your conditions.</td>
</tr>
<tr>
<td>Video Quality</td>
<td>Drag the slider bar to adjust the overall Video Quality. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely affect response time.</td>
</tr>
</tbody>
</table>
| Enable Refresh  | The CN8000A can redraw the screen every 1 to 99 seconds, eliminating unwanted artifacts from the screen. Select Enable Refresh and enter a number from 1 through 99. The CN8000A will redraw the screen at the interval you specify. This feature is disabled by default. Click to put a check mark in the box next to Enable Refresh to enable this feature. **Note:**  
  1. The switch starts counting the time interval when mouse movement stops.  
  2. Enabling this feature increases the volume of video data transmitted over the network. The lower the number specified, the more often the video data is transmitted. Setting too low a value may adversely affect overall operating responsiveness. |
| Color Depth Control | This setting determines the richness of the video display by adjusting the amount of color information. |
| Tolerance       | This setting also relates to video quality. It governs detecting or ignoring pixel changes. A high setting can result in a lower quality display due to less data transfer. A lower setting will result in better video quality, but setting the threshold too low may allow too much data to be transferred, negatively impacting network performance. |
**Gamma Adjustment**

If it is necessary to correct the gamma level for the remote video display, use the *Gamma* function of the Video Adjustment dialog box.

- For greater control, clicking the *Advanced* button brings up the following dialog box:

  ![Gamma Adjustment Dialog Box](image)

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

**Note:** For best results, change the gamma while viewing a remote computer.
The Message Board
To alleviate the possibility of access conflicts resulting from multiple user logins, the CN8000A provides a message board that allows users to communicate with each other:

![Message Board](image)

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable Chat</td>
<td>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 the user has disabled Chat.</td>
</tr>
<tr>
<td>Occupy/Release Keyboard/Video/Mouse</td>
<td>When a port is set to Occupy mode (see page 73), you can use this button to occupy the KVM. 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 the user has occupied the KVM.</td>
</tr>
<tr>
<td>Occupy/Release Keyboard/Mouse</td>
<td>When a port is set to Occupy mode (see page 73), you can use this button to occupy the KM. 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 the user has occupied the KM.</td>
</tr>
<tr>
<td>Show/Hide User List</td>
<td>User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.</td>
</tr>
</tbody>
</table>
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.

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.

User List Panel
The names of all the logged in users are listed in this panel.
- Your name appears in blue; other users' names appear in black.
- By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- If a user's name is selected, and you want to post a message to all users, select All Users 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.
6. The WinClient Viewer

Virtual Media

The Virtual Media feature allows a drive, folder, image file, or removable disk on a local client computer to appear and act as if it were installed on the remote server. Virtual Media also supports a smart card reader function that allows a reader plugged into a local client computer to appear as if it were plugged into the remote server.

Virtual Media Icons

The Virtual Media icon on the WinClient Control Panel changes, to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>The icon displays in blue to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>The icon displays in blue with a / to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.</td>
</tr>
</tbody>
</table>

Virtual Media Redirection

To implement the virtual media redirection feature, do the following:

1. Click the Virtual Media icon to bring up the Virtual Media dialog box:

   ![Virtual Media Dialog Box](image)

   2. Click **Add**; then select the media source.
Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 187 for details about mounting these media types.

3. To add additional media sources, click **Add**, and select up to three media sources.

   Up to three virtual media choices can be mounted. The top three in the list are the ones that are selected. To rearrange the selection order, highlight the device you want to move, then click the Up or Down Arrow button to promote or demote it in the list.

4. **Read** refers to the redirected device being able to send data to the remote server; **Write** refers to the redirected device being able to have data from the remote server written to it. The default is for Write to not be enabled (Read only). If you want the redirected device to be writable as well as readable, click to put a check in the **Enable Write** checkbox:

**Note:**

1. If a redirected device cannot be written to, or if a user does not have write permissions, it appears in gray and cannot be selected.

2. See *Virtual Media Support*, page 187, for a list of supported virtual media types.
3. To remove an entry from the list, select it and click **Remove**.

4. After you have made your media source selections, click **Mount**. The dialog box closes. The virtual media devices that you have selected are redirected to the remote system, where they show up as drives, files and folders on the remote file system.

![My Computer Window](image)

Once mounted, you can treat the virtual media as if they were really on the remote server – drag and drop files to/from them; open files on the remote system for editing and save them to the redirected media, etc.

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

5. To end the redirection, bring up the **Control Panel** and click on the Virtual Media icon. All mounted devices are automatically unmounted.
Smart Card Reader

The smart card reader function allows a reader plugged into a local client computer’s USB port to be redirected, and appear as if it were plugged into the remote server. One purpose of smart cards (Common Access Cards, for example), is to allow authentication to the remote server from the local client.

When a smart card reader is connected to the local client computer, an entry for it appears when you bring up the Virtual Media dialog box and click **Add**:

```
Make your selection; then click **Mount** to complete the redirection.
```

**Note:** If you mount a smart card reader, you cannot mount any other virtual media device. If any virtual media devices are already mounted, you must unmount them before you can mount the smart card reader.
6. The WinClient Viewer

**Zoom**

The Zoom icon controls the zoom factor for the remote view window. Settings are as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>Sizes and displays the remote view window at 100%.</td>
</tr>
<tr>
<td>75%</td>
<td>Sizes and displays the remote view window at 75%.</td>
</tr>
<tr>
<td>50%</td>
<td>Sizes and displays the remote view window at 50%.</td>
</tr>
<tr>
<td>25%</td>
<td>Sizes and displays the remote view window at 25%.</td>
</tr>
<tr>
<td>1:1</td>
<td>Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don’t resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.</td>
</tr>
</tbody>
</table>
The On-Screen Keyboard

The CN8000A supports an on-screen keyboard, available with a PC or Sun layout and in multiple languages, with all the standard keys for each supported language. Click this icon to pop up the on-screen keyboard:

One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems aren’t the same, you don’t have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer on the port he is accessing; and use the on-screen keyboard to communicate with it.

Click the drop-down menu to select a PC or SUN keyboard layout.

Note: You must use your mouse to click on the keys. You cannot use your actual keyboard.

To change languages, do the following:

1. Click the down arrow next to the currently selected language to drop-down the language list.

2. Select the new language from the list.
To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.
Mouse Pointer Type

The CN8000A offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:

![Mouse Pointer Type Icon]

Note: The icon on the Control Panel changes to match your choice.

Mouse DynaSync Mode

Clicking this icon selects whether synchronization of the local and remote mouse pointers is accomplished either automatically or manually.

Automatic Mouse Synchronization (DynaSync)

*Mouse DynaSync* provides automatic locked-in synching of the remote and local mouse pointers – eliminating the need to constantly resync the two movements.

The icon on the toolbar indicates the synchronization mode status as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon Available Enabled]</td>
<td>This icon indicates that Mouse DynaSync is available and is <strong>enabled</strong>. This is the default setting when Mouse DynaSync is available.</td>
</tr>
<tr>
<td>![Icon Available Not Enabled]</td>
<td>The / over this icon indicates that Mouse DynaSync is available but is <strong>not enabled</strong>.</td>
</tr>
</tbody>
</table>

When *Mouse DynaSync* is available, clicking the icon toggles its status between enabled and /disabled. If you choose to disable Mouse DynaSync mode, you must use the manual synching procedures described in the next section.
Mac Considerations

- For Mac systems, there is a second DynaSync setting to choose from. If the default synchronization result is not satisfactory, you can try the **Automatic For Mac 2** setting. To select Mac 2, right click in the text area of the Control Panel and select *Mouse Sync Mode → Automatic for Mac 2*:

![Mouse Sync Mode Settings]

Manual Mouse Synchronization

If you are using Manual mouse synchronization instead of automatic DynaSync and the local mouse pointer goes out of sync with the remote system's mouse pointer, there are a number of methods to bring them back into sync:

