1-Local / Remote Share Access Single Port

DVI KVM over IP Switch
CN9600

User Manual

www.aten.com

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.

Warning: Operation of this equipment in a residential environment could cause radio interference.

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)

이 기기는 업무용 (A 급) 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:

International	886-2-8692-6959
China	86-400-810-0-810
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988 1-949-428-1111

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 CN9600 package consists of:

- 1 CN9600 DVI KVM over IP Switch
- 1 Custom KVM Cable Set
- 1 USB 2.0 Virtual Media 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 CN9600 since this manual was published. Please visit our website to download the most up-to-date version.

Manual Date: 2020-02-03

Contents

5. Accessing Remote Server

6. The Windows Client Viewer

7. Local Access

8. The Log File

9. The Log Server

Appendix

About this Manual

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

Chapter 1, Introduction, introduces you to the CN9600 system. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup, describes how to set up your installation. Diagrams showing the necessary steps are provided.

Chapter 3, Browser Login, describes how to log into the CN9600 with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 4, Configuration, explains the administrative procedures that are employed to configure the CN9600's working environment.

Chapter 5, Accessing Remote Server, describes how to access the CN9600 remotely.

Chapter 6, The Windows Client Viewer, explains how to use the control panel of the CN9600.

Chapter 7, Local Access, describes how to access the CN9600 locally.

Chapter 8, The Log File, shows how to use the log file utility to view the events that take place on the CN9600.

Chapter 9, The Log Server, explains how to install and configure the Log Server.

An *Appendix*, provides specifications and other technical information regarding the CN9600.

Conventions

This manual uses the following conventions:

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

Product Information

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

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

This Page Intentionally Left Blank

Chapter 1
Introduction

Overview

The CN9600 DVI KVM over IP Switch is a cost-efficient over-IP device, which allows remote access of digital video, audio and virtual media via remote control of a PC or workstation. The CN9600 enables over-IP capability by connecting compatible ATEN DVI KVM switch and/or LCD console, such as the CS1768 (8-Port USB DVI/Audio KVM Switch) or CL3800 (DVI LCD Console).

The CN9600 expands on previous models by providing a more compact, slimmer and space-saving design for utility optimization, and a FPGA graphics processor that offers better image and video quality to enhance user experience, while also meeting the RS-232 DTE/DCE standards for serial control.

For user-friendly operation, a mini USB port on the front panel is designed as a Laptop USB Console (LUC) port. Users just simply connect a laptop to the LUC port, and can access any computer connected to the switch for easy on-site management. That means no additional monitor, keyboard and mouse is strongly required locally for routine maintenance. Besides, the CN9600's Virtual Media function allows a user to perform diagnostic testing, file transfers, or apply OS/applications updates and patches from a remote console.

To ensure seamless connectivity, the CN9600 is equipped with dual LAN and dual power functionality to keep operation in the server room smooth and efficient. The CN9600 also supports microphone and speakers on the local and remote console.

Integrating all these advanced functionalities, the CN9600 provides an affordable and durable over-IP server management solution while assuring users with operational dependability and efficiency.

Features and Benefits

Hardware

- Compact and slim design for space utility optimization
- Provides a FPGA graphics processor for better image quality and enhanced fps (frames per second) throughput for crisp video display response
- Provides over-IP capability to DVI KVM switches that do not have built-in over-IP functionality

Note: Compatible KVM Switch: ATEN DVI Single Link KVM Switches.

- Local console provides USB keyboard and mouse support
- A mini USB port on the front panel serves as a Laptop USB Console (LUC) port
- Two 10/100/1000 Mbps NICs for redundant LAN or two IP operation
- Dual Power Supply for power backup
- Supports multiplatform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices
- Virtual Media support

Note: Some of the CN9600's features may not be supported, depending on the functionality of the cascaded KVM switch. (For example, some switches do not support virtual media.)

- High video resolution – up to 1920 x 1200 @ 60Hz for both local and remote consoles
- Audio support – microphone and speakers are supported on the local and remote console

Management

- Complies to the RS-232 DTE/DCE standards for serial control
- Up to 64 user accounts – up to 32 users can simultaneously share control
- Console access right management
- End session feature – administrators can terminate running sessions
- Event logging and Windows-based Log Server support

- Event Logging – the CN9600 can record all events and write them to a searchable database
- Supports instant notification of critical system events via email, SNMP trap and Syslog
- Firmware upgradable via remote access
- Access the CN9600 via a built-in serial viewer, or via third-party software (such as PuTTY) for Telnet and SSH sessions
- Out of Band support – access the CN9600 through its serial port using a dial-up connection
- Port Share Mode allows multiple users to gain access to a server simultaneously
- Local/Remote Share Mode conveniently grants shared or exclusive console privilege
- Integration with ATEN CC2000 Management Software
- Integration with ATEN CCVSR Video Session Recording Software
- Supports ATEN KVM over IP Console Station (KA8270 / KA8280 / KA8278 / KA8288)
- DDNS – allows mapping of a dynamic IP address assigned by a DHCP server to a host name
- Supports export/import of user account and configuration settings
- Supports permission-controlled browser operation
- Supports IPv6

Easy-to-Use Interface

- Browser-based and AP GUIs offer a unified multilanguage interface to minimize user training time and increase productivity
- Multiplatform client support (Windows, Mac OS X, Linux, Sun)
- Multibrowser support (IE, Mozilla, Firefox, Safari, Opera, Netscape)
- Browser-based UI in pure Web technology allows administrators to perform administrative tasks without pre-installed Java software package requirements
- Full-screen or sizable and scalable Virtual Remote Desktop
- Magic Panel with configurable function for quick launch

Advanced Security

- Smart Card/CAC Reader support
- External authentication support: RADIUS, LDAP, LDAPS and MS Active Directory
- Supports TLS 1.2 data encryption and RSA 2048-bit certificates to secure users logging in from browsers
- 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 keyboard/mouse, video, and virtual media data encryption
- Supports IP/MAC Filter
- Supports password protection
- Private CA

Virtual Media

- Virtual media enables file applications, OS patching, software installation and diagnostic testing
- Works with USB-enabled servers at OS and BIOS level
- Supports USB 1.1 and USB 2.0 DVD/CD drives, USB mass storage devices, PC hard drives, folders and ISO images

Virtual Remote Desktop

- Video quality and video tolerance can be adjusted to optimize data transfer speed; monochrome color depth, threshold and noise settings can be adjusted for compression of the data bandwidth in low bandwidth situations
- Full-screen video display or scalable video display
- Message Board for communication among remote users
- On-screen keyboard with multilanguage support
- Mouse DynaSync^{TM} – automatically synchronizes the local and remote mouse movements
- Supports Exit Macros
- BIOS-level access

System Requirements

Remote User Computers

Remote user computers (also referred to as client computers) are the ones the users log into the switch with from remote locations over the Internet. The following equipment must be installed on these computers:

- The computers used to access the switch have at least a P III 1 GHz processor, with their screen resolution set to 1024 x 768. It is recommended that your PC has P IV 2 GHz and at least 1 Gb of RAM.
- Browsers must support TLS 1.2 encryption.
- A network transfer speed of at least 128 kbps is required.
- For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.

Servers

Servers are the computers connected to the switch via KVM Cables. The following equipment must be installed on these servers:

- For USB KVM Cable Connections: a Type A USB port and USB host controller
- For virtual media connection, an extra Type A USB and USB host controller.

Cables

- A custom USB KVM cable set to link the CN9600 to a server or KVM switch are provided with this package.
- Custom KVM cable sets are available in various lengths, as shown in the table below:

Cable Type	Length	CS Part Number
USB	1.8 m	2L-7D02U / 2L-7D02UI
	3.0 m	2L-7D03U / 2L-7D03UI
	5.0 m	2L-7D05U

To purchase additional cable sets, contact your dealer.

- One custom Console cable set to link the CN9600 to a local console is provided with this package.
- Cat 5e/6 or higher Ethernet cable (not provided with this package), should be used to connect the CN9600 to the LAN, WAN, or Internet.

Video

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

Resolution	Refresh Rates
640 x 480	60, 72, 75, 85
720 x 400	70, 85
800 x 600	56, 60, 72, 75, 85
1024 x 768	60, 70, 75, 85
1152 x 864	75
1280 x 720	60
1280 x 960	60
1280 x 1024	60, 75
1366 x 768	60
1440 x 900	60
1440 x 1050	60
1600 x 900	60
1600 x 1200	60
1680 x 1050	60
1920 x 1080	60
1920 x 1200	60

Operating Systems

- Supported operating systems for remote user computers that log into the CN9600 include Windows 2000 or later, and other systems capable of running Sun's Java Runtime Environment (JRE) 6, Update 3, or later (Linux, Mac, Sun, etc.).
- Supported operating systems for servers that connect to the CN9600 are shown in the table below:

OS		Version
Windows		2000 or later
Linux	RedHat	7.1 or later
	Fedora	Core 5 or later
	SuSE	9.0 or later
	Mandriva (Mandrake)	9.0 or later

OS		Version
UNIX	AIX	4.3 or later
	FreeBSD	3.51 or later
	Sun	Solaris 8 or later
Novell	Netware	5.0 or later
Mac		OS 9 or later
DOS		6.2 or later

Browsers

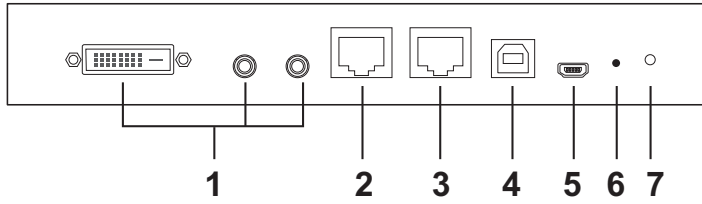
Supported browsers for users that log into the CN9600 include the following:

Browser		Version
Internet Explorer		6 or later
Chrome		8.0 or later
Firefox	Windows	3.5 or later
	Linux	3.0 or later
Safari	Windows	4.0 or later
	Mac	3.1 or later
Opera		10,0 or later
Mozilla	Windows	1.7 or later
	Sun	1.7 or later
Netscape		9.0 or later

* See *Mac Systems*, page 132, for further information regarding Safari.

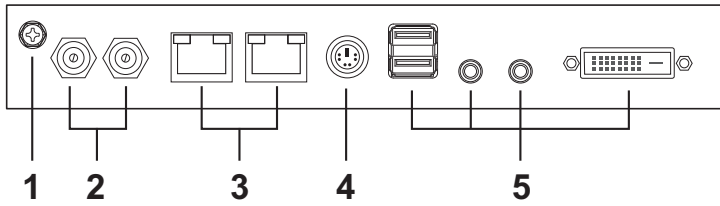
Components

Front View



No.	Component	Description
1	PC/KVM Port	Use the KVM cable provided with this package that links the CN9600 to your PC / Server for this port. Connect the DVI video display, microphone and speakers to the server or the KVM switch you are installing. Each connector is color coded and marked with an appropriate icon.
2	RS-232 DTE Port	Connect a serial data terminal equipment device (e.g. a PC) to this port.
3	RS-232 DCE Port	Connect a serial data communication equipment device (e.g. a modem) to this port.
4	USB Type-B Port	Connect the keyboard/mouse to the server or the KVM switch you are installing.
5	Laptop USB Console (LUC) Port	For laptop local access (See *Local Access*, page 99), connect the laptop's USB to this port. Make sure the mode of USB IO Settings (see *USB IO Settings*, page 57) is set to LUC. If the mode of *USB IO Settings* is set to Virtual Media, this port will not work.
6	Reset button	Press the Reset button for more than three (3) seconds to revert to factory settings.
7	Power LED	Lights Green when the CN9600 is powered up.

Rear View



No.	Component	Description
1	Grounding Terminal	Connect to a suitable grounding object.
2	Power Jacks	Plug the power adapter provided with this package into an AC power source, then plug the power adapter cable into any power jack. Plug another power adapter into an AC power source, then plug the power cable into the other CN9600 power jack. **Note:** Dual power operation is optional – the second power source is for back-up; a second power adapter requires a separate purchase.
3	LAN Ports	Connect a Cat 5e/6 network cable to these ports for uplink connection.
4	Control Port	This port only connects to an optional control box that requires a separate purchase.
5	Local Console Port	Connect the cable for the local console (USB keyboard, DVI monitor, USB mouse, microphone and speakers) to this port. Each connector is color coded and marked with an appropriate icon.

Chapter 2
Hardware Setup

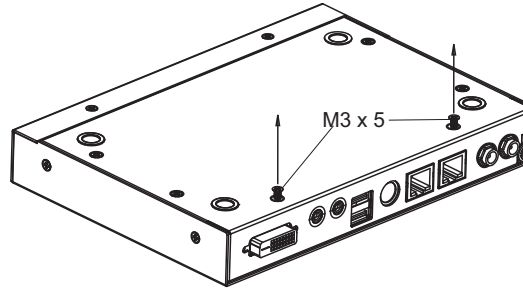
1. Important safety information regarding the placement of this device is provided on page 113. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
3. Any installation that does not follow the instructions in this guide may be hazardous.
4. The power source for this product is intended to be supplied by a power adapter only, not a DC mains.

Mounting

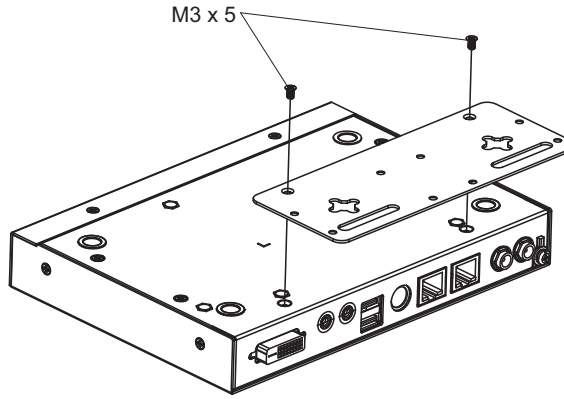
The CN9600 can be mounted on most standard 19" (1U) racks or mounted on a wall.