1. Perform a video and mouse auto sync by clicking the *Video Settings* icon on the Control Panel (see page 94).
2. Perform an *Auto Sync* with the Video Adjustment function (see *Video Settings*, page 94, for details).
3. Invoke the *Adjust Mouse* function with the *Adjust Mouse* hotkeys (see *Adjust Mouse*, page 86, for details).
4. Move the pointer into all 4 corners of the screen (in any order).
5. Drag the Control Panel to a different position on the screen.
6. Set the mouse speed and acceleration for each problematic computer attached to the switch. See *Additional Mouse Synchronization Procedures*, page 185, for instructions.
## Customize Control Panel

Clicking the *Customize Control Panel* icon brings up a dialog box that allows you to configure the items that appear on the Control Panel, as well as its graphical settings:

The dialog box is organized into six main sections as described in the table, below:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize Control Panel</td>
<td>Allows you to select which icons display in the Control Panel</td>
</tr>
</tbody>
</table>
| Control Panel Style   | - Enabling *Transparent* makes the Control Panel semi-transparent, so that you can see through it to the display underneath.  
                         - Enabling *Icon* causes the Control Panel to disappear and display as an icon (shown left) on the screen until you mouse over it. When you mouse over the icon, the full panel comes up. This function only works when the Control Panel is dragged out of its default position (top center or bottom center of the screen). |
### Screen Options

- If **Full Screen Mode** is enabled, the remote display fills the entire screen.
- If **Full Screen Mode** is not enabled, the remote display appears as a window on the local desktop. If the remote screen is larger than what is able to fit in the window, scrollbars will appear.
- If **Keep Screen Size** is enabled, the remote screen is not resized.
  - If the remote resolution is smaller than that of the local monitor, its display appears like a window centered on the screen.
  - If the remote resolution is larger than that of the local monitor, its display is scaled to the local size.
- If **Keep Screen Size** is not enabled, the remote screen is resized to fit the local monitor's resolution.

### User Info

- If **Show User Numbers** is enabled, the total number of users logged into the CN8000A displays in the text row of the Control Panel (See the Control Panel diagram on page 81 for an example.)

### Snapshot

These settings let the user configure the CN8000A's screen capture parameters (see the **Snapshot** description under Control Panel Functions, page 82):

- **Path** lets you select a directory that the captured screens automatically get saved to. Click **Browse**; navigate to the directory of your choice; then click **OK**. If you don't specify a directory here, the snapshot is saved to your desktop.
- Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file.
- If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.

### Keyboard Pass Through

- When this is enabled, the Alt-Tab key press is passed to the remote server and affects that server. If it is not enabled, Alt-Tab acts on your local client computer.
Power Management

Clicking the Power Management icon brings up the power manager window, allowing you to log in and configure devices connected to a PN0108 Power Over the NET™ device:

For information on configuring Power Over the NET™ devices, see the PN0108’s user manual.
Admin Utility
Clicking the Admin Utility icon brings up a window that allows you to configure the CN8000A via Viewer based GUI with the web browser administrative functionalities:

The sidebar menu items available on this page are based upon the user’s permissions. For information on how to use these functions, See Administration, page 33, for details.
Chapter 7  The JavaClient Viewer

Introduction

The JavaClient Viewer makes the CN8000A accessible to all platforms that have the Java Runtime Environment (JRE) installed. (See System Requirements, page 6, for the required JRE version.) The JRE is available for free download from the Java web site (http://java.com).

To run the JavaClient Viewer, after you log in (see Logging In, page 27), Click the Viewer link on the lower Sidebar panel, shown below.

![Sidebar panel with Viewer link]

**Note:** For the JavaClient Viewer to launch it must be set as the default viewer. See User Preferences, page 74, for details.
A second or two after you click the Viewer 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.
- 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 JavaClient control panel is hidden at the top center of the screen. It becomes visible when you move the mouse pointer into that area:

Note: 1. The above image shows the complete Control Panel. The icons that appear can be customized. See Control Panel Configuration, page 125, for details.
2. To place the control panel anywhere on the screen, move the mouse pointer over the text bar area and drag the panel to the new position.

- By default, the text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, information will be displayed that describes the icon's function.
- If the Show User Numbers function has been enabled under Control Panel Configuration (see User Info, page 109), the total number of users currently logged into the CN8000A displays next to the text row on the right.
- Right clicking in the text row area brings up a menu that allows you to select and use the Control Panel options. All Control Panel functions are discussed in the sections that follow.
### Control Panel Functions

The Control Panel functions are described in the table below:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Toggle Icon" /></td>
<td>This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.</td>
</tr>
<tr>
<td><img src="image2" alt="Expand Icon" /></td>
<td>When you click this icon, the Control Panel collapses into 4 categories: Keyboard/Mouse, Video, Macro and Advanced. Hover your mouse over the categories to see the submenu list. Click the icon again to revert to the original Control Panel format.</td>
</tr>
<tr>
<td><img src="image3" alt="Macro Icon" /></td>
<td>Click to bring up the Macros dialog box (see Macros, page 118 for details).</td>
</tr>
<tr>
<td><img src="image4" alt="Video Settings Icon" /></td>
<td>Click to bring up the Video settings dialog box. Right-click to perform a quick Auto Sync (see Video Settings, page 120, for details).</td>
</tr>
<tr>
<td><img src="image5" alt="Auto Sync Icon" /></td>
<td>Click to perform a video and mouse autosync operation. It is the same as clicking the Auto-sync button in the Video Options dialog box (see Video Settings, page 120).</td>
</tr>
<tr>
<td><img src="image6" alt="Mode Icon" /></td>
<td>Toggles the display between Full Screen Mode and Windowed Mode.</td>
</tr>
<tr>
<td><img src="image7" alt="Snapshot Icon" /></td>
<td>Click to take a snapshot (screen capture) of the remote display. See Snapshot, page 109, for details on configuring the Snapshot parameters.</td>
</tr>
<tr>
<td><img src="image8" alt="Message Board Icon" /></td>
<td>Click to bring up the Message board (see page 121).</td>
</tr>
<tr>
<td><img src="image9" alt="Ctrl+Alt+Del Icon" /></td>
<td>Click to send a Ctrl+Alt+Del signal to the remote system.</td>
</tr>
<tr>
<td><img src="image10" alt="Virtual Media Icon" /></td>
<td>Click to toggle the remote display between grayscale and color.</td>
</tr>
<tr>
<td><img src="image11" alt="Virtual Media Icon" /></td>
<td>Click to bring up the Virtual Media dialog box. The / over the icon will indicate that a media device has been mounted. The icon changes back when the virtual media icon is clicked again and the device is unmounted. See Virtual Media, page 123, for specific details.</td>
</tr>
</tbody>
</table>
7. The JavaClient Viewer

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
</table>
| ![icon] | Click to zoom the remote display window.  
  **Note:** This feature is only available in windowed mode (Full Screen Mode is off). See Zoom, page 123, for details. |
| ![icon] | Click to bring up the on-screen keyboard (see The On-Screen Keyboard, page 124). |
| ![icon] | Click to select the mouse pointer type.  
  **Note:** This icon changes depending on which mouse pointer type is selected (see Mouse Pointer Type, page 124). |
| ![icon] | Click to toggle Automatic or Manual mouse sync.  
  - When the selection is **Automatic**, the icon to the right appears.  
  - When the selection is **Manual**, a / appears over the icon.  
  (See Mouse DynaSync Mode, page 106 for a complete explanation of this feature.) |
| ![icon] | Click to display a drop-down list of **User** macros. Access and run macros more conveniently rather than using the Macros dialog box (see the Macros icon in the table above, and the Macros section on page 118). |
| ![icon] | Click this icon to open a Viewer based GUI with the web browsers administrative functionalities. |
| ![icon] | Click to bring up the Control Panel Configuration dialog box.  
  See Control Panel Configuration, page 125, for details on configuring the Control Panel. |
| ![icon] | 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.
Macros

The Macros icon provides access to three functions found in the Macros dialog box: Hotkeys, User Macros, and System Macros. Each of these functions is described in the following sections.

Hotkeys

Various actions related to manipulating the remote server can be accomplished with hotkeys. Selecting the Hotkeys radio button lets you configure which hotkeys perform the actions.

Hotkey operation is the same under the JavaClient as it is under the WinClient. See Hotkeys, page 85, for details.

Note: Toggle Mouse Display is not available in the JavaViewer version.
User Macros
User Macros are used to perform specific actions on the remote server. To create the macro, do the following:

1. Select the User Macros radio button, then click Add.

User Macro operation is the same under the JavaClient as it is under the WinClient. See User Macros, page 87, for details.

System Macros
System Macros are used to create exit macros for when you close a session. For example, as an added measure of security, you could create a macro that sends the Winkey-L combination which would cause the remote device’s login page to come up the next time the device was accessed. To create the macro, do the following:

1. Select System Macros, then click Add.

System Macro operation is the same under the JavaClient as it is under the WinClient. See System Macros, page 91, for details.
Search
Search allows you to find previously created macros and have them listed in the large upper panel for you to play or edit.

The Search operation is the same under the JavaClient as it is under the WinClient. See Search, page 91, for details.

Video Settings
The Video settings dialog box allows you to adjust the placement and picture quality of the remote screen display on your monitor.

Video Settings operation is the same under the JavaClient as it is under the WinClient. See Video Settings, page 94, for details.
Message Board

The CN8000A 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:

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
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.
- If another user sends a message to the message board and your message board is not open, a window showing the message pops up on your screen.
Virtual Media

The Virtual Media feature allows a folder or image file on a local client computer to appear and act as if it were installed on the remote server. Virtual Media also supports a smart card reader function that allows a reader plugged into a local client computer to appear as if it were plugged into the remote server.

To implement this redirection feature, do the following:

1. Click the Virtual Media icon to bring up the Virtual Media dialog box:

Virtual Media operation is the same under the JavaClient as it is under the WinClient. See Virtual Media, page 99, for details.

Note: Only the ISO File and Folder virtual media functions are supported with the Java Viewer.

Zoom

The Zoom icon controls the zoom factor for the remote view window. Settings are as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>Sizes and displays the remote view window at 100%.</td>
</tr>
<tr>
<td>75%</td>
<td>Sizes and displays the remote view window at 75%.</td>
</tr>
<tr>
<td>50%</td>
<td>Sizes and displays the remote view window at 50%.</td>
</tr>
<tr>
<td>25%</td>
<td>Sizes and displays the remote view window at 25%.</td>
</tr>
<tr>
<td>1:1</td>
<td>Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don’t resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.</td>
</tr>
</tbody>
</table>
The CN8000A supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language. Click this icon to pop up the on-screen keyboard:

On-Screen Keyboard operation is the same under the JavaClient as it is under the WinClient. See The On-Screen Keyboard, page 104, for details.

Mouse Pointer Type

The CN8000A offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:

Note: The icon on the Control Panel changes to match your choice.
7. The JavaClient Viewer

**Mouse DynaSync Mode**
Clicking this icon selects whether synchronization of the local and remote mouse pointers is accomplished either automatically or manually. DynaSync operation is the same under the JavaClient as it is under the WinClient. See *Mouse DynaSync Mode*, page 106, for details.

**Control Panel Configuration**
Clicking the Control Panel icon brings up a dialog box that allows you to configure the items that appear on the Control Panel, as well as its graphical settings:

![Control Panel Configuration](image)

Control Panel Configuration is almost the same under the JavaClient as it is under the WinClient. See *Customize Control Panel*, page 108, for details.

**Note:** The following functions found with the WinClient are not available with the JavaClient: the Transparent control panel style; and Screen Options. In addition, the BMP graphics format (in the Snapshot section), has been replaced by PNG.
Chapter 8
The Log Server

The Log Server is a Windows-based administrative utility that records all the events that take place on selected CN8000A units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. With Windows running, put the CN8000A software CD that came with this product into the CD (DVD) drive.
2. Navigate to the Log Server AP Installer folder on the CD.
3. Click the Log Server icon to execute LogServerSetup.exe and start the installation.
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:

![Log Server Main Screen](image)

**Note:**
1. The MAC address of the Log Server computer must be specified in the ANMS - Event Destination settings – see Log Server, page 49 for details.
2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server program does not run.*, page 184 if the program doesn’t start.

The screen is divided into three components:

- A **Menu Bar** at the top
- A panel that will contain a list of CN8000A units in the middle (see *The Log Server Main Screen*, page 133, for details).
- A panel that will contain an **Events List** at the bottom

Each of the components is explained in the sections that follow.
8. The Log Server

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 CN8000A List window to enable it.

**Configure**

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new CN8000A units to the CN8000A List, edit the information for units already on the list, or delete CN8000A units from the list.

- To add a CN8000A to the CN8000A List, click **Add**.
- To edit or delete a listed CN8000A, first select the one you want in the CN8000A 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:

![Add a Server Dialog Box](image-url)

Address: [Server Address]  Port: [5000]
Description: [Server Description]
Limit: [100] Days

[OK] [Cancel]
A description of the fields is given in the table, below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>This can either be the IP address of the CN8000A or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the CN8000A in the ANMS settings (see ANMS - Event Destination, page 48).</td>
</tr>
<tr>
<td>Port</td>
<td>Key in the port number that was specified for the Log Server’s Service Port in the ANMS settings (see Log Server, page 49).</td>
</tr>
<tr>
<td>Description</td>
<td>This field is provided so that you can put in a descriptive reference for the unit to help identify it.</td>
</tr>
<tr>
<td>Limit</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>New search</td>
<td>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 CN8000A.</td>
</tr>
<tr>
<td>Search last results</td>
<td>This is a secondary search performed on the events that resulted from the last search.</td>
</tr>
<tr>
<td>Search excluding last results</td>
<td>This is a secondary search performed on all the events in the database for the selected CN8000A excluding the events that resulted from the last search.</td>
</tr>
<tr>
<td>Server List</td>
<td>CN8000A 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.</td>
</tr>
<tr>
<td>Priority List</td>
<td>Sets the level for how detailed the search results display should be. Least is the most general; Most is the most specific. Least results appear in black; Less results appear in blue; Most results appear in red.</td>
</tr>
<tr>
<td>Start Date</td>
<td>Select the date that you want the search to start from. The format follows the YYYY/MM/DD convention, as follows: 2009/11/04</td>
</tr>
<tr>
<td>Start Time</td>
<td>Select the time that you want the search to start from.</td>
</tr>
<tr>
<td>End Date</td>
<td>Select the date that you want the search to end at.</td>
</tr>
<tr>
<td>End Time</td>
<td>Select the time that you want the search to end at.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Key in the pattern that you are searching for here. The multiple character wildcard (<em>) is supported. E.g., h</em>ds would match hands and hoods.</td>
</tr>
<tr>
<td>Results</td>
<td>Lists the events that contained matches for the search.</td>
</tr>
<tr>
<td>Search</td>
<td>Click this button to start the search.</td>
</tr>
<tr>
<td>Print</td>
<td>Click this button to print the search results.</td>
</tr>
<tr>
<td>Export</td>
<td>Click this button to write the search results to a .txt file.</td>
</tr>
<tr>
<td>Exit</td>
<td>Click this button to exit the Search dialog box.</td>
</tr>
</tbody>
</table>

**Maintenance**

This function allows the administrator to perform manual maintenance of the database if the CN8000A misses the automatic maintenance.
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:

![Retry dialog box]

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 CN8000A units that have been selected for the Log Server to track (see Configure, page 129).
- The lower (Event) panel displays the log events for the currently selected CN8000A (the highlighted one - if there are more than one). To select a CN8000A unit in the list, simply click on it.
The List Panel

The List panel contains six fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording</td>
<td>Determines whether the Log Server records log events for this CN8000A 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. <strong>Note:</strong> Even though a CN8000A is not the currently selected one, if its Recording check box is checked, the Log Server will still record its log events.</td>
</tr>
<tr>
<td>Address</td>
<td>This is the IP Address or DNS name that was given to the CN8000A when it was added to the Log Server (see Configure, page 129).</td>
</tr>
<tr>
<td>Port</td>
<td>This is the port number that was assigned to the CN8000A when it was added to the Log Server (see Configure, page 129).</td>
</tr>
<tr>
<td>Connection</td>
<td>If the Log Server is connected to the CN8000A, 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 - Event Destination settings (see page 48) and specified in the Configure dialog box (see Configure, page 129).</td>
</tr>
<tr>
<td>Days</td>
<td>This field displays the number of days that the CN8000A's log events are to be kept in the Log Server's database before expiration (see Configure, page 129).</td>
</tr>
<tr>
<td>Description</td>
<td>This field displays the descriptive information given for the CN8000A when it was added to the Log Server (see Configure, page 129).</td>
</tr>
</tbody>
</table>

The Tick Panel

The lower panel displays tick information for the currently selected CN8000A. 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

LDAP Server Configuration

Introduction

The CN8000A allows log in authentication and authorization through external programs. This chapter describes how to configure Active Directory and OpenLDAP for CN8000A authentication and authorization.