Attaching the Bracket

1. Detach the screws from the underside of the unit as shown:

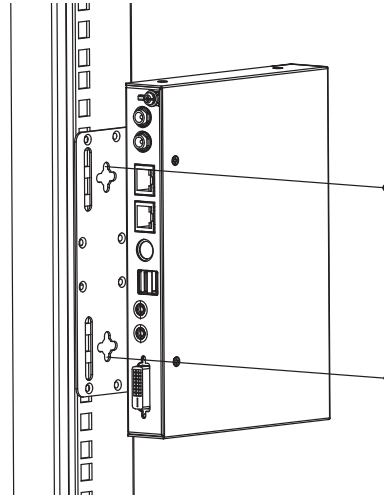


2. Attach the bracket and secure the bracket using the screws from the previous step.



Rack Mount

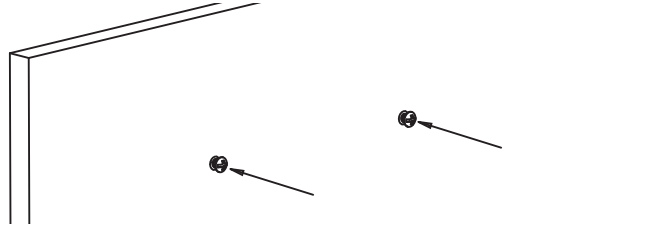
1. Position the device in the rack and align the holes in the mounting brackets with the holes on the rack.
2. Screw the mounting bracket to the rack.



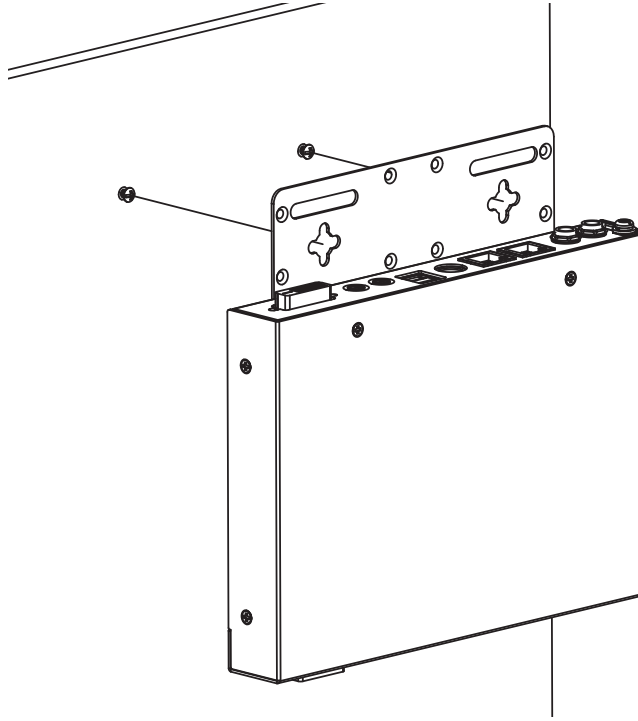
Wall Mount

CN9600 wall mounting is designed to be hanged onto a wall.

1. On the wall you wish to wall mount your unit, attach two screws as the hanger hooks for the bracket's corresponding hanger keyholes (you may need to draw the positions of the hanger screws on the wall prior to attaching the screws), take care to leave enough space for the hanger keyholes. An example is shown:



2. Hang the unit to hanger hooks matching the bracket's hanger keyholes.



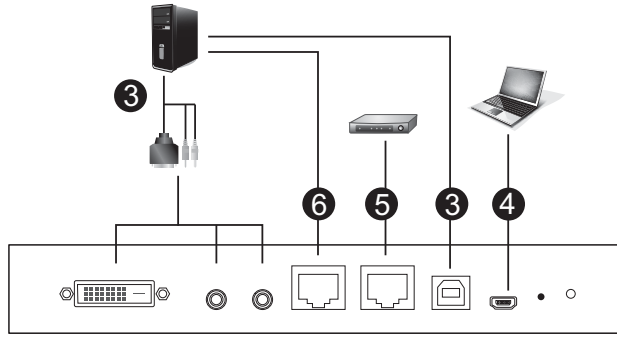
Hardware Installation

Follow the steps below and refer to the diagram on the following page (the steps and the numbers correspond to each other) for hardware installation.

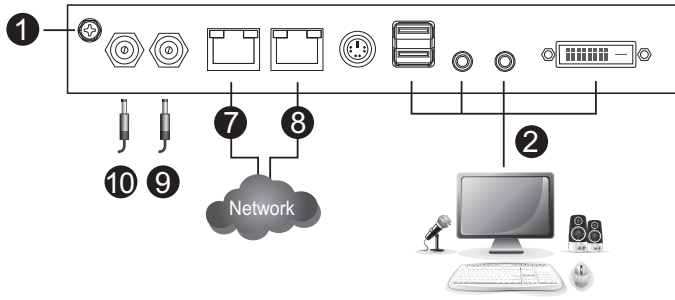
1. Connect the unit's grounding terminal to a suitable grounded object.
2. Plug your USB keyboard, mouse, DVI monitor, speakers and microphone into the local console port section located on the rear panel.
3. By using the KVM cable provided with the package, connect the unit's PC/KVM Port and USB Type-B Port to the keyboard, video, mouse, speakers and microphone ports of the server or KVM switch that you are installing.
4. (Optional) If you wish to access locally using Laptop USB Console (LUC) function, connect a USB port of the laptop to this (LUC) port.

   Make sure you have set the mode in USB IO Setting to LUC. Refer to *USB IO Settings* on page 57 for more information.
5. (Optional) If you are using other serial devices (data terminal equipment) such as a touch panel, connect it to the RS-232 DCE Port with a network switch console cable.
6. (Optional) If you are using other serial devices (data communication equipment) such as a PC, connect it to the RS-232 DTE Port with a network switch console cable.
7. Plug a network cable into one of the unit's LAN ports.
8. (Optional) Plug a second network cable into the other LAN port for dual LAN operation.
9. Plug the power adapter provided with this package into an AC power source and plug the power adapter cable into one of the unit's power jacks. Now the CN9600 is turned on.
10. (Optional) Plug another power adapter into an AC power source and plug the power cable into the other power jack for dual power operation.

Note: The second power connection acts as power back-up. A second power adapter can be purchased from your ATEN supplier.

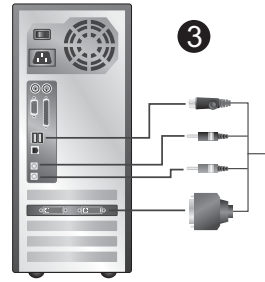


Front View



Rear View

USB KVM Cable Connection



This Page Intentionally Left Blank

Chapter 3
Browser Login

The CN9600 can be accessed either from an Internet type browser, or via the following methods:

- Windows Client or Java Client (*Windows and Java Client Viewer (web access)*, page 66);
- Windows or Java application (AP) program (*The Windows Client AP*, page 67 or *The Java Client AP*, page 70);
- Laptop USB Console (LUC) port (*Laptop USB Console (LUC)*, page 100); and
- Local Console (see *Local Console*, page 99)

The next several chapters describe browser-based operations.

Logging In

To operate the CN9600 from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the CN9600 you want to access in the browser's URL location bar.

   The default IP address for non-DHCP environment is 192.168.0.60.