To allow authentication and authorization for the CN8000A via LDAP or LDAPS, the Active Directory’s LDAP Schema must be extended so that an extended attribute name for the CN8000A – 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:

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, you must do the following 3 procedures: 1) create a new attribute; 2) extend the object class with the new attribute; and 3) edit the Active Directory users with the extended schema.

The CN8000A supports two types of Active Directory users: The first supports both authentication and authorization parameter settings on the LDAP server; the second supports shadow user access rights – where authentication takes place on the LDAP server, but authorization is via the CN8000A’s user database.

Editing Active Directory users with the Type 1 schema is described on page 141; editing Active Directory users with the Type 2 schema is described on page 147.

Creating a New Attribute
To create a new attribute do the following:


2. In the left panel of the screen that comes up, right-click Attributes:


4. In the warning message that appears, click Continue to bring up the Create New Attribute dialog box.
5. 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.

---

**Extending the Object Class With the New Attribute**

To extend the object class with the new attribute, do the following:

2. In the left panel of the screen that comes up, select **Classes**.
3. In the right panel, right-click **person**.
9. LDAP Server Configuration
4. Select Properties; the person Properties dialog box comes up with the General page displayed. Click the Attributes tab.

5. On the Attributes page, click Add.
6. In the list that comes up, select permission, then click OK to complete step 2 of the procedure.

![Select Schema Object](image)

**Editing Active Directory Users**

**Type 1**

For Type 1 users, both authentication and authorization parameter settings are supported on the LDAP server. To edit a Type 1 Active Directory user do the following:

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

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

5. On the Attribute Editor page of the dialog box that appears, select permission from the list.
6. Click **Edit** to bring up the *String Attribute Editor*.

7. Key in the desired CN8000A permission attribute values (see *The Permission Attribute Value*, page 145 for details). For example:
8. Click **OK**. When you return to the *Attribute Editor* page, the *permission* entry now reflects the new permissions:

![Attribute Editor](image)

- a) Click **Apply** to save the change and complete the procedure.
- b) Repeat the *Editing Active Directory Users* procedure for any other Type 1 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 CN8000A a user will access; and 2) a string that indicates the access rights the user has on the CN8000A 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 CN8000A’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 CN8000A, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Grants the user administrator privileges, allowing the user to configure the system.</td>
</tr>
<tr>
<td>W</td>
<td>Allows the user to access the system via the Windows Client program.</td>
</tr>
<tr>
<td>J</td>
<td>Allows the user to access the system via the Java applet.</td>
</tr>
<tr>
<td>P</td>
<td>Allows the user to Power On/Off, Reset devices via an attached PN0108.</td>
</tr>
<tr>
<td>L</td>
<td>Allows the user to access log in formation via the user's browser.</td>
</tr>
<tr>
<td>V</td>
<td>Limits the user's access to only viewing the video display.</td>
</tr>
<tr>
<td>S</td>
<td>Allows the user to use the Virtual Media function – Read Only.</td>
</tr>
<tr>
<td>M</td>
<td>Allows the user to use the Virtual Media function – Read/Write.</td>
</tr>
<tr>
<td>T</td>
<td>Allows the user to access the system via Telnet.</td>
</tr>
<tr>
<td>H</td>
<td>Allows the user to access the system via SSH.</td>
</tr>
<tr>
<td>A</td>
<td>Allows the user to access the system via Telnet and SSH.</td>
</tr>
</tbody>
</table>
Permission Examples

Access rights examples are given in the table, below:

<table>
<thead>
<tr>
<th>User</th>
<th>String</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| User1  | 10.0.0.166&w,v                 | 1. User has *Windows Client* and *View Only* rights on a CN8000A with an IP address of 10.0.0.166.  
2. User has no rights on any other CN8000A units administered by the LDAP server. |
| User2  | 10.0.0.164&p,x;10.0.0.166&j,c  | 1. User has *PON* and *Virtual Media* rights on a CN8000A with an IP address of 10.0.0.164.  
2. User has *Java Applet* and *Administrator* rights on a CN8000A with an IP address of 10.0.0.166.  
3. User has no rights on any other CN8000A units administered by the LDAP server. |
| User3  | v;j;10.0.0.164&p,j             | 1. User has *View Only* and *Log Information* rights on all CN8000A 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 CN8000A with an IP address of 10.0.0.164. |
| User4  |                                | User has no access rights to any CN8000A units administered by the LDAP server.                                                                                                                       |
| User5  | v,w                            | User has *View Only* and *Windows Client* rights on all CN8000A 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 CN8000A 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 CN8000A with an IP address of 10.0.0.166.  
3. User has *Administrator* and *Java Applet* rights on the CN8000A with an IP address of 10.0.0.164. |
Type 2
For Type 2 users, authentication takes place on the LDAP server, but authorization is via the CN8000A’s user database. To edit a Type 2 user, do the following:

1. Follow Steps 1 – 6 of Editing a Type 1 user (beginning on page 141)
2. In the String Attribute Editor, key in the values shown in the screenshot, below:

![String Attribute Editor Screenshot](image)

**Note:** Where *user* represents the Username of a CN8000A user whose permissions reflect the permissions you want Jason to have.

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

![Attribute Editor Screenshot](image)
c) Click **Apply** to save the change and complete the procedure. Jason now has the same permissions as user.

d) Repeat the **Editing Active Directory Users** procedure for any other users you wish to add.

---

**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:

```plaintext
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:

![Screenshot of OpenLDAP console](image)

**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 CN8000A, the CN8000A 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 CN8000A is shown in the figure, below:
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 CN8000A is shown in the figure, below:

(Continues on next 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 CN8000A directory tree (shown in the figure, above).

Note: The example above shows the permissions for a Type 1 Schema. For a Type 2 Schema, change the permissions line to su/user. (Where user represents the Username of a CN8000A user whose permissions reflect the permissions you want steve to have.)
The following figure illustrates an LDIF file that defines the OpenLDAP group for the CN8000A.

(Continues on next page.)
Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., cn8000a.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

• This product is for indoor use only.
• 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.

- Avoid circuit overloads. Before connecting equipment to a circuit, know the power supply’s limit and never exceed it. Always review the electrical specifications of a circuit to ensure that you are not creating a dangerous condition or that one doesn’t already exist. Circuit overloads can cause a fire and destroy equipment.
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.
Consignes de sécurité

Général

- Ce produit est destiné exclusivement à une utilisation à l’intérieur.
- Veuillez lire la totalité de ces instructions. Conservez-les afin de pouvoir vous y référer ultérieurement.
- Respectez l’ensemble des avertissements et instructions inscrits sur l’appareil.
- Ne placez jamais l’unité sur une surface instable (chariot, pied, table, etc.). Si l’unité venait à tomber, elle serait gravement endommagée.
- N’utilisez pas l’unité à proximité de l’eau.
- Ne placez pas l’unité à proximité de ou sur des radiateurs ou bouches de chaleur.
- Le boîtier de l’unité est doté de fentes et d’ouvertures destinées à assurer une ventilation adéquate. Pour garantir un fonctionnement fiable et protéger l’unité contre les surchauffes, ces ouvertures ne doivent jamais être bloquées ou couvertes.
- L’unité ne doit jamais être placée sur une surface molle (lit, canapé, tapis, etc.) car ses ouvertures de ventilation se trouveraient bloquées. De même, l’unité ne doit pas être placée dans un meuble fermé à moins qu’une ventilation adaptée ne soit assurée.
- Ne renversez jamais de liquides de quelque sorte que ce soit sur l’unité.
- Débranchez l’unité de la prise murale avant de la nettoyer. N’utilisez pas de produits de nettoyage liquide ou sous forme d’aérosol. Utilisez un chiffon humide pour le nettoyage de l’unité.
- L’appareil doit être alimenté par le type de source indiqué sur l’étiquette. Si vous n’êtes pas sûr du type d’alimentation disponible, consultez votre revendeur ou le fournisseur local d’électricité.
- Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.
- L’unité est équipée d’une fiche de terre à trois fils. Il s’agit d’une fonction de sécurité. Si vous ne parvenez pas à insérer la fiche dans la prise murale, contactez votre électricité afin qu’il remplace cette dernière qui doit être obsolète. N’essayez pas d’aller à l’encontre de l’objectif de la fiche de terre. Respectez toujours les codes de câblage en vigueur dans votre région/pays.
• L’équipement doit être installé à proximité de la prise murale et le dispositif de déconnexion (prise de courant femelle) doit être facile d’accès.

• La prise murale doit être installée à proximité de l’équipement et doit être facile d’accès.

• Veillez à ce que rien ne repose sur le cordon d’alimentation ou les câbles. Acheminez le cordon d’alimentation et les câbles de sorte que personne ne puisse marcher ou trébucher dessus.

• En cas d’utilisation d’une rallonge avec cette unité, assurez-vous que le total des ampérages de tous les produits utilisés sur cette rallonge ne dépasse pas l’ampérage nominal de cette dernière. Assurez-vous que le total des ampérages de tous les produits branchés sur la prise murale ne dépasse pas 15 ampères.

• Pour contribuer à protéger votre système contre les augmentations et diminutions soudaines et transitoires de puissance électrique, utilisez un parasurtenseur, un filtre de ligne ou un système d’alimentation sans coupure (UPS).

• Placez les câbles du système et les câbles d’alimentation avec précaution ; veillez à ce que rien ne repose sur aucun des câbles.

• Lors du branchement ou du débranchement à des blocs d’alimentation permettant la connexion à chaud, veuillez respecter les lignes directrices suivantes:
  • Installez le bloc d’alimentation avant de brancher le câble d’alimentation à celui-ci.
  • Débranchez le câble d’alimentation avant de retirer le bloc d'alimentation.
  • Si le système présente plusieurs sources d’alimentation, déconnectez le système de l'alimentation en débranchant tous les câbles d'alimentation des blocs d'alimentation.

• N’insérez jamais d’objets de quelque sorte que ce soit dans ou à travers les fentes du boîtier. Ils pourraient entrer en contact avec des points de tension dangereuse ou court-circuiter des pièces, entraînant ainsi un risque d’incendie ou de choc électrique.

• N’essayez pas de réparer l’unité vous-même. Confiez toute opération de réparation à du personnel qualifié.

• Si les conditions suivantes se produisent, débranchez l’unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
  • Le cordon d’alimentation ou la fiche ont été endommagés ou éraillés.
  • Du liquide a été renversé dans l’unité.
• L’unité a été exposée à la pluie ou à l’eau.
• L’unité est tombée ou le boîtier a été endommagé.
• Les performances de l’unité sont visiblement altérées, ce qui indique la nécessité d’une réparation.
• L’unité ne fonctionne pas normalement bien que les instructions d’utilisation soient respectées.

• N’utilisez que les commandes qui sont abordées dans le mode d’emploi. Le réglage incorrect d’autres commandes peut être à l’origine de dommages qui nécessiteront beaucoup de travail pour qu’un technicien qualifié puisse réparer l’unité.

• Ne connectez pas le connecteur RJ-11 portant la marque « Sensor » (Capteur) à un réseau de télécommunication public.

• Evitez toute surcharge du circuit. Avant de connecter l’équipement à un circuit, vérifiez la limite de l’alimentation et ne la dépassez pas. Controlez toujours les caractéristiques électriques d’un circuit pour vous assurer de ne pas créer de situation dangereuse ou qu’il n’y en a pas déjà. Les surcharges du circuit peuvent provoquer un incendie et détruire l’équipement.
Montage sur bâti

- Avant de travailler sur le bâti, assurez-vous que les stabilisateurs sont bien fixées sur le bâti, qu’ils sont étendus au sol et que tout le poids du bâti repose sur le sol. Installez les stabilisateurs avant et latéraux sur un même bâti ou bien les stabilisateurs avant si plusieurs bâtis sont réunis, avant de travailler sur le bâti.

- Chargez toujours le bâti de bas en haut et chargez l’élément le plus lourd en premier.

- Assurez-vous que le bâti est à niveau et qu’il est stable avant de sortir une unité du bâti.

- Agissez avec précaution lorsque vous appuyez sur les loquets de libération du rail d’unité et lorsque vous faites coulisser une unité dans et hors d’un bâti ; vous pourriez vous pincer les doigts dans les rails.

- Une fois qu’une unité a été insérée dans le bâti, étendez avec précaution le rail dans une position de verrouillage puis faites glisser l’unité dans le bâti.

- Ne surchargez pas le circuit de l’alimentation CA qui alimente le bâti. La charge totale du bâti ne doit pas dépasser 80 % de la capacité du circuit.

- Assurez-vous que tous les équipements utilisés sur le bâti, y-compris les multiprises et autres connecteurs électriques, sont correctement mis à la terre.

- Assurez-vous que les unités présentes dans le bâti bénéficient d’une circulation d’air suffisante.

- Assurez-vous que la température ambiante de fonctionnement de l’environnement du bâti ne dépasse pas la température ambiante maximale spécifiée pour l’équipement par le fabricant.

- Ne marchez sur aucun appareil lors de la maintenance d’autres appareils d’un bâti.
Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: http://eservice.aten.com
- For telephone support, see Telephone Support, page iii.

North America

<table>
<thead>
<tr>
<th>Email Support</th>
<th><a href="mailto:support@aten-usa.com">support@aten-usa.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Technical Support</td>
<td>Troubleshooting Documentation Software Updates</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>1-888-999-ATEN ext 4988</td>
</tr>
</tbody>
</table>

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 CN8000A in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your client computer must be on the same network segment as the CN8000A. After you have connected and logged in you can give the CN8000A its fixed network address. (See Network, page 43.)

First Time Browser Login