   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/CN9600
   ```

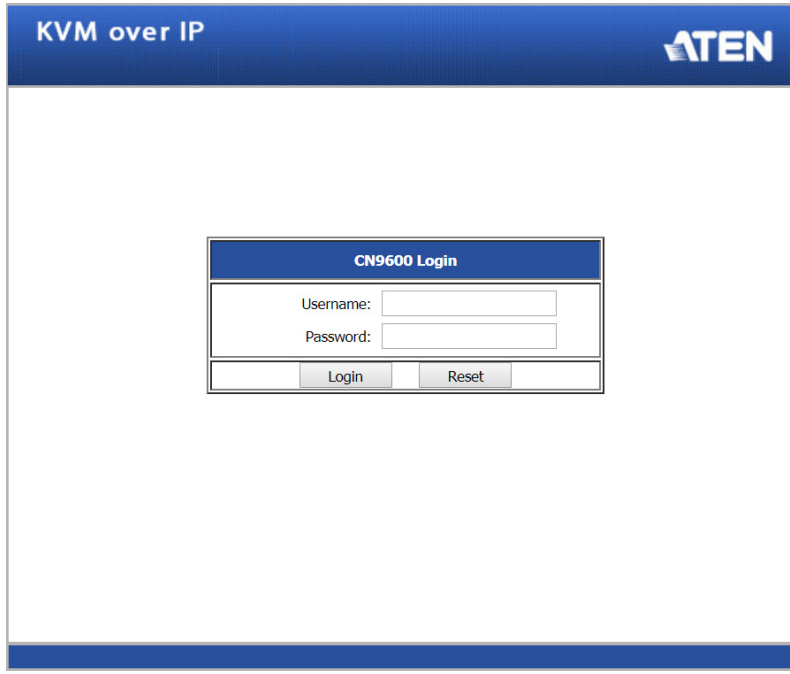
   If you don't know the IP address and login string, ask your Administrator.

   2. If you are the administrator, and are logging in for the first time, the various ways to determine the CN9600's IP address are described in the Appendix on page 117.

2. If a **Security Alert** appears, click **Continue to this website** to accept the certificate – it can be trusted. (See *Trusted Certificates*, page 123, for details.) If a second certificate appears, accept it as well.

Note: The **Security Alert** screen's appearance varies depending on the browser version.

The CN9600 login page appears:



3. Provide a valid **Username** and **Password** (set by the CN9600 administrator), and click **Login** to continue.

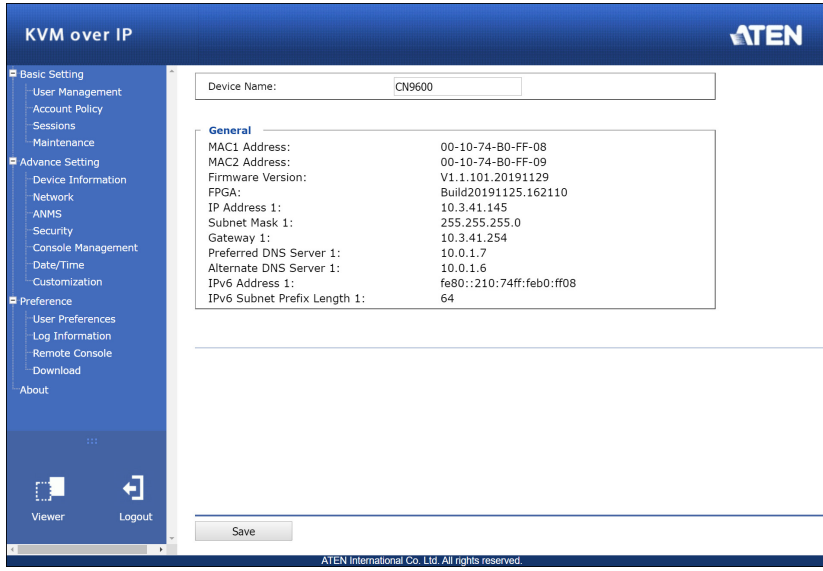
Note: 1. If you are the administrator and are logging in for the first time, use the default username (*administrator*) and the default password (*password*). For security purposes, the system will prompt you to change the login password. The password must be different from your login password.

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.

The main page appears after logging in successfully.

Main Screen

After you have successfully logged in, the CN9600 Main screen appears:



The Main screen consists of the user menu in the left panel, with a *Viewer* icon (to launch the Java or WinClient Viewer) as well as a *Logout* icon displayed in the bottom of the menu.

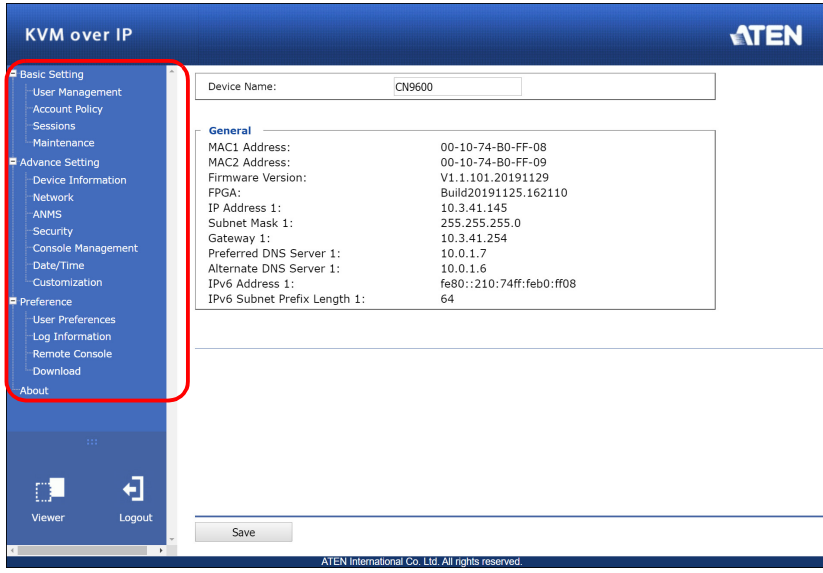
Note: If a user does not have permission to perform a particular activity, the menu option for that activity does not appear. See *User Management*, page 22, for permission details.

This Page Intentionally Left Blank

Chapter 4
Configuration

Introduction

The administration utilities, represented by the links and icons located at the left panel of the CN9600 web page, are used to configure the CN9600's operating environment. This chapter discusses each of them in turn.



Note: 1. As you make your configuration changes in each dialog box, click **Save** to apply the settings.

2. Some configuration changes only take effect after a CN9600 reset. To have the changes take effect, log out and then log back in again.

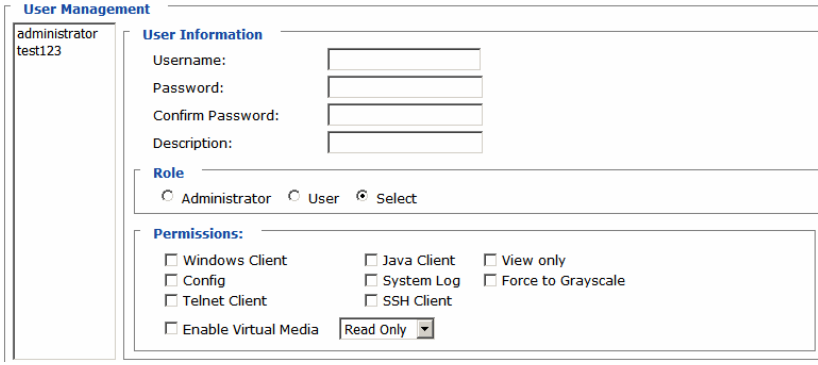
3. If you don't have configuration privileges (see *User Management*, page 22), the Administration configuration dialogs are not available.

Basic Setting

The following sections describe the screens under *Basic Setting*. Click the **User Management**, **Account Policy**, **Sessions** and **Maintenance** links in the left panel menu to view the screens.

User Management

The User Management screen allows you to add, edit or remove user accounts to the CN9600, as well as modify the role and permissions of each account:



User Information

- **Username:** This is the user name of the account.
- **Password / Confirm Password:** Enter a new password if you are changing it. Re-enter the new password to confirm it.
- **Description:** Enter a descriptive word or phrase to describe the account.

Role

This allows the administrator to select which permissions the account will be allowed.

- **Administrator**: Gives the user Administrator level access. All permissions except *View Only* and *Force to Grayscale* are granted (see permissions below).
- **User**: Gives the user User level access. Windows Client and Java Client permissions are granted (see permissions below).
- **Select**: This allows you to manually select the user's permission in the *Permissions* section.

Permissions

Click to check/uncheck an item to grant/deny access to that aspect of the CN9600's operation.

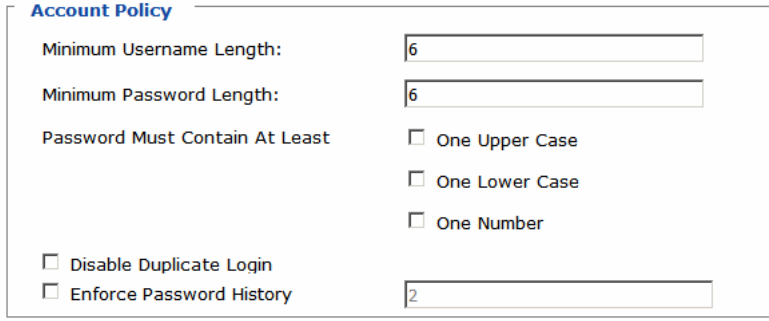
- **Windows Client**: Checking this allows a user to access the CN9600 via the Windows Client software.
- **Config:** Checking this allows the user to set up and modify the CN9600's operating environment.
- **Telnet**: Checking this allows a user to access the CN9600 via the network protocol of the same name.
- **Enable Virtual Media**: Checking this allows a user to utilize the CN9600's Virtual Media capabilities (see *Virtual Media*, page 87 for details). User the drop down menu to select whether the user has **Read/ Write**, or **Read Only** permission.
- **Java Client**: Checking this allows a user to access the CN9600 via the Java Client software.
- **System Log**: Checking this allows a user to view the contents of the log file.
- **SSH Client**: Checking this allows a user to access the CN9600 via SSH sessions.
- **View Only**: Checking this restricts a user from operating the keyboard and the mouse.
- **Force to Grayscale**: Checking this renders the remote display to be in grayscale. This can speed up I/O transfer in low bandwidth situations.

After filling out the fields, click the action you want the CN9600 to apply:

- *Reset* - Click this to clear the fields.
- *Add* - Click this to add the new account to the CN9600.
- *Update* - Click this to update the settings of an existing account.
- *Remove* - Click this to remove the selected account.

Account Policy

Set the parameters for the username and password.



- Minimum Username Length: Enter the minimum number (0 – 20) of characters required for a username (default is 6).
- Minimum Password Length: Enter the minimum number (0 – 20) of characters required for a password (default is 6).
- Password Must Contain At Least: check the checkbox to make sure the password must contain at least *One Upper Case*, *One Lower Case* and/or *One Number* character.

Note: This policy only affects user accounts created after this policy has been enabled, as well as password changes to existing user accounts.

- Check *Disable Duplicate Login* to ensure that only one session for each user account is active. This prevents users from logging in with the same account at the same time.
- To prevent users from using the same password when they are required to recreate their passwords, you can check *Enforce Password History*. In the field, enter the number of password changes that must occur before a previous password can be used a second time.

Sessions

The Sessions screen lets the administrator see at a glance all the users currently logged into the CN9600, and provides information about each of their sessions.

Username	IP	Login Time	Client	Category	Devices	Ports
administrator	10.3.41.102	2013/03/21 02:51:12	Browser	Administrator	None	

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

- The *IP* heading refers to the IP address that the user has logged in from.
- The *Client* heading refers to the means the user employed to connect to the CN9600 (Browser, WinClient AP, Java Client AP, etc.).
- The *Category* heading lists the type of user who has logged in: Admin (Administrator), User, or Select. (See *Download*, page 62 for details about user types.)

This screen also gives the administrator the option of forcing a user to logout. To do that, click to select the user and click **End Session**.

Click **Refresh** to update the screen.

Maintenance

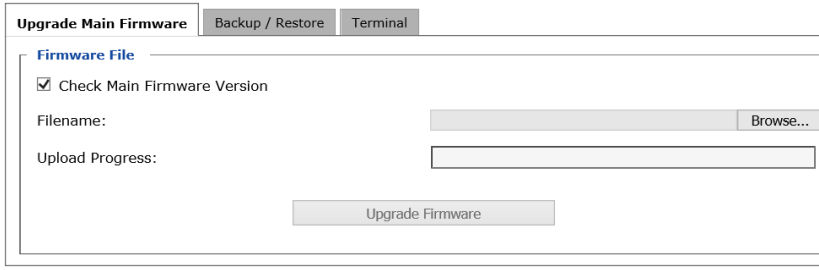
The Maintenance screen allows the Administrator to upgrade the CN9600's firmware, backup/restore the CN9600's configuration settings and allows you to configure the unit's setting using Terminal.

Upgrade Main Firmware

As new versions of the CN9600 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 CN9600; and click *Maintenance* in the left panel menu to bring up the *Firmware File* dialog box as follows:



3. Click **Browse** and navigate to the directory that the new firmware file is in and select the file.
4. Click the **Upgrade Firmware** button.

   If **Check 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 the upgrade version, a message appears informing you of the fact and the procedure stops.

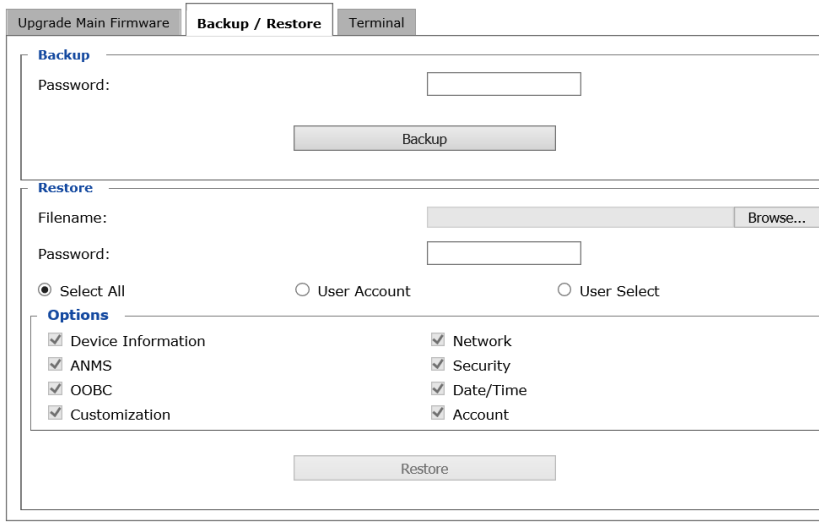
Note: If you want to install an older firmware version, you must uncheck the **Check Firmware Version** checkbox before clicking **Upgrade Firmware**.

5. After the upload completes, a message appears on the screen to show you the progress of the system upgrade.
6. When the system upgrade finishes, the current user will be logged out automatically and the system will inform the user that the system will reboot shortly.

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

Backup / Restore

The Backup / Restore screen gives you the ability to back up the CN9600's configuration and user profile information. Backed up User Account and Configuration information can be restored with the *Restore* section. Information currently configured on the CN9600 will be replaced with the information that you restore.



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 restore the configuration later.

2. Click **Backup**.

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

Note: The CN9600 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.

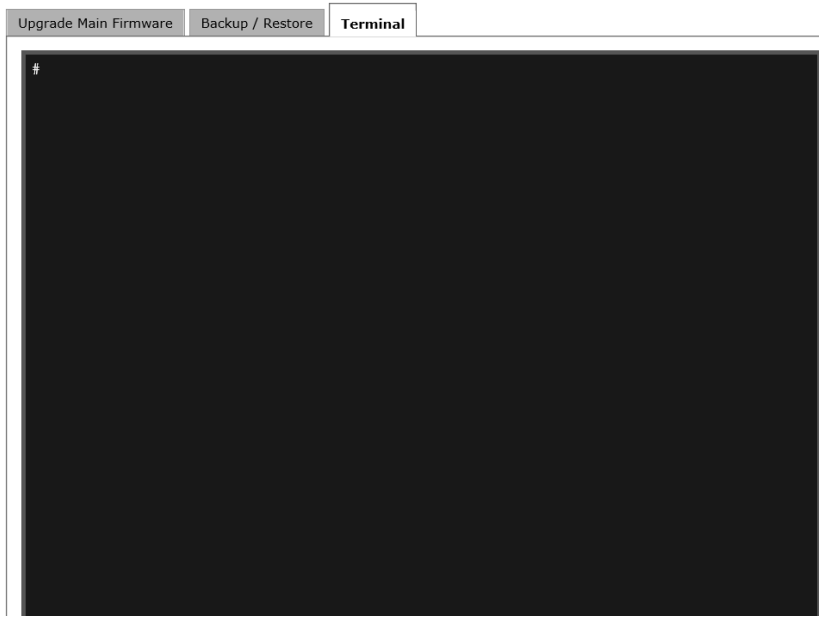
To restore a previous backup, do the following:

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 was not set, you can leave this field blank.
2. Click **Browse** and navigate to the file and select it.
3. Select which parts of the backup you wish to restore:
   - Select *Select All* to restore all information
   - Select *User Account* to only restore User Account information
   - Select *User Select* to choose which backed up information you wish to restore. When this was selected, check/uncheck the checkbox(es) to select/deselect what you wish to be restored.
4. When you have made your selections, click **Restore**.

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

Terminal

The Terminal section allows you to configure the unit using terminal commands.



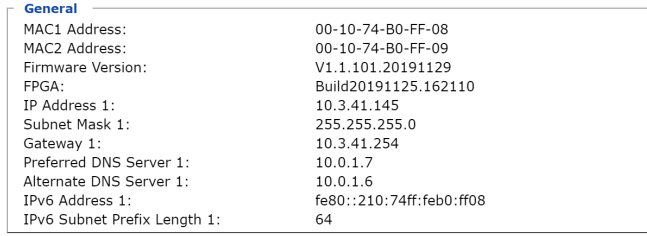
For a list of configurable commands, type *help*.

Advanced Setting

The following sections describe the administration utilities covered under *Advanced Setting*, including the **Device Information**, **Network**, **ANMS**, **Security, Console Management**, **Date/Time, Customization** screens.

Device Information

The Device Information screen provides information about the CN9600's status. You can change the device name in this screen.

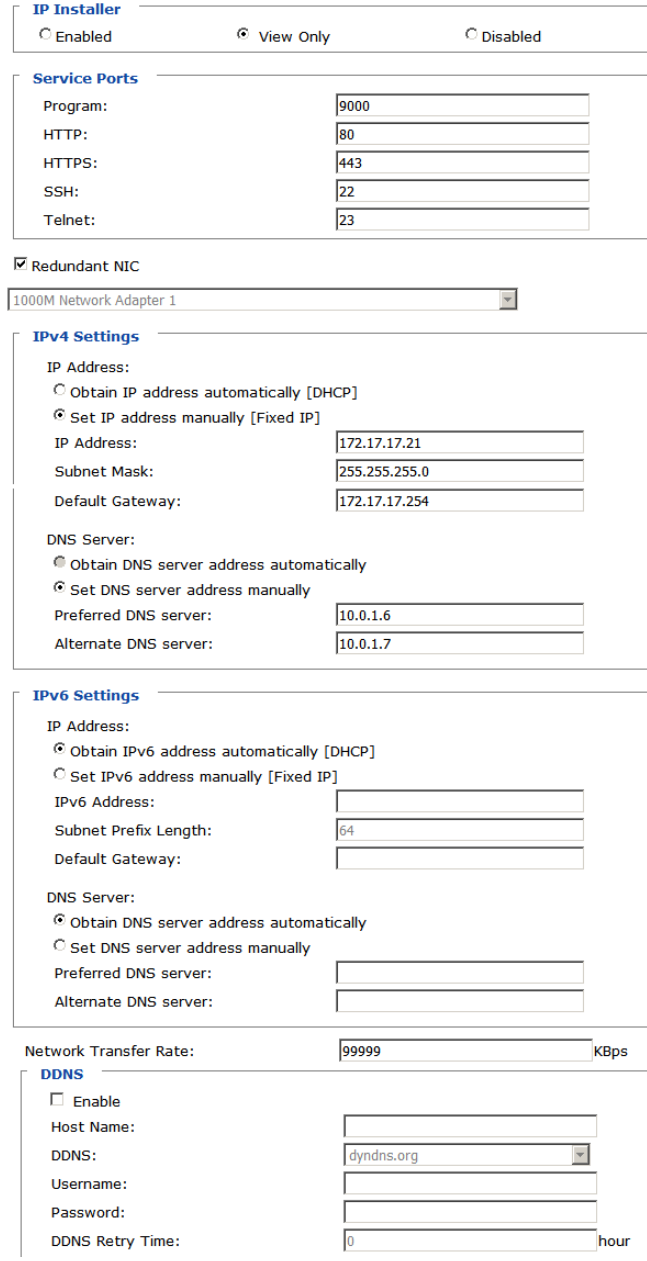


General

- **Device Name**: To make it easier to manage installations that have more than one CN9600, each one can be given a name. Enter a name (16 characters max.) for the CN9600 then click **Save**.
- **MAC (1, 2) Address**: The CN9600's MAC Address displays here.
- **Firmware Version / FPGA**: Indicates the CN9600's current firmware version level and build. New versions of the CN9600's firmware can be downloaded from our website as they become available (see *Upgrade Main Firmware*, page 26). You can reference this number to see if there are newer versions available on the website.
- **IP Address**: Displays the CN9600's Internet Protocol Version 4 (32 bit) address (in the legacy format).
- **Subnet Mask**: This is the subnet mask for the IP connection.
- **Gateway**: This is the CN9600's gateway address.
- **IPV6 Address / IPv6 Subnet Prefix Length**: Displays the CN9600's Internet Protocol Version 6 (128 bit) address (in the new format). See *IPv6*, page 119 for details.

Network

The Network screen is used to specify the CN9600's network environment.



IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the CN9600. Click one of the radio buttons to select *Enabled, View Only, or Disabled* for the IP Installer utility. See p. 117 for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the CN9600 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

Specify the ports that the CN9600 uses for various network services.

- **Program**: This is the port number for connecting to the CN9600 from the Windows Client and Java Viewers, and from the Windows and Java Client AP programs. The default is 9000.
- **HTTP**: The port number for a browser login. The default is 80.
- **HTTPS**: The port number for a secure browser login. The default is 443.
- **SSH**: The port number for a secure shell login. The default is 22.
- **Telnet**: The port number for a secure console login. The default is 23.

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 there is no firewall (on an Intranet, for example), it does not matter what these numbers are set to, since they have no effect.

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 log in. If not, an invalid port number (or no port number) is specified, the CN9600 will not be found.

Redundant NIC

A Redundant NIC ensures that the CN9600 is always online by switching to another network adapter in case the primary connection fails.

- Check *Redundant NIC* if you are using the secondary LAN port for a second IP address.
- If you are using the secondary LAN port for a second IP address, leave Redundant NIC unchecked. Use the drop-down menu and select 1000M Network Adapter 2, then set the IP and DNS addresses for it.

IPv4 Settings

The CN9600 can either have its IP address assigned dynamically at bootup (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the **Obtain an IP address automatically**, radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Set IP address manually**, radio button and fill in the IP address.

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

2. If the CN9600 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, you can use the IP installer. See *IP Address Determination*, page 117, for information.

The CN9600 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 **Use the following DNS server address**, radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

IPv6 Settings

The CN9600 can either have its IPv6 address assigned dynamically at bootup (DHCP), or it can be given a fixed IPv6 address.

- For dynamic IP address assignment, select the **Obtain an IPv6 address automatically**, radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Set IPv6 address manually**, radio button and fill in the IP address.

The CN9600 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 **Use the following DNS server address**, radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

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 CN9600 transfers data to remote computers. The range is from 4–99999 Kilobytes per second (KBps).

DDNS

DDNS maps a dynamic IP address assigned by a DHCP server to a host name. The CN9600 can update the DDNS server with its IP address at certain time intervals. To enable the DDNS capability for the CN9600, do the following:

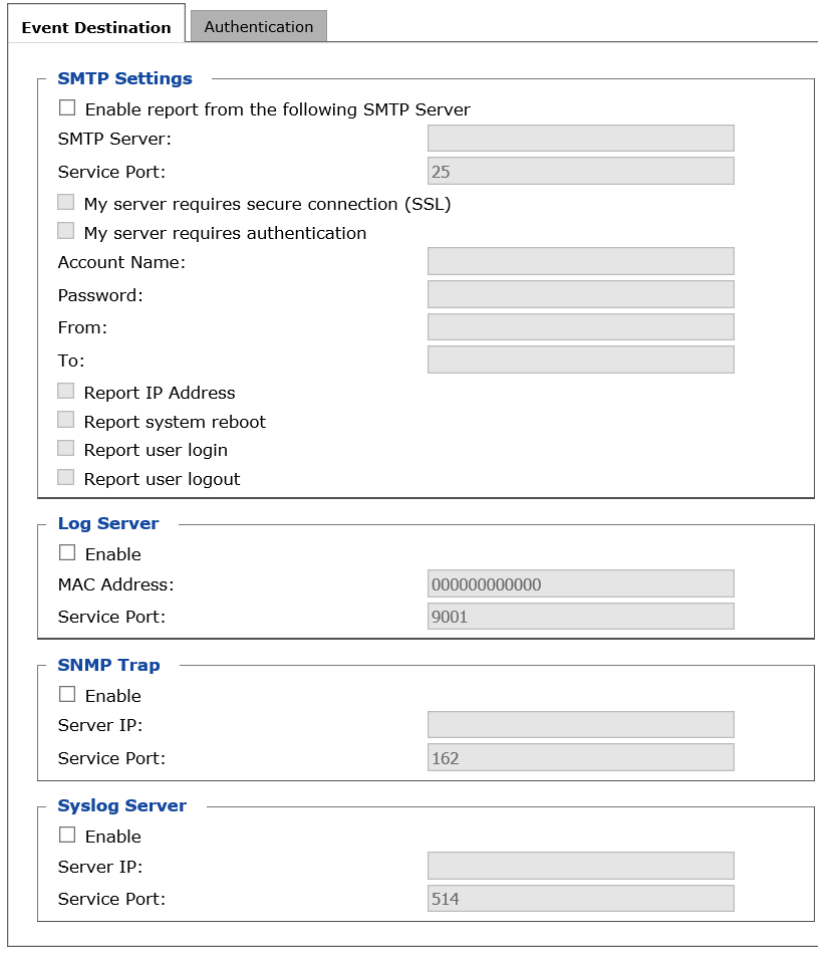
1. Check **Enable**.
2. Enter the hostname that you registered with your DDNS service provider.
3. Drop down the list to select the DDNS service you are registered with.
4. Key in the Username and Password that authenticates you with your DDNS service.
5. In the DDNS Retry Time field, key in how many hours the CN9600 waits before updating the DDNS server.

ANMS

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

Event Destination

This section lets you configure the SMTP, Log Server, SNMP Trap and Syslog Server settings.



■ SMTP Settings

To have the CN9600 email reports from the SMTP server to you, do the following:

1. Check **Enable report from the following SMTP server** and key in the IP address and service port of your SMTP server.
2. If you're connecting to a secure server, check **My server requires secure connection (SSL)**.
3. If your server requires authentication, check **My server requires authentication** and key in the appropriate account information in the **Account Name** and **Password** fields.
4. Key in the email address of where the report is being sent from in the **From** field.

   Note: Only one email address is allowed in the *From* field, and it cannot exceed 64 English alphanumeric character.

5. Key in the email address (addresses) of where you want the SMTP reports sent to in the **To** field.

   Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 English alphanumeric character.

6. Check the information below if you wish to include them in the report email:
   - Report IP Address
   - Report system reboot
   - Report user login
   - Report user logout

■ Log Server

Important operations occur on the CN9600, such as logins and internal status messages, are kept in an automatically generated log file in the Log Server. See Chapter 9, *The Log Server* for details on setting up the log server. The *Log File* is discussed on page 103.

Check **Enable** to enable the Log Server function and specify the **MAC address** and the **Service Port** of the computer the Log Server runs on.

The Log Server will listen for log details.

Note: The valid port range is 1–65535. The default port number is 9001. The port number must different than the one used for the *Program* port (see *Service Ports*, page 32).

■ SNMP Trap

To be notified of SNMP trap events, do the following:

1. Check **Enable SNMP Agent**.
2. Enter the **Server IP** and the **Service Port** of the computer to be notified of SNMP trap events. The valid port range is 1-65535. Default is 162.

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

■ Syslog Server

To record all the events that take place on the CN9600 and write them to a Syslog server, do the following:

1. Check **Enable**.
2. Enter the **Server IP** and the **Service Port** of the Syslog Server. The valid port range is 1-65535. Default is 514.

Authentication

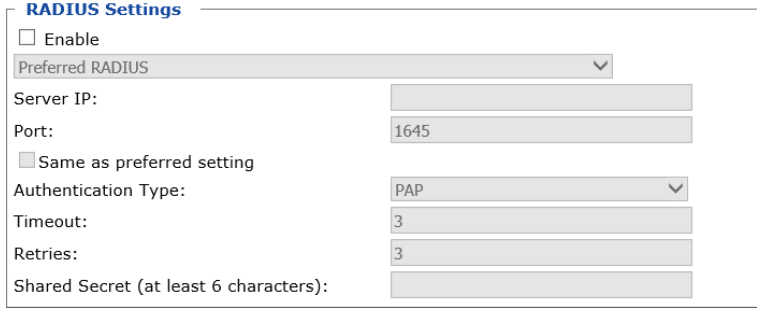
The CN9600 allows log in authentication and authorization through external programs.

This screen lets you configure the RADIUS, LDAP, and CC Management settings.

If you want to use a RADIUS, LDAP, CC Authentication instead of the CN9600 device authentication, check **Disable Device Authentication**. Selecting this option will disable login authentication locally on the CN9600.

■ RADIUS Settings

To allow authentication and authorization for the CN9600 through a RADIUS server, do the following:

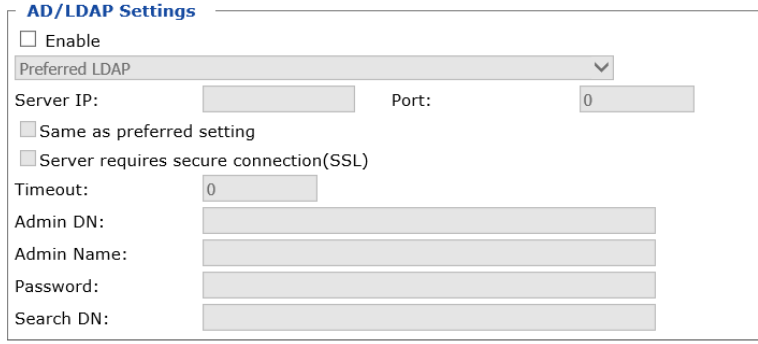


1. Check **Enable**.
2. Click the drop-down menu to select whether you wish to use Preferred RADIUS or Alternate RADIUS.
3. Enter the **Server IP** addresses and **Port** number.
4. Check **Same as preferred setting** if your Alternate RADIUS is the same as the preferred.
5. In the **Timeout** field, set the time in seconds that the CN9600 waits for a RADIUS server reply before it times out.
6. In the **Retries** field, set the number of allowed RADIUS retries.
7. In the **Shared Secret** field, enter the character string that you want to use for authentication between the CN9600 and the RADIUS Server.

■ LDAP Settings

To allow authentication and authorization via LDAP or LDAPS, the Active Directory's LDAP Schema must be extended so that an extended attribute name for the CN9600 – CN9600-*userProfile* – is added as an optional attribute to the person class.

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.



To allow authentication and authorization for the CN9600 via LDAP / LDAPS, refer to the information in the following table.

Item	Action
Enable	Check *Enable* to allow LDAP / LDAPS authentication and authorization.
Preferred / Alternate LDAP	Click for a drop-down menu to select Preferred LDAP or Alternate LDAP.
Server IP	Fill in the IP address and port number for the server. The default port numbers for LDAP and LDAPS are 389 and 636 respectively.
Port	
Timeout (seconds)	Set the time in seconds that the CN9600 waits for an LDAP or LDAPS server reply before it times out.
Admin DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: cn=LDAPAdmin,ou=cn9600,dc=aten,dc=com
Admin Name	Key in the Group Name for CN9600 administrator users.
Password	Key in the LDAP administrator's password.

Item	Action
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. If *Enable Authorization is not checked, this field must include the entry where* the CN9600 *Admin Group is created.* Consult the LDAP / LDAPS administrator to ascertain the appropriate value.

- Use the following keyword for Radius and LDAP setting: **su/[username]** – the username must be a real user account that exists in the local account.
- Use **iKVM50-userProfile** as LDAP attribute and su/[username] as its attribute value.

■ CC Management Settings

To allow authorization for the CN9600 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.

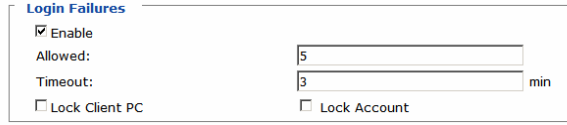
Note: *Authentication* refers to determining the authenticity of the person logging in. *Authorization* refers to assigning permission to use the device's various functions.

Security

The Security screen controls access to the CN9600 and allows you configure the login failure policies, filter settings, encryption settings, security level, working mode, private certificate and certificate signing request.

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.



The meanings of the entries are explained below.

- Login Fail Policy: Select the login failure policy that the CN9600 applies.

  Lock Client PC – If this is enabled, after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No logins from that computer will be accepted. The default is unchecked. This function relates to the client computer's IP. If the IP is changed, the computer will no longer be locked out.

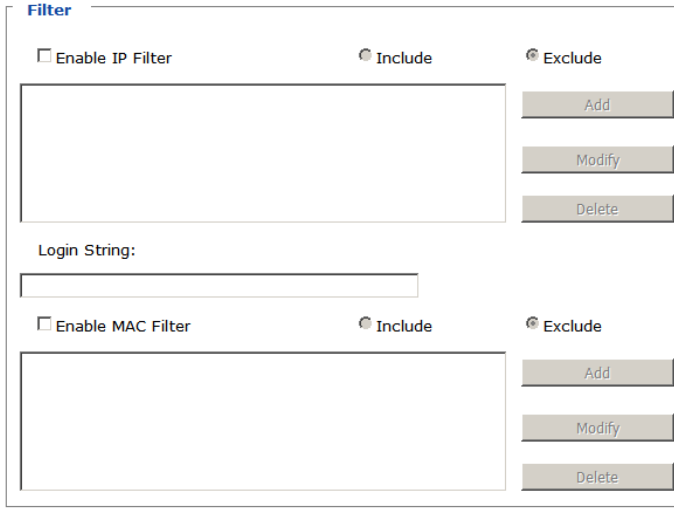
  Lock Account – If this is enabled, after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is unchecked.

- **Allowed –** Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.
- **Timeout –** Sets the amount of time (in minutes) that a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.

Note: If **Login Failures** is not enabled, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.

Filter

IP and MAC Filters control access to the CN9600 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. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.



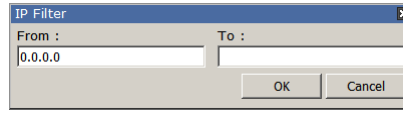
To enable IP and/or MAC filtering, check **IP Filter Enable** and/or **MAC Filter Enable**.

- If the **Include** button is checked, all the addresses within the filter range are allowed access while all other addresses are denied.
- If the **Exclude** button is checked, all the addresses within the filter range are denied access while all other addresses are allowed.

■ Adding Filters

To add an IP filter, do the following:

1. Click **Add**, enter the IP address range you want to filter and click **OK**.



2. 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:

2. Specify the MAC address in the dialog box and click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

Note: 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 words, 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 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 filter list box and click **Delete**.

The Filter section also lets administrators specify a *Login String* that users must include (in addition to the IP address) when they access the CN9600 with a browser. For example:

```
192.168.0.126/CN9600
```

- 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 CN9600 login page using the IP address alone. This makes your installation less secure.

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

Encryption

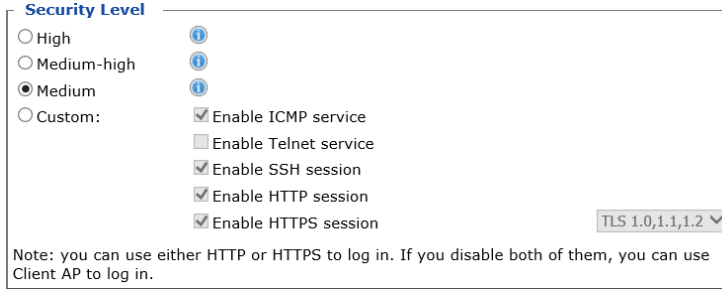
These flexible encryption alternatives for keyboard/mouse, video, and virtual media data let you choose any combination of DES, 3DES, AES, RC4, or a Random cycle of any or all of them.

Enabling encryption will affect system performance – no encryption offers the best performance while the more 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, followed by 3DES or AES
- The RC4 + DES combination offers the least impact of any combination

Encryption

For increased security, you can check or uncheck the boxes to High, Medium - high, Medium or Custom security features.



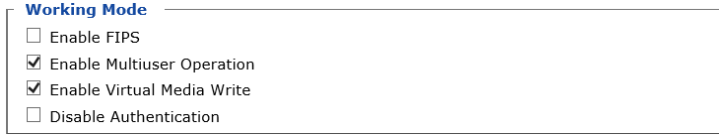
1. High (Disable all services except: SSHv2, HTTPS(TLS v1.2))
2. Medium-high (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.2), ICMP)
3. Medium (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.0, 1.1, 1.2), ICMP) (**Default**)

4. Custom: Click to check the following security options you wish to apply:

- Enable ICMP service
- Enable Telnet service
- Enable SSH session
- Enable HTTP session
- Enable HTTPS session (Select between “TLS 1.2”, “TLS 1.0, 1.1, 1.2”.)

Mode

Use this section to set the working mode parameters.

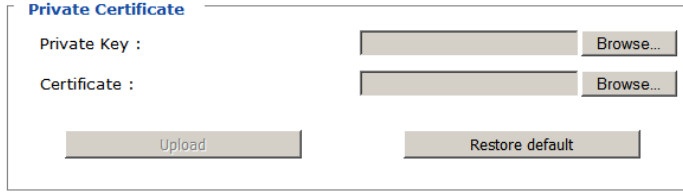


- **Enable FIPS** for FIPS security standard. The default is **Disabled**.
- **Enable Multiuser Operation** to permit more than one user to log into the CN9600 at the same time. The default is **Enabled**.
- **Enable Virtual Media Write** allows redirected virtual media devices on a user’s system to 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**.
- If **Disable Authentication** is checked, no authentication procedures are used to check users attempting to log in. Users gain Administrator access to the CN9600 switch simply by entering combination of username and password. The default is **Disabled**.

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 127 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

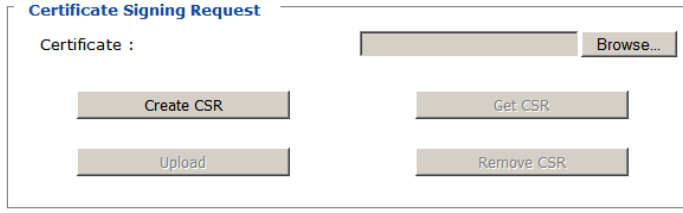
To import the private certificate, do the following:

1. Click **Browse** to the right of **Private Key**, navigate to where your private encryption key file is located and select it.
2. Click **Browse** to the right of **Certificate**, navigate 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.

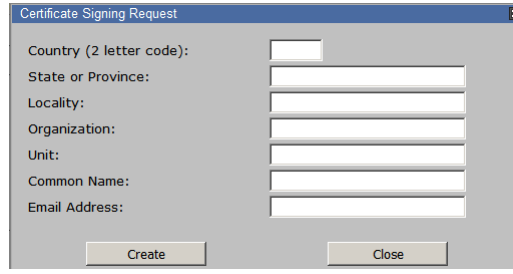
Certificate Signing Request

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:

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	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 *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

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 CN9600.

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 CN9600.

Note: When you upload the file, the CN9600 checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

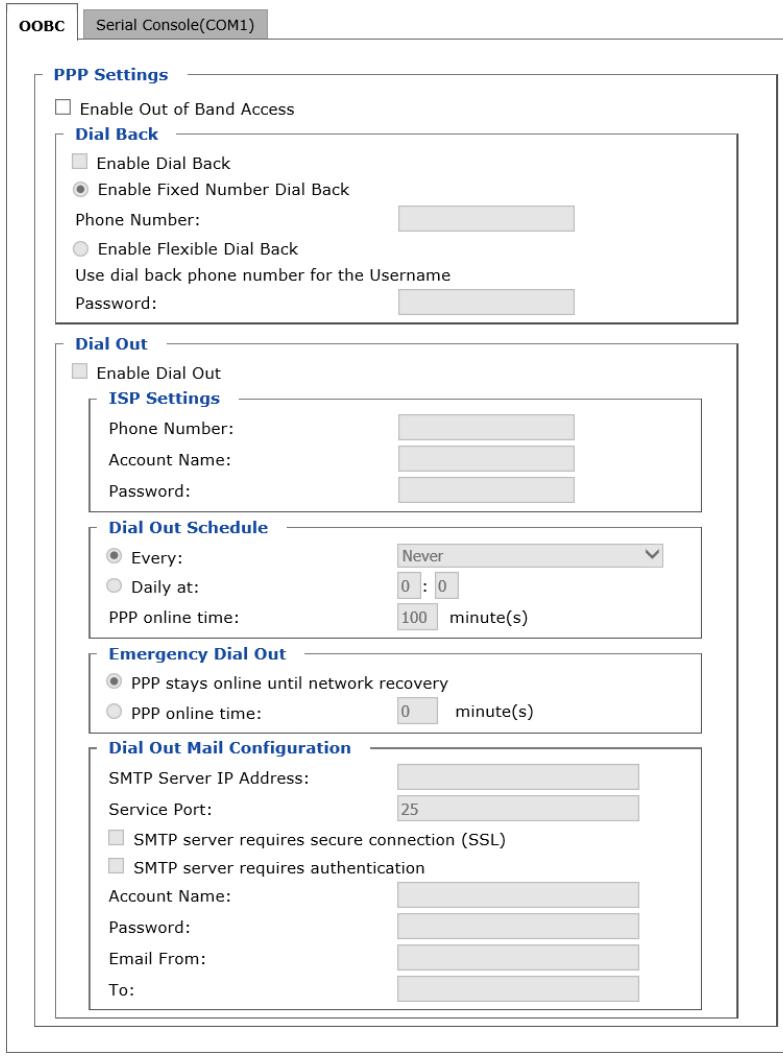
If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Remove CSR**.

Console Management

This section discusses methods of opening the CN9600 console via OOBC (Out of Band Configuration) or serial connection.

OOBC

In case the CN9600 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, check the **Enable Out of Band Access** checkbox.

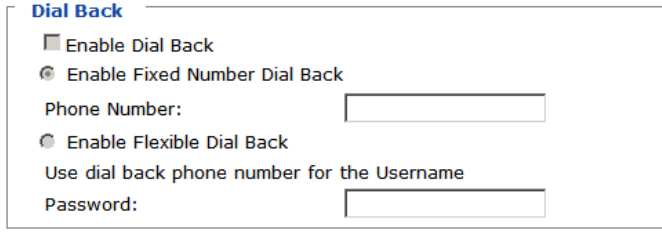


■ PPP Settings

After enabling Out of Band Access, the **Enable Dial Back**, and **Enable Dial Out** functions become available and are described in the following sections.

Dial Back

If this function is enabled, the unit disconnects calls being dialed in, and dials back according to the options specified below:



- **Enable Fixed Number Dial Back**: When enabled, the CN9600 hangs up the modem during an incoming call, and dials back to the modem whose phone number is specified in the Phone Number field.

  Enter the phone number of the modem that you want the CN9600 to dial back to in the **Phone Number** field.

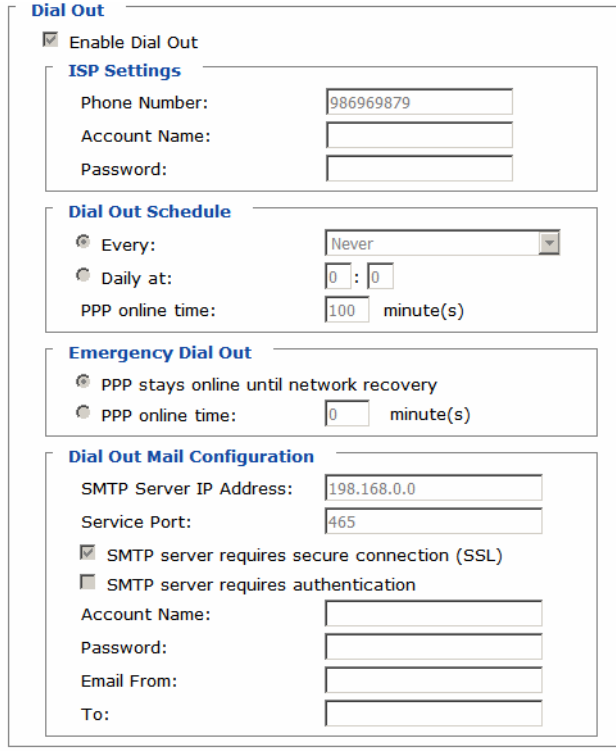
- **Enable Flexible Dial Back:** When enabled, CN9600 dials back to any modem that is convenient for the user.

  Enter the password that the users must specify in the **Password** field.

  When connecting to the CN9600's modem, users will specify the phone number of the modem that they want the CN9600 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 CN9600 to dial out over the ISP connection.
  - **Every** provides a list of fixed times from every hour to every four hours.
    - If you select *Every two hours* (for example), the CN9600 will start dialing out every two hours beginning at 00:00.
    - If you do not want the CN9600 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.
- **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 online.

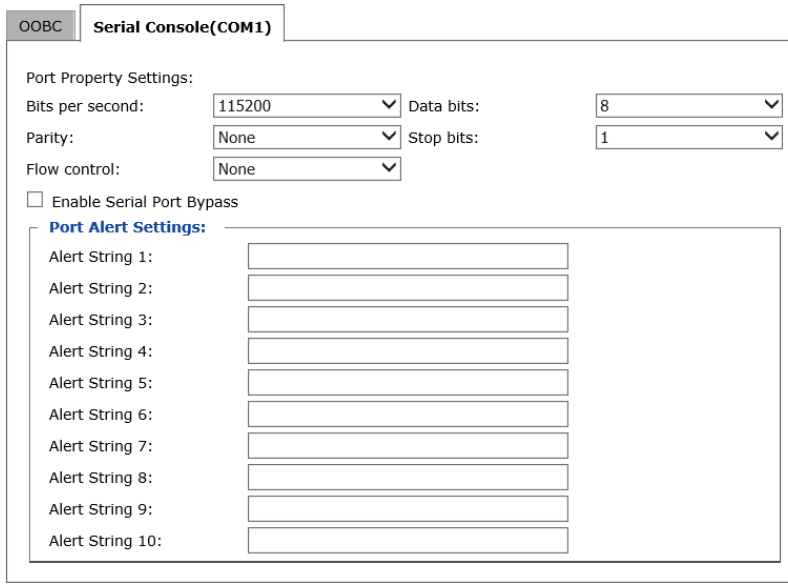
- **Emergency Dial Out:** If the CN9600 gets disconnected from the network, or the network goes down, this function puts the switch online via the ISP dial up connection.
  - If you choose **PPP stays online until network recovery**, the PPP connection to the ISP will last until the network comes back up or the switch reconnects to it.
  - If you choose **PPP online time**, the connection to the ISP will terminate after the specified time. A setting of zero means it is always online.
- **Dial Out Mail Configuration**: This section provides email notification of problems that occur on the devices connected to the CN9600'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.

  - Enter 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, check the **SMTP server requires secure connection (SSL)** checkbox
  - If your server requires authentication, check the **SMTP server requires authentication** checkbox, and enter the appropriate account name and password in the fields below.
  - Enter the email address of the person responsible for the SMTP server (or some other equally responsible administrator) in the **Email From** field.
  - Enter the recipient email address(es) 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.

Serial Console

To configure the CN9600 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*.



Select the values that match the ones used by the connected serial console device. The port property settings that the CN9600 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 115200 (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).

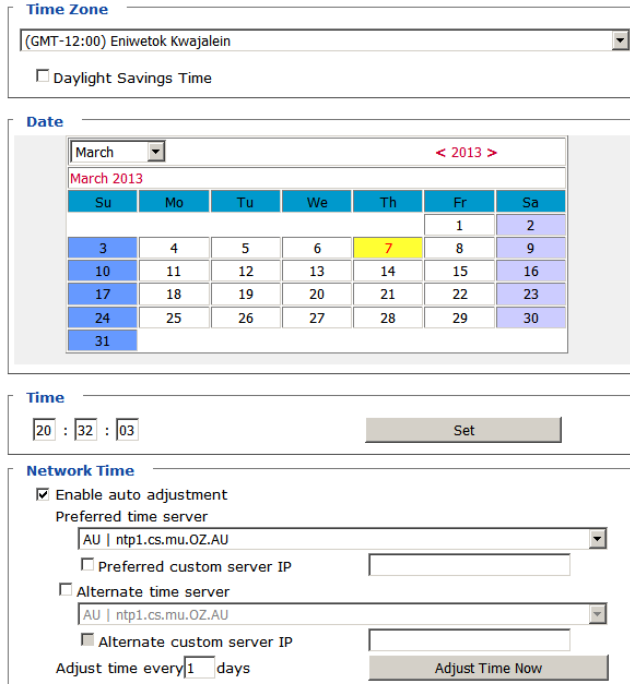
- **Flow Control:** This allows you to choose how the data flow will be controlled. Choices are: None, Hardware, and XON/XOFF. Set this to match the flow control setting of the serial console device. Default is None.

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.

- **Enable Serial Port Bypass**: For DCE and DTE communication (see component 2 & 3 of components on page 9), check this option.
- **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.

Date/Time

The Date/Time dialog page sets the CN9600 time parameters:



Set the parameters according to the information below.

Time Zone

- Use the drop-down menu to select 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 / Time

- 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.
- 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:

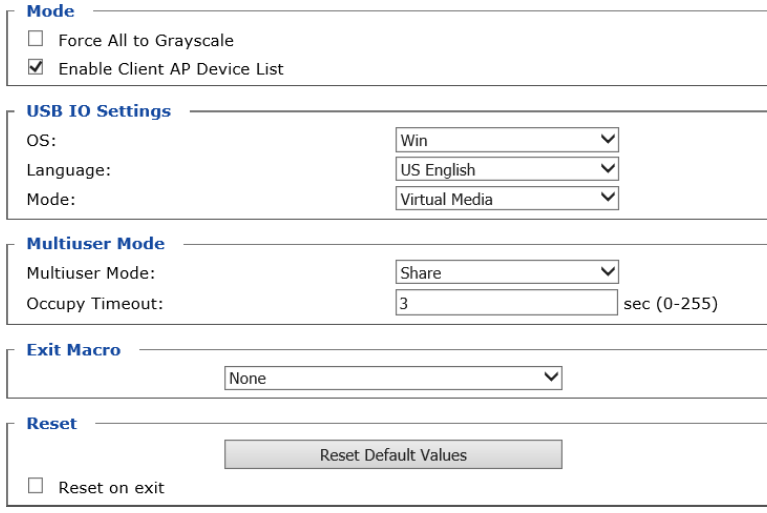
1. Check **Enable auto adjustment**.
2. Click the drop-down menu to select your preferred time server from the time server list

   – or –

   Check **Preferred custom server IP** and enter the IP address of the time server of your choice.
3. If you want to configure an alternate time server, check **Alternate time server** and repeat step 2 for the alternate time server entries.