The easiest way to assign an IP address is when you login from a browser for the first time and use the Easy Installation Wizard. Refer to Logging In, page 27, (see step 5) for details on the procedure involved.

IP Installer

The IP Installer utility provides a simple method to ascertain and configure IP related settings for ATEN and Altusen network enabled devices.

The utility can be obtained from the Download area of our website. Look under Download - Driver & Software, and select the model of your switch. After downloading the utility to your client computer, do the following:

1. Unzip the contents of IPInstaller.zip to a directory on your hard drive.
2. Double click IPInstaller.exe, and the following screen appears:
Network Device IP Installer
The way that the IP Installer works is that it searches and lists all compatible ATEN devices on your network. You can select a model from the Device List and set its IP Address settings using the options listed below, then click Set IP to implement the change on the device.

Device List
When the IP Installer main window comes up, the utility scans the network for devices and lists the ones it finds in the device list panel. The device list panel consists of four columns, as shown in the following table:

<table>
<thead>
<tr>
<th>Heading</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Displays the device name assigned to the switch.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Displays the switches model name (CN8000A, PN9108, SN0116, etc.).</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the device's MAC address.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the device's current IP address.</td>
</tr>
</tbody>
</table>

Clicking Enumerate causes the utility to broadcast an Enumerate command and wait for replies from all the devices. It then refreshes the list based on the response it receives.

Protocol
Use this drop-down box to select the type of protocol IPv4 or IPv6, you are using for the network adapters on your LAN.

Network Adapter
The Network Adapter selection box, located just below the Device List, pertains to computers that have more than one network adapter installed. Users can use this to select the adapter that they want Enumerate to be directed to.

Set IP
There are two methods of specifying an IP address: Dynamic, and Static:
- If you want to obtain an IP address dynamically, select Obtain an IP address automatically (DHCP).
- If you want to use a static IP address, select Specify an IP address, then fill in the information for:
  - IPv4: IP Address, Subnet Mask, and Gateway.
  - IPv6: IPv6 Address, Subnet Prefix Length, and Default Gateway
After you have made your changes, click **Set IP** to set the IP address for the device you have selected.

**Note:** The screen will freeze for a moment or two until the utility has finished setting the IP.

### About
Clicking the **About** button brings up a dialog box with information about the product – including the current firmware version.

### Browser
1. Set your client 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 CN8000A.)
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 CN8000A that is suitable for the network segment that it resides on.
4. After you log out, reset your client computer's IP address to its original value.

### AP Windows Client
For computers running Windows, the CN8000A's IP address can be determined with the Windows AP program (see **Preferences**, page 30). When you run the program it searches the network segment for CN8000A 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, or clicking **Admin Utility**, and then clicking **Network** under the Advanced Settings menu. See **Network**, page 43, for details.
IPv6

At present, the CN8000A supports two IPv6 address protocols: Link Local IPv6 Address, and IPv6 Stateless Autoconfiguration.

**Link Local IPv6 Address**

At power on, the CN8000A is automatically configured with a Link Local IPv6 Address (for example, fe80::210:74ff:fe61:1ef). To find out what the Link Local IPv6 Address is, log in with the CN8000A’s IPv4 address and click the Basic Settings icon. The address is displayed at the bottom of the Basic Settings page (see page 34).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

http://[fe80::2001:74ff:fe6e:59%5]

for the URL bar.

If you are logging in with the AP program, you would key:

fe80::2001:74ff:fe6e:59%5

for the IP field of the Server panel (see The Windows Client Connection Screen, page 135).

**Note:**

1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the CN8000A.

2. The %5 is the %interface used by the client computer. To see your client computer’s IPv6 address: from the command line issue the following command: ipconfig /all. The % value appears at the end of the IPv6 address.
IPv6 Stateless Autoconfiguration

If the CN8000A’s network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the CN8000A can obtain its prefix information from that device in order to generate its IPv6 address. For example, 2001::74ff:fe6e:59.

As above, the address is displayed at the bottom of the Basic Settings page.

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

http://[2001::74ff:fe6e:59]

for the URL bar.

If you are logging in with the AP program, you would key:

2001::74ff:fe6e:59

for the IP field of the Server panel (see The Windows Client Connection Screen, page 135).
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 CN8000A 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.
# Keyboard Emulation

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

<table>
<thead>
<tr>
<th>PC Keyboard</th>
<th>Sun Keyboard</th>
<th>PC Keyboard</th>
<th>Mac Keyboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Ctrl] [T]</td>
<td>Stop</td>
<td>[Shift]</td>
<td>Shift</td>
</tr>
<tr>
<td>[Ctrl] [F2]</td>
<td>Again</td>
<td>[Ctrl]</td>
<td>Ctrl</td>
</tr>
<tr>
<td>[Ctrl] [F3]</td>
<td>Props</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [F4]</td>
<td>Undo</td>
<td>[Ctrl] [1]</td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [F5]</td>
<td>Front</td>
<td>[Ctrl] [2]</td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [F6]</td>
<td>Copy</td>
<td>[Ctrl] [3]</td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [F7]</td>
<td>Open</td>
<td>[Ctrl] [4]</td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [F8]</td>
<td>Paste</td>
<td>[Alt]</td>
<td>Alt</td>
</tr>
<tr>
<td>[Ctrl] [F9]</td>
<td>Find</td>
<td>[Print Screen]</td>
<td>F13</td>
</tr>
<tr>
<td>[Ctrl] [F10]</td>
<td>Cut</td>
<td>[Scroll Lock]</td>
<td>F14</td>
</tr>
<tr>
<td>[Ctrl] [1]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Ctrl] [2]</td>
<td></td>
<td>[Enter]</td>
<td>Return</td>
</tr>
<tr>
<td>[Ctrl] [3]</td>
<td></td>
<td>[Backspace]</td>
<td>Delete</td>
</tr>
<tr>
<td>[Ctrl] [4]</td>
<td></td>
<td>[Insert]</td>
<td>Help</td>
</tr>
<tr>
<td>[Ctrl] [H]</td>
<td>Help</td>
<td>[Ctrl] F15</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** When using key combinations, press and release the first key (Ctrl), then press and release the activation key.
PPP Modem Operation

Basic Setup
In addition to the browser and AP methods, the CN8000A 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:

   ![Diagram of hardware setup](image)

   2. From your computer, use your modem terminal program to dial into the CN8000A’s modem.

   **Note:**
   1. If you don’t know the CN8000A modem’s serial parameters, get them from the CN8000A 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 CN8000A 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-CN8000A-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 CN8000A (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 CN8000A.
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:

9. In the Security Alert dialog box, click View Certificate. The Certificate Information dialog box appears:

![Certificate Information Dialog Box]

**Note:** There is a red and white X logo over the certificate to indicate that it is not trusted.

10. Click Install Certificate.

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

12. When the Wizard presents a caution screen:

![Security Warning]

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

**Certificate Trusted**

The certificate is now trusted:

![Certificate Trusted](image)

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:

![Certificate Information](image)
Mismatch Considerations

If the site name or IP address used for generating the certificate no longer matches the current address of the CN8000A a mismatch warning occurs:

![Security Alert Image]

You can click Yes to go on, or you can disable mismatch checking.

To disable mismatch checking, do the following:

1. After the page you are logging in to comes up open the browser’s Tools menu; Select Internet Options → Advanced.

2. Scroll to the bottom of the list and uncheck Warn about trusted certificates:

![Internet Options Image]

3. Click OK. The next time you run the browser the change will be in effect.
Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at www.openssl.org. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted openssl.exe to.
2. Run openssl.exe with the following parameters:

```bash
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf
```

**Note:**
1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).
2. If there are spaces in the input, surround the entry in quotes (e.g., “ATEN International”).

To avoid having to input information during key generation the following additional parameters can be used:

```
/C /ST /L /O /OU /CN /emailAddress.
```

**Examples**

```bash
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf -subj /C=yourcountry/ST=yourstateorprovince/L=yourlocationor city/O=yourorganization/OU=yourorganizationalunit/CN=yourcommonname/emailAddress=name@yourcompany.com
```

```bash
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf -subj /C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN /CN=ATEN/emailAddress=eservice@aten.com.tw
```

**Importing the Files**

After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files that you upload in the Private Certificate panel of the Security page (see page 62).
# Troubleshooting

## General Operation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Erratic operation | The CN8000A needs to be started before the KVM switch.  
1. If the CN8000A 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 CN8000A, reset or restart the KVM switch.  
The CN8000A needs to be reset (see Firmware Upgrade/Reset Switch, page 11, point 1). |
| I can’t access the CN8000A, even though I have specified the IP address and port number correctly. | If the CN8000A is behind a router, the router’s Port Forwarding (also referred to as Virtual Server) feature must be configured. See Port Forwarding, page 170, 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 Mouse Display function to shrink the non-functioning pointer. See page 86 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 94) so that less video data is transmitted. |
| Changing Mouse Sync Mode to Manual makes the CN8000A crash. | The CN8000A hasn’t crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the CN8000A to get it going right away (see Firmware Upgrade/Reset Switch, page 11, 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 CN8000A to provide it. Therefore, only PON devices that don’t have their own over IP functionality (such as the PN0108) are supported. |
| When I am in a web browser session, and making configuration changes, and I am timed out, the settings changes I have made are lost. | If you don’t click Apply, the CN8000A isn’t aware that you are working, and times you out. Without clicking Apply, none of your changes are recognized. You must click Apply as you go along in order to have the settings saved on the CN8000A and reset the timeout counter. |
| 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. |
When the remote server is running Fedora the mouse pointer on the remote server does not move, whether I am accessing it from the local console or a local client computer.

If the remote server is connected with a PS/2 cable, log into the CN8000A with a browser; open a viewer; on the control panel set Mouse DynaSync to **Manual**. See page 106 for details.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the remote server is running Fedora the mouse pointer on the remote server does not move, whether I am accessing it from the local console or a local client computer.</td>
<td>If the remote server is connected with a PS/2 cable, log into the CN8000A with a browser; open a viewer; on the control panel set Mouse DynaSync to <strong>Manual</strong>. See page 106 for details.</td>
</tr>
</tbody>
</table>
## Windows

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| When I log in, the browser generates a CA Root certificate is not trusted, or a Certificate Error response. | 1. The certificate’s name is not found on Microsoft’s list of Trusted Authorities. The certificate can be trusted. See **Trusted Certificates**, page 174, for details.  
2. You can eliminate this message by importing a certificate issued by a recognized third party certificate authority (see **Obtaining a CA Signed SSL Server Certificate**, page 62). |
| After I import the site’s certificate, I still get a message warning me about the site when I log in. | Certificate security checking noticed a certificate address mismatch – however the certificate can be trusted. You can click **Continue to the website (not recommended)** to go on, or you can disable mismatch checking. See **Mismatch Considerations**, page 177 for a complete explanation of this topic. |
| Remote mouse pointer is out of step.                                   | 1. Check the status of the **Mouse DynaSync Mode** setting (see **Mouse DynaSync Mode**, page 106). 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 94), to sync the local and remote monitors.  
3. If that doesn't resolve the problem, use the **Adjust Mouse** feature (see **Adjust Mouse**, page 86) to bring the pointers back in step.  
4. If the above fails to resolve the problem, refer to **Additional Mouse Synchronization Procedures**, page 185, for further steps to take. |
| Part of remote window is off my monitor.                              | Use the **AutoSync** feature (see **Video Settings**, page 94), 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.                                                                                                               |
| Under Virtual Media, I can mount an ISO file, but I cannot access it.  | Virtual Media under the WindowsClient only supports ISO files less than 4G.Bytes. If the ISO file is 4GBytes or greater it cannot be accessed.                                                                                                                                 |
| My anti virus program reports that there is a Trojan after I access the CN8000A with my browser and then open the Windows Client Viewer. | The Windows Client Viewer uses an ActiveX plugin (windows.ocx) that some antivirus programs mistakenly see as a virus or trojan. We have tested our firmware extensively and found no evidence of a virus or trojan. You can add the plugin to your antivirus program’s White List and use the Viewer safely. If you are reluctant to use the Windows Client Viewer, however, you can simply use the Java Client Viewer, instead. |
Java

For mouse synchronization problems, see Macros, page 118, Mouse DynaSync Mode, page 125, and Sun / Linux, page 186. For other problems, see the table below:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Applet won't connect to the CN8000A</td>
<td>1. Java 6 Update 3 or higher must be installed on your computer.</td>
</tr>
<tr>
<td></td>
<td>2. Make sure to include the correct login string when you specify the CN8000A's IP address.</td>
</tr>
<tr>
<td></td>
<td>3. Close the Java Applet, reopen it, and try again.</td>
</tr>
<tr>
<td>I have installed the latest Java JRE, but I am having performance and stability problems.</td>
<td>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.</td>
</tr>
<tr>
<td>Java Applet performance deteriorates.</td>
<td>Exit the program and start again.</td>
</tr>
<tr>
<td>National language characters don't appear.</td>
<td>Use the CN8000A's On-Screen Keyboard and be sure that the local and remote computers are set to the same language. (See The On-Screen Keyboard, page 124.)</td>
</tr>
<tr>
<td>When I log in, the browser generates a CA Root certificate is not trusted, or a Certificate Error response.</td>
<td>The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See Trusted Certificates, page 174, for details.</td>
</tr>
<tr>
<td>There is no Virtual Media icon on my Control Panel.</td>
<td>The virtual media function only supports the Windows Client programs.</td>
</tr>
</tbody>
</table>
### Sun Systems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video display problems with HDB15 interface systems</td>
<td>The display resolution should be set to 1024 x 768:</td>
</tr>
<tr>
<td>(e.g., Sun Blade 1000 servers).¹</td>
<td>Under Text Mode:</td>
</tr>
<tr>
<td></td>
<td>1. Go to <strong>OK mode</strong> and issue the following commands:</td>
</tr>
<tr>
<td></td>
<td>setenv output-device screen:r1024x768x60</td>
</tr>
<tr>
<td></td>
<td>reset-all</td>
</tr>
<tr>
<td></td>
<td>Under XWindow:</td>
</tr>
<tr>
<td></td>
<td>1. Open a console and issue the following command:</td>
</tr>
<tr>
<td></td>
<td>m64config -res 1024x768x60</td>
</tr>
<tr>
<td></td>
<td>2. Log out</td>
</tr>
<tr>
<td></td>
<td>3. Log in</td>
</tr>
<tr>
<td>Video display problems with 13W3 interface systems (e.g.</td>
<td>The display resolution should be set to 1024 x 768:</td>
</tr>
<tr>
<td>Sun Ultra servers).*</td>
<td>Under Text Mode:</td>
</tr>
<tr>
<td></td>
<td>1. Go to <strong>OK mode</strong> and issue the following commands:</td>
</tr>
<tr>
<td></td>
<td>setenv output-device screen:r1024x768x60</td>
</tr>
<tr>
<td></td>
<td>reset-all</td>
</tr>
<tr>
<td></td>
<td>Under XWindow:</td>
</tr>
<tr>
<td></td>
<td>1. Open a console and issue the following command:</td>
</tr>
<tr>
<td></td>
<td>m64config -res 1024x768x60</td>
</tr>
<tr>
<td></td>
<td>2. Log out</td>
</tr>
<tr>
<td></td>
<td>3. Log in</td>
</tr>
<tr>
<td>The local and remote mouse pointers do not sync</td>
<td>The default configuration is for the local and remote mouse pointers to</td>
</tr>
<tr>
<td></td>