4. In **Adjust time every days** field, enter a number for the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

Customization

This section provides more customizable options and are described below.



Mode

Check **Force All to Grayscale** to enable this function. When enabled, the remote displays of all devices connected to the CN9600 are changed to grayscale. This can speed up I/O transfer in low bandwidth situations.

Check **Enable Client AP Device List** to enable this function. When enabled, the unit will be discoverable in the Server List when using the WinClient or Java Client AP (see *The Windows Client Viewer*, page 71, and *The Java Client Viewer*, page 97). Disabling this function will render the unit undiscoverable in the Server List but can still be connected to.

USB IO Settings

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.

Mode: The drop-down menu allows you to select whether you would like the system to accept Virtual Media (see *Virtual Media* on page 87 for more details) or to have local Laptop USB Console (LUC) access via the LUC Port (see *Laptop USB Console (LUC)*, page 100).

Multiuser Mode

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 85).

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.

Exit Macro

Click the drop-down menu to select the user created system Exit Macro you would like to use and click **Save**. See *System Macros* on page 101 for details on creating exit macros.

Reset

Click **Reset Default Values** to reset the CN9600 to the default factory settings.

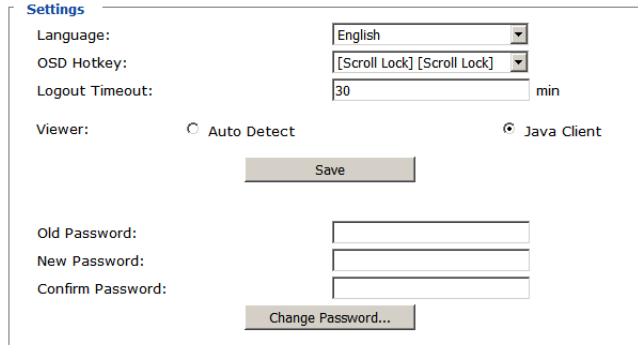
If you wish to reboot the device after you log out, check **Reset on exit**.

Preferences

The following sections describe the administration utilities covered on this section, including the **User Preferences**, **Log Information**, **Remote Console** and **Download** screens.

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.



■ Language

Click the drop-down menu to selects the language that the interface displays in.

■ OSD Hotkey

Select the keyboard combination to call the OSD function.

■ Logout Timeout:

When the session is idling, the time set here determines how long the CN9600 will wait for before terminating the session.

■ 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:

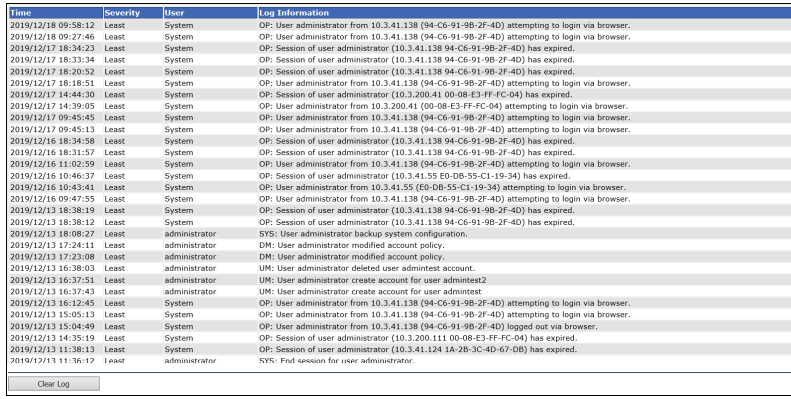
- **Old Password:** Enter the old password.

- **New Password:** Enter the new password.
- **Confirm Password:** Repeat the new password.

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

Logs

The CN9600 logs all the events that take place on it. Following a reset, all logs are cleared. Click **Log Information** to view the logs:



Time	Severity	User	Log Information
2019/12/18 09:58:12	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/18 09:27:46	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/17 18:34:23	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/17 18:33:34	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/17 18:20:52	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/17 18:18:51	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/17 14:44:30	Least	System	OP: Session of user administrator (10.3.200.41 00-08-E3-FF-FC-04) has expired.
2019/12/17 14:39:05	Least	System	OP: User administrator from 10.3.200.41 (00-08-E3-FF-FC-04) attempting to login via browser.
2019/12/17 09:45:45	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/17 09:45:13	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/16 18:34:58	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/16 18:31:57	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/16 11:02:59	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/16 10:46:37	Least	System	OP: Session of user administrator (10.3.41.55 E0-DB-55-C1-19-34) has expired.
2019/12/16 10:43:41	Least	System	OP: User administrator from 10.3.41.55 (E0-DB-55-C1-19-34) attempting to login via browser.
2019/12/16 09:47:55	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/13 18:38:19	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/13 18:38:12	Least	System	OP: Session of user administrator (10.3.41.138 94-C6-91-9B-2F-4D) has expired.
2019/12/13 18:08:27	Least	administrator	SYS: User administrator backup system configuration.
2019/12/13 17:24:11	Least	administrator	DM: User administrator modified account policy.
2019/12/13 17:23:08	Least	administrator	DM: User administrator modified account policy.
2019/12/13 16:38:03	Least	administrator	UM: User administrator deleted user admintest account.
2019/12/13 16:37:51	Least	administrator	UM: User administrator create account for user admintest2
2019/12/13 16:37:43	Least	administrator	UM: User administrator create account for user admintest
2019/12/13 16:12:45	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/13 15:05:13	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/12/13 15:04:49	Least	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) logged out via browser.
2019/12/13 14:35:19	Least	System	OP: Session of user administrator (10.3.200.111 00-08-E3-FF-FC-04) has expired.
2019/12/13 11:38:13	Least	System	OP: Session of user administrator (10.3.41.124 1A-2B-3C-4D-67-DB) has expired.
2019/12/13 11:36:12	Least	administrator	SYS: End session for user administrator.

Clear Log

A maximum of 1024 events are kept in the log file. As new events are recorded, they are placed at the top of the list. When a new event is recorded after there are 1024 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 1024), set up the Log Server AP program. See *The Log Server*, page 105.

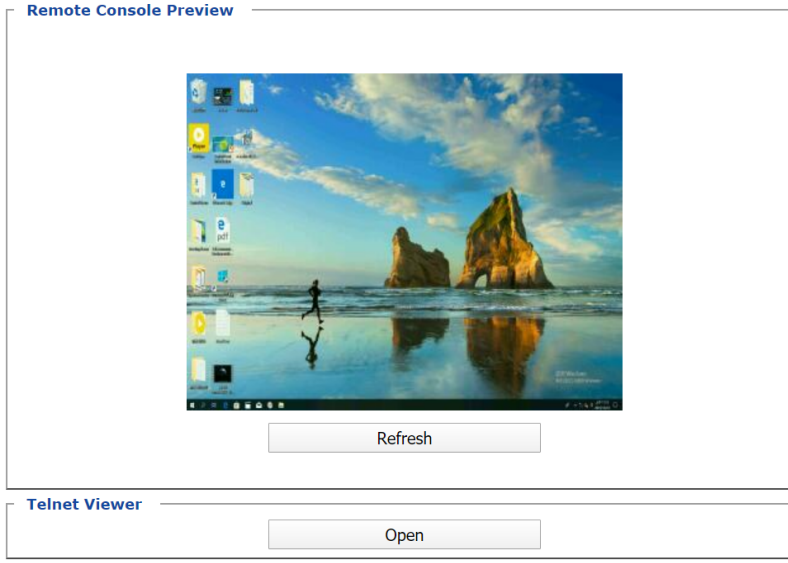
To clear the log file, click on the **Clear Log** icon at the lower right of the page.

Remote Console

This section provides remote console related preference options.

Remote Console Preview

The preview in this screen shows a snapshot of the server's display as follows:



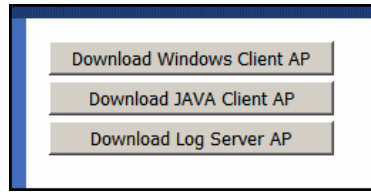
Clicking **Refresh** updates the snapshot of the remote display.

Telnet Viewer

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.

Download

The Download page lets you download the standalone *Windows Client AP*, *Java client AP* and *Log Server AP*.

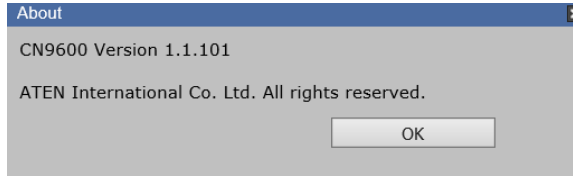


1. Click the button of the AP you want to download.
2. Follow the on-screen instructions to complete the installation and have the program icon placed on your desktop.

- For more information on the *Windows Client AP* and *Java Client AP*, refer to Chapter 5 on page 65.
- For details on the *Log Server AP*, refer to Chapter 9 on page 105.

About

Click *About* to see the current firmware version and copyright information of your CN9600.



Viewer

Click the Viewer icon to view and configure the server's display/monitor in a separate window.

A second or two after you clicking the *Viewer* icon, the remote server's display appears as a window on your desktop. The type of viewer will depend on the preference settings and the type of browser you are using.

Logout

Click the Logout icon when you are done configuring the CN9600's operating environment. This logs you out of the CN9600 GUI.

This Page Intentionally Left Blank

Chapter 5
Accessing Remote Server

Introduction

The remote server can be accessed as if it were your local system. A window will be presented and the remote server is displayed inside this window.

- You can maximize the window, drag the borders to resize the window and 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.

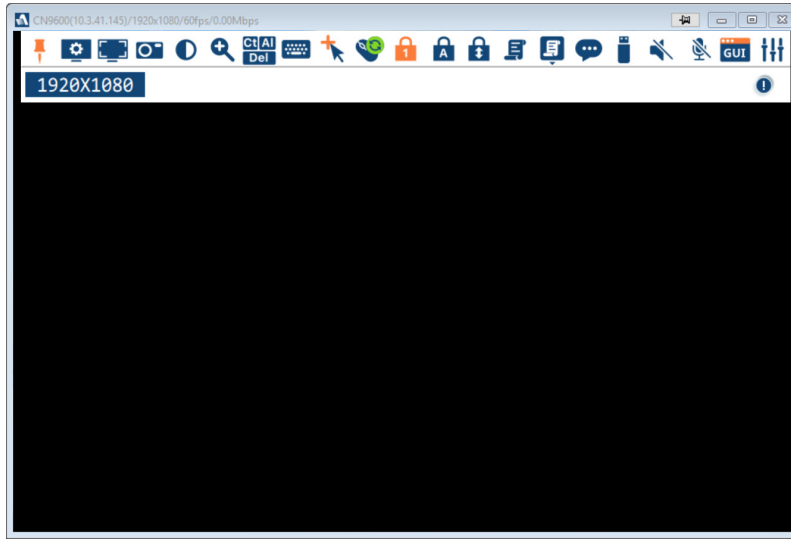
There are several ways you can access the remote servers and are listed below:

1. **Windows viewer** accessed directly from the web browser GUI.
2. **Java viewer** accessed directly from the web browser GUI. Refer to