<td>automatically sync when you connect. Automatic mouse sync only supports</td>
</tr>
<tr>
<td></td>
<td>USB mice on Windows and Mac (G4 or higher) systems, however. You must</td>
</tr>
<tr>
<td></td>
<td>select <strong>Manual</strong> as the <strong>Mouse DynaSync Mode</strong> choice, and sync the</td>
</tr>
<tr>
<td></td>
<td>pointers manually. See <strong>Mouse DynaSync Mode</strong>, page 106 for further</td>
</tr>
<tr>
<td></td>
<td>details.</td>
</tr>
</tbody>
</table>

¹ These solutions work for most common Sun VGA cards. If using them fails to resolve the problem, consult the Sun VGA card's manual.
## Mac Systems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The local and remote mouse pointers do not sync.</td>
<td>There are two USB I/O settings for the Mac: Mac 1, and Mac 2 (see Date/Time, page 70). 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.</td>
</tr>
<tr>
<td>When I log in to the switch with my Safari browser, it hangs when I use the Snapshot feature.</td>
<td>Force close Safari, then reopen it. Don’t use the Snapshot feature in the future. To use the Snapshot feature with Safari, upgrade to Mac OS 10.4.11 and Safari 3.0.4.</td>
</tr>
</tbody>
</table>

## The Log Server

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Log Server program does not run.</td>
<td>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: <a href="http://www.microsoft.com/data/download.htm">http://www.microsoft.com/data/download.htm</a> 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.</td>
</tr>
</tbody>
</table>
Appendix

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 7 / 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 (5 units in from the left).
   d) Disable **Enhance Pointer Precision**.

![Mouse Properties dialog box](image)
Sun / Linux

Open a terminal session and issue the following command:

Sun:  xset m 1
     Linux: xset m 0
     or
     xset m 1

(If one doesn’t help, try the other.)
Supported KVM Switches

The KVM switches that can be used in a cascaded installation are as follows:

<table>
<thead>
<tr>
<th>ACS1208A</th>
<th>ACS1216A</th>
<th>CS1308</th>
<th>CS1316</th>
<th>CS1708A</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS1716A</td>
<td>CS1754</td>
<td>CS1758</td>
<td>CS228</td>
<td>CS428</td>
</tr>
</tbody>
</table>

Note: 1. Some of the CN8000A’s features may not be supported, depending on the functionality of the cascaded KVM switch. (For example, some switches do not support virtual media.)

2. Some features found on the cascaded KVM switches may not be supported on the CN8000A. (For example, the CS1754’s audio, and the CS1708A/CS1716A must use PS/2 connectors when cascading.)

Virtual Media Support

WinClient ActiveX Viewer / WinClient AP

- IDE CDROM/DVD-ROM Drives – Read Only
- IDE Hard Drives – Read Only
- USB CDROM/DVD-ROM Drives – Read Only
- USB Hard Drives – Read/Write*
- USB Flash Drives – Read/Write*
- USB Floppy Drives – Read/Write

* These drives can be mounted either as Drives or Removable Disks (see Virtual Media, page 99). Mounting them as removable disks allow booting the remote server if the disk contains a bootable OS. In addition, if the disk contains more than one partition, the remote server can access all the partitions.

- ISO Files – Read Only
- Folders – Read/Write
- Smart Card Readers

Java Applet Viewer / Java Client AP

- ISO Files – Read Only
- Folders – Read/Write
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 CN8000A and remove its housing.
2. Use a jumper cap to short the jumper on the mainboard labeled J10.
3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from J10.
6. Close the housing and power on the CN8000A.

After you start back up, you can use the default Username: administrator and Password: password to log in.
## Specifications

<table>
<thead>
<tr>
<th>Function</th>
<th>CN8000A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectors</strong></td>
<td></td>
</tr>
<tr>
<td>Console Ports</td>
<td>1 x SPHD-18 Male (Yellow)</td>
</tr>
<tr>
<td>KVM (Computer) Ports / Virtual Media</td>
<td>1 x SPHD-18 Female (Yellow)</td>
</tr>
<tr>
<td>Laptop USB Console (LUC)</td>
<td>1 x USB Mini Type B Female (Black)</td>
</tr>
<tr>
<td>PON1</td>
<td>1 x DB-9 Male (Black)</td>
</tr>
<tr>
<td>Modem</td>
<td>1 x DB-9 Male (Black)</td>
</tr>
<tr>
<td>LAN Ports</td>
<td>1 x RJ-45 Female</td>
</tr>
<tr>
<td>Power</td>
<td>1 x DC Jack</td>
</tr>
<tr>
<td><strong>Switches</strong></td>
<td></td>
</tr>
<tr>
<td>Reset</td>
<td>1 x Semi-recessed Pushbutton</td>
</tr>
<tr>
<td><strong>LEDs</strong></td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>1 (Orange)</td>
</tr>
<tr>
<td>Link</td>
<td>1 (Green)</td>
</tr>
<tr>
<td>10/100/1000 Mbps</td>
<td>1 (10 Mbps: Orange / 100 Mbps: Orange + Green / 1000 Mbps: Green)</td>
</tr>
<tr>
<td><strong>Emulation</strong></td>
<td></td>
</tr>
<tr>
<td>Keyboard / Mouse</td>
<td>USB, PS/2</td>
</tr>
<tr>
<td>Video</td>
<td>Up to 1920 x 1200 @ 60 Hz; DDC2B</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>DC 5.3 V; 7.26 W</td>
</tr>
<tr>
<td><strong>Environmental</strong></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>0° to 50° C (CN8000A)</td>
</tr>
<tr>
<td></td>
<td>0° to 40° C (Power Adapter)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-20° to 60° C</td>
</tr>
<tr>
<td>Humidity</td>
<td>0 - 80% RH, Non-condensing</td>
</tr>
<tr>
<td><strong>Physical Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Housing</td>
<td>Metal</td>
</tr>
<tr>
<td>Weight</td>
<td>0.49 kg</td>
</tr>
<tr>
<td>Dimensions (L x W x H)</td>
<td>20.20 x 8.14 x 2.50 cm</td>
</tr>
</tbody>
</table>

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 cannot be processed without the original proof of purchase.

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

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

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

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

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

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

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

A
Access Ports, 44
Account Policy, 59
Administration, 33
ANMS, 48, 51
Firmware upgrading, 38
Network, 43
Administration Page
Date/Time, 70
Administrator Login Failure, 188
ANMS, 48, 51
Authentication
external, 48, 51

B
Backup Configuration / User Accounts, 39
Benefits, 3

C
Cables, 6
custom, 13
CC Management, 54
Certificate
Signing Request, 63
CN8000
Front view, 11
Rear view, 12
Configuration
backup, 39
restore, 39
Console cable, 13
Control Panel
Functions, 82, 116
JavaClient, 115
WinClient, 81
Corrupt Password, 188
Create CSR, 63

D
Date/Time Settings, 70
Device Information, 42
Dial Back, 65
DIN Rail Mounting, 16
Disable Local Authentication, 51
DNS Server, 25, 45
DynaSync, 106, 125
Encryption, 60
External authentication, 48, 51

F
Features, 3
Firmware upgrade, 38
Forgotten Password, 188

H
Hardware
Setup, 17
Hotkeys, 85, 118
Windows Client, 85

I
Installation, 17
Invalid login, 28
IP
Address determination, 165
Installer, 43
IP Installer, 165

J
Java Applet
Navigation, 114

K
Keyboard
On-Screen, 104, 124
Keyboard Emulation, 171
Mac, 171

L
LDAP
Permission attributes, 145
Permission examples, 146
LDAP Settings, 53
Log Server
Configure, 129
Events, 130
Installation, 127
Main Screen, 128, 133
Maintenance, 131
Menu Bar, 129
Options, 132
Search, 130
Starting Up, 128
Tick Panel, 134
Log server, 49
Logging in
Browser, 27
Login
Invalid login, 28
Login Failures, 55
Login String, 58

M
MAC
Address, 23, 42
Mac Keyboard Emulation, 171
Macros, 118
JavaClient, 118
Search, 91, 120
System, 91, 119
User, 87, 119
WinClient, 85
Main Webpage Elements, 29
Message Board
Java Applet, 121
Windows Client, 97
Modem operation, 172
Mounting
DIN Rail, 16
Rack, 15
Mouse
DynaSync Mode, 106, 125
Synchronization, 106, 125
Mouse pointer type, 106, 124
Mouse Synchronization, 185

N
Network, 43
Network Time, 71
Network Transfer Rate, 47

O
Online
Registration, iii
On-Screen Keyboard, 104, 124
OpenLDAP
Server Configuration, 149
Server Installation, 148
OSD
Navigation, 22
Overview, 21
Password, 21
Overview, 1

P
Password, 21
Port Access
Sessions, 37
Index

Port Forwarding, 170
PPP, 172
Private Certificates, 178

R
Rack Mounting, 15
Safety information, 159
RADIUS
examples, 52
RADIUS Settings, 51
refresh screen, 95
Requirements
Operating Systems, 8
Restore Configuration / User Accounts, 39

S
Safety Instructions
General, 157
Rack Mounting, 159
screen, refresh, 95
Search
Macros, 91, 120
Security, 55
Login string, 58
Self-signed certificates, 178
Sessions, 37
SMTP Settings, 48
SNMP Server, 49
Sun Keyboard Emulation, 171
Sun Systems
Troubleshooting, 183
Supported KVM Switches, 187
Synchronization
mouse, 106, 125
System Macros, 91, 119
System Requirements, 6

T
Technical Support, 164
Telephone support, iii
Tick Panel, 134
Time settings, 70
Troubleshooting
General Operation, 179
Java, 182
Log Server, 184
Mac Systems, 184
Sun Systems, 183
Windows, 181
Trusted Certificates, 174

U
User Accounts
backup, 39
restore, 39
User Macros, 87, 119
User Management, 34
User Notice, iii
User Station Filters, 56

V
Video Settings
JavaClient Viewer, 120
Windows Client, 94
Virtual Media
JavaClient, 123
WinClient, 99
Virtual Media Support, 187

W
WinClient Viewer, 79
Windows Client
Message Board, 97
Starting up, 79