3. **Windows Client Viewer AP** (without browser). Refer to *The Windows Client AP* on page 67 and *The Windows Client Viewer* on page 71 respectively on how to access the remote server and how to utilize the viewer.
4. **Java Client Viewer AP** (without browser). Refer to *The Java Client AP* on page 70 and *The Java Client Viewer* on page 97 respectively on how to access the remote server and how to utilize the viewer.

To download the Windows Client AP and the Java Client AP from the web GUI. Refer to *Download*, page 62 for more details.

Windows and Java Client Viewer (web access)

The Windows and Java Client Viewer is accessible via a web browser. After you log into the web configuration page (see *Logging In*, page 17), click the **Viewer** icon on the left panel menu. A second or two after, the remote server's display appears as a window on your desktop:



The control/access of the remote server is laid out in the control panel. Refer to *The WinClient Control Panel* on page 71 for access/control information.

By default (where your preference is set to Auto Detect, see *User Preferences*, page 59), if you use Internet Explorer as your browser, the Windows Client viewer is used. If you use other browsers, the Java Client viewer is used.

If you set the preference to Java Client, the Java Client viewer is also used.

The Windows Client AP

The Windows Client AP is a Windows Client program allowing you to access the Windows Client without going through the browser configuration page.

Download

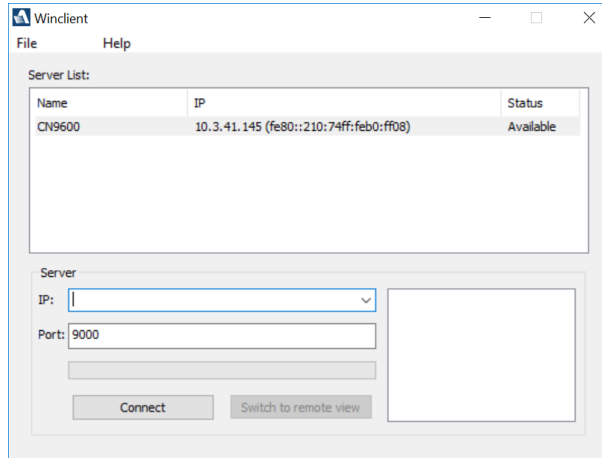
To download the stand-alone Windows Client program, do the following:

1. In the web GUI, go to the Download page. Refer to *Download*, page 62 for more details.
2. Click the **Download Windows Client AP** button.
3. Save the file to a convenient location or create a shortcut on the desktop.

Starting Up

For the first time running the AP, right-click the Windows Client AP and click “Run as administrator” to start.

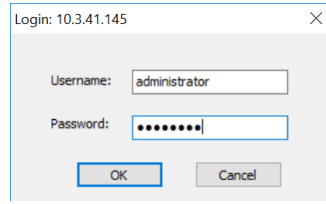
The Windows Client Connection Screen is shown below and each components are described in the table.



Item	Description
Server List	When you run the CN9600 Windows Client program, it automatically searches the user's local LAN segment for CN9600 units, and lists whichever ones it finds in this box. If you want to connect to one of these units, double-click to connect.

Server	If the CN9600 you wish to connect to is at a remote location, it will not be found on your LAN. You can enter its IP address and port yourself. If you don't know the Port number, contact the Administrator. When the IP address and Port number for the unit you wish to connect to have been specified, click **Connect** to start the connection.
Connect	Starts connecting to the CN9600.
Disconnect	These buttons become active once you log into the CN9600. See page 69 for details.
Switch to remote view	
Message panel	The blank field on the right of the Server section shows the current status of the server connection.

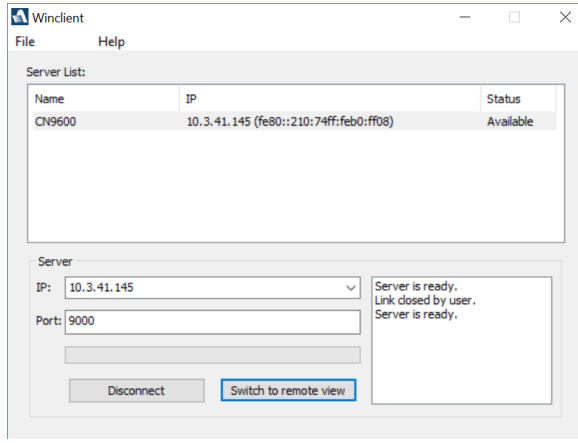
1. Double-click the unit. When the CN9600 is connected to the unit, a login window appears:



2. Provide a valid Username and Password and click **OK** to continue.

Note: The default Username is *administrator* and the default Password is *password*.

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



At this time there are two active buttons and are described in the table below:

Button	Action
Disconnect	Breaks the connection to the CN9600.
Switch to remote view	In some cases, administrators do not wish to have users connect to the CN9600 with a browser. *Switch to remote view* solves this problem as it opens a window on the user's desktop containing the remote server's display that is the same as the one that appears with the browser-based Windows client. Refer to Chapter 6, *The Windows Client Viewer*, for operation details.

3. Click **Switch to remote view** to access the remote server.

Refer to *The WinClient Control Panel* on page 71 for information about the remote access interface.

The Java Client AP

The Java Client AP is an AP program provided to make the CN9600 accessible to all platforms. It is, like the Windows Client AP, a Java Client program allowing you to access the Java Client without going through the browser configuration page.

Systems that have JRE 6 Update 3 or later installed can connect. Java is available for free download from Sun's Java web site (http://java.sun.com).

The Java Client Connection Screen and its connection steps are the same as the Windows Client AP section. Refer to *The Windows Client AP* on page 67 for more details.

Since the control/access of the remote server using the Java Client AP is also the same as the Windows Client, refer to *The WinClient Control Panel* on page 71 for access/control information.

Chapter 6
The Windows Client Viewer

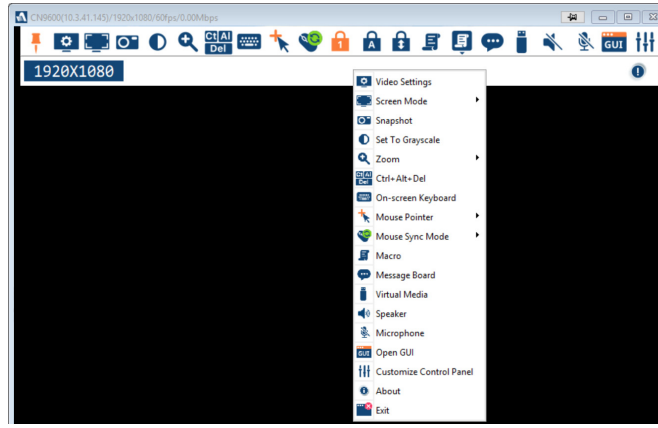
The WinClient Control Panel

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

Note: 1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Control Panel Configuration*, page 97, 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.

- The panel is consisted of two rows.
- The second row shows the video resolution of the remote display, the bus the user is on, and an information button where you can click it for a menu-style version of the control panel toolbar (see below).
- Right clicking the second row area also brings up the menu-style control panel. This menu allows you to select options for the *Screen Mode*, *Zoom*, *Mouse Pointer type*, and *Mouse Sync Mode.* These functions are discussed in the sections that follow.



Control Panel Functions

The Control Panel functions are described in the table below.

Icon	Function
	This is a toggle. Click to ping the Control Panel to the window where it is always displayed on top of other screen elements. Click again to have it display normally.
	Click to bring up the Video Options dialog box. (See *Video Settings*, page 82, for details).
	Toggles the display between *Full Screen Mode* and *Windowed Mode*.
	Click to take a snapshot (screen capture) of the remote display. To configure the Snapshot parameters, refer to *Snapshot* on page 98.
	Click to toggle the remote display between color and grayscale.
	Click to zoom the remote display window. **Note:** This feature is only available in windowed mode (Full Screen Mode is off). See *Zoom*, page 91 for details.
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click to bring up the on-screen keyboard (see *The On-Screen Keyboard*, page 92).
	Click to select the mouse pointer type. **Note:** This icon changes depending on which mouse pointer type is selected (see *Mouse Pointer Type*, page 93).
	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is *Automatic*, a green mark appears on the icon. ◆ When the selection is *Manual*, a red mark appears on the icon. See *Mouse DynaSync Mode*, page 93 for a complete explanation of this feature.

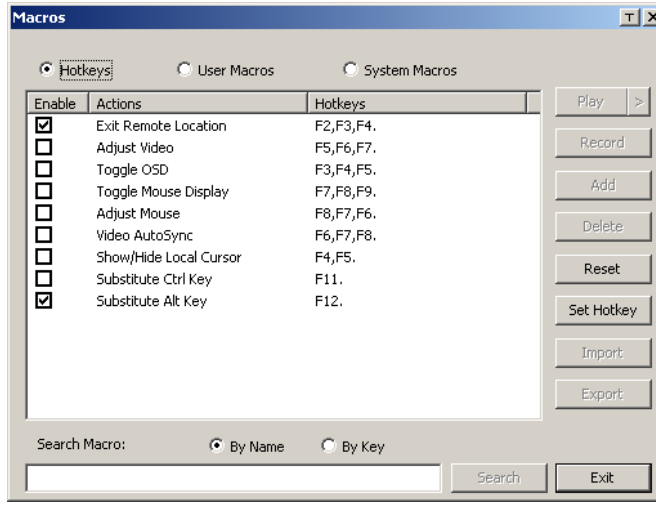
Icon	Function
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is *On*, the LED is bright orange. ◆ When the lock state is *Off*, the LED is dull blue. Click on the icon to toggle the status. **Note:** These icons and your local keyboard 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.
	Click to bring up the Macro dialog box (see *Macros*, page 74 for more details).
	Click to bring up the Message Board (see *The Message Board*, page 85).
	Click to bring up the *Virtual Media* dialog box. The icon changes when a virtual media device is mounted on the port. See *Virtual Media*, page 87, for specific details. **Note:** This icon displays in gray when the function is disabled or not available to the user.
	Click this to turn the speaker on or off.
	Click this to turn the microphone on or off.
	Click to access the viewer-based configuration (see *Open GUI (Configuration)*, page 96).
	Click to bring up the Control Panel Configuration dialog box. See *Control Panel Configuration*, page 97, for details on configuring the Control Panel.

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**.

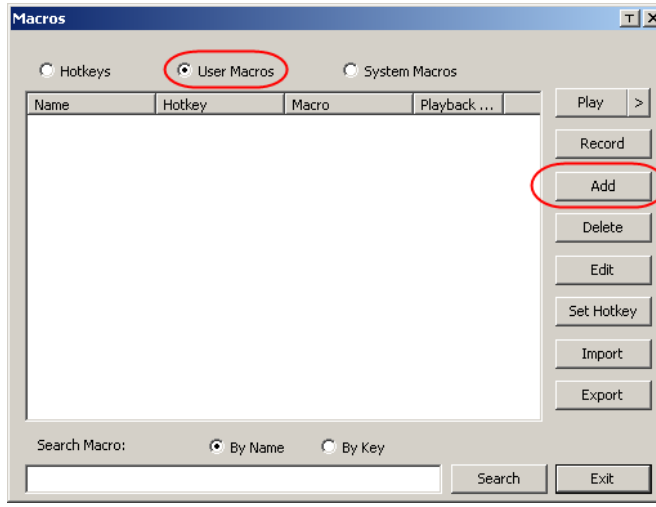
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit remote location	Exits the remote view. This is equivalent to clicking the *Exit* icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	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.
Toggle Control Panel	Toggles the Control Panel **Off** and **On**. The default keys are F3, F4, F5.
Toggle Mouse Display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to 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.
Adjust mouse	This synchronizes the local and remote mouse movements. The default keys are F8, F7, F6.
Video Auto-sync	This combination performs an auto-sync operation. It is equivalent to clicking the *Video Autosync* icon on the Control Panel. The default keys are F6, F7, F8.
Show/Hide Local Cursor	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.
Substitute Ctrl key	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.
Substitute Alt key	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.

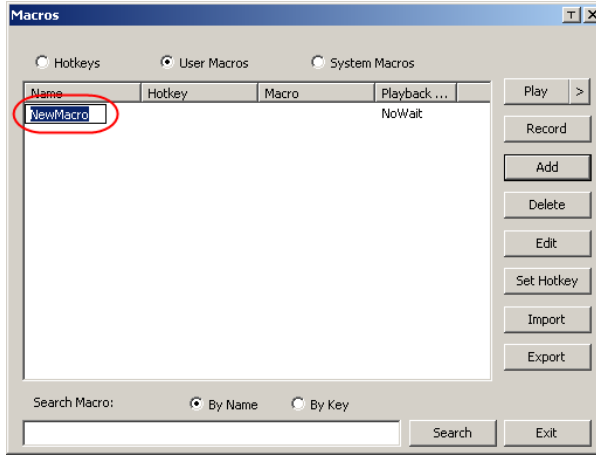
User Macros

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**.

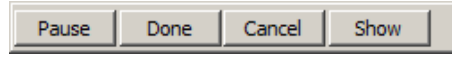


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:

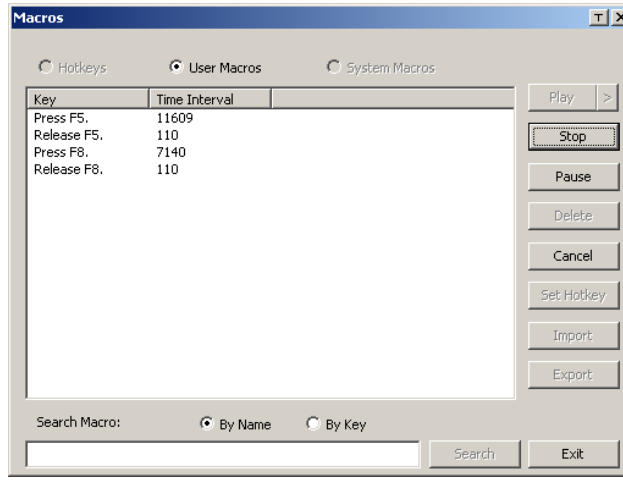


3. Click **Record**.

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



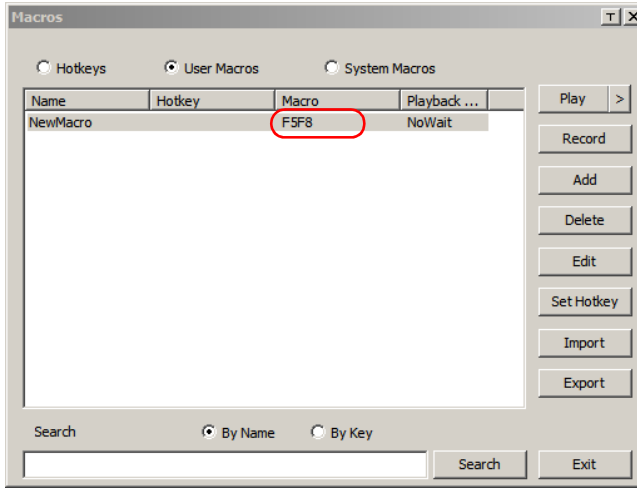
4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes:



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

Note:
- Case is not considered – typing **A** or **a** has the same effect.
- When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
- 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 shown in Step 1:



6. You can give each macro a set of hotkeys, as illustrated in *Hotkeys*, page 74.

7. You can also assign the playback mode and select either **Play Without Wait** (*Nowait)* or **Play with Time Control**.

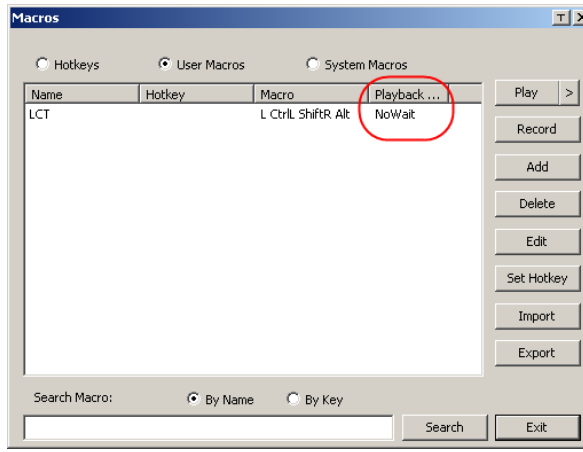
   If you run the macro from this dialog box, you have the option of specifying how the macro runs.

   - If you choose *Play Without Wait*, the macro runs the key presses 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.

8. 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.

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

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 , page 73).
3. By opening this dialog box and clicking **Play**.

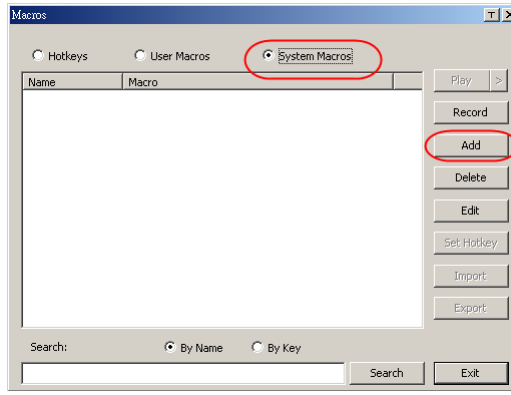
Note: User Macros are stored on the Local Client computer of each user. Therefore there is no limitation on the of number of macros, the size of the macro names, or makeup of the hotkey combinations that invoke them.

Search 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, enter a string for the search and click **Search**. All instances that match your search string appear in the upper panel.

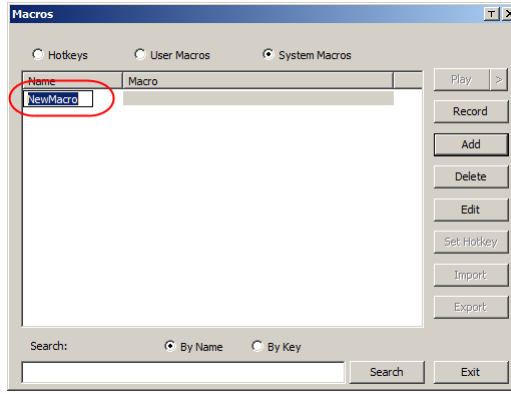
System Macros

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**.

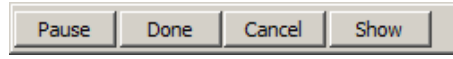


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



3. Click **Record**.

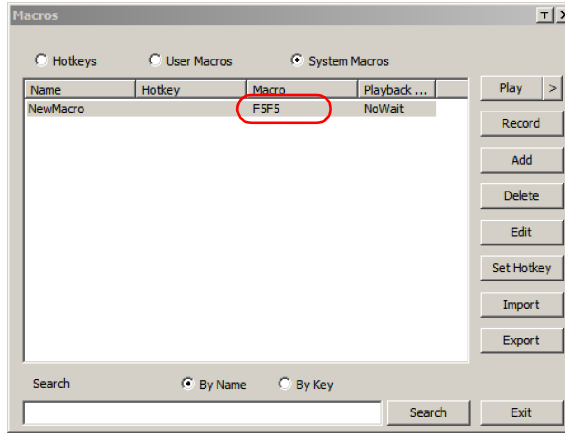
   The dialog box disappears, and a small panel appears at the top left of the screen:



4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** 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 80).

Note:
- Case is not considered – typing **A** or **a** has the same effect.
- When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
- 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:



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.

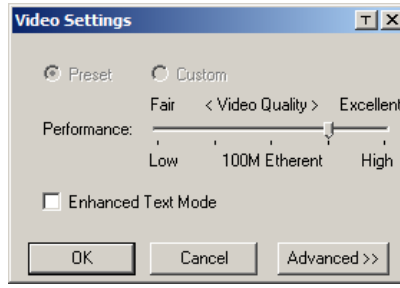
Once the system macros have been created, you can choose to run any one them upon logging out of the CN9600 (see *Customization*, page 56 for details).

Note: 1. Information about the Search function is given on page 79.

2. Systems macros are stored on the CN9600, therefore macro names may not exceed 64 English alphanumeric character, and hotkey combinations may not exceed 256 Bytes (each key usually takes 3–5 Bytes).

Video Settings

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



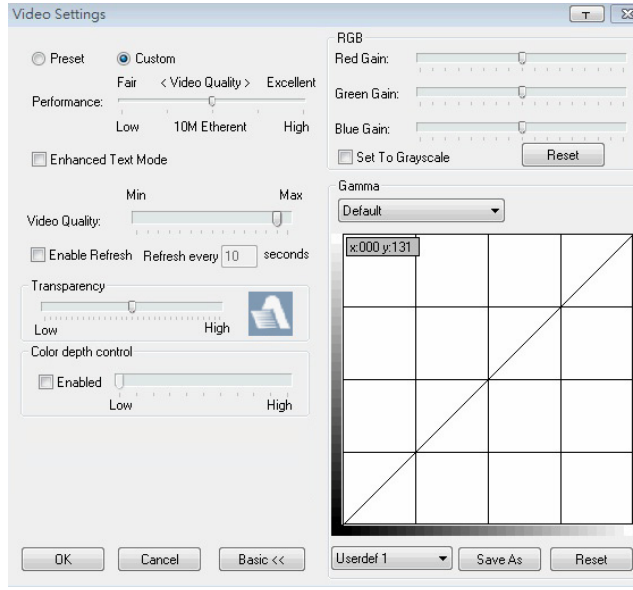
The adjustment options are as follows:

Option	Usage
	Click this to control the transparency of the Video Settings dialog box.
Performance	Select the type of internet connection that exists between the Local Client computer and the CN9600. The CN9600 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.
Enhanced Text Mode	Check this to solve video display problems related to video screen resolution that affect some interface systems (e.g., Sun Blade 1000 servers).
Advanced	See page 83 for details.

Gamma Adjustment

For greater control and if it is necessary to correct the gamma level for the remote video display, use the Gamma function of the **Advanced** Video Settings by clicking the **Advanced** button.

For gamma level, there are ten preset and four user-defined levels to choose from. Click the drop-down menu and choose the most suitable one.



The additional options in the Advanced screen are as follows:

Option	Usage
RGB	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.
Gamma	This section allows you to adjust the video display's gamma level. 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.

Option	Usage
Video Quality	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.
Enable Refresh	The CN9600 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 CN9600 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.
Transparency	Drag the slider bars to adjust the transparency of the remote display.
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.

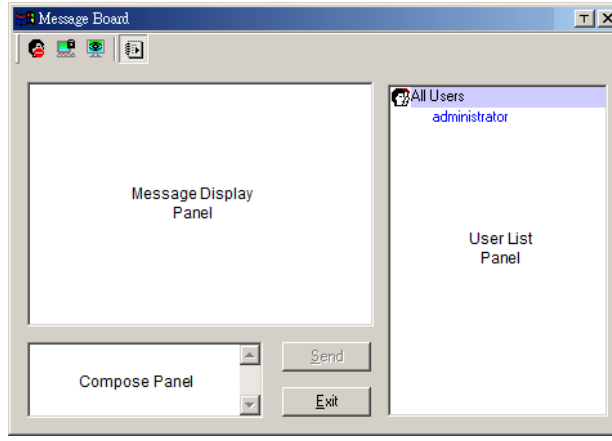
Click **OK** to save your changes and close the dialog box.

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 CN9600 provides a message board that allows users to communicate with each other:



The Button Bar

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

Button	Action
	**Enable/Disable** Chat. When disabled, messages posted to the board are not displayed. The button is shadowed when Chat is disabled. The icon displays next to the user's name in the User List panel when the user has disabled Chat.
	**Occupy/Release** Keyboard/Video/Mouse. 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.
	**Occupy/Release** Keyboard/Mouse. When a port is set to *Occupy* mode (see *Mode*, page 45), 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.
	**Show/Hide** User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.

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 will not appear.

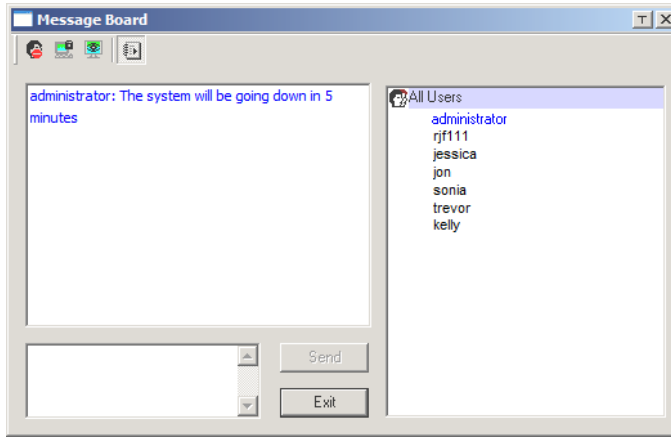
Compose Panel

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 while 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.



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. To enable this function, set the mode under *USB IO Settings*, page 57 to "Virtual Media" first.

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

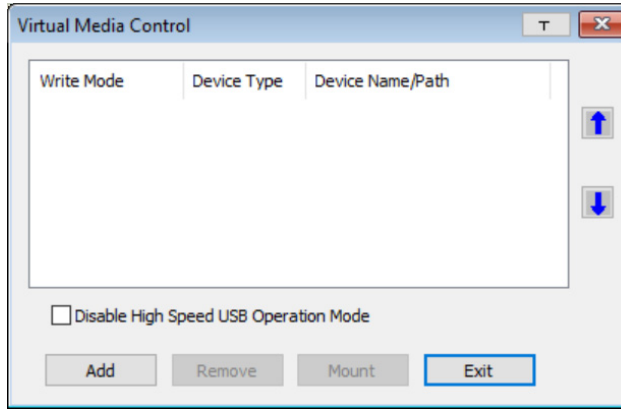
The *Virtual Media* icon on the **Control Panel** changes to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

Icon	Function
	The icon displays as shown on the left to indicate that the virtual media function is disabled or not available.
	The icon displays as shown on the left to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.
	The icon displays as shown on the left to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.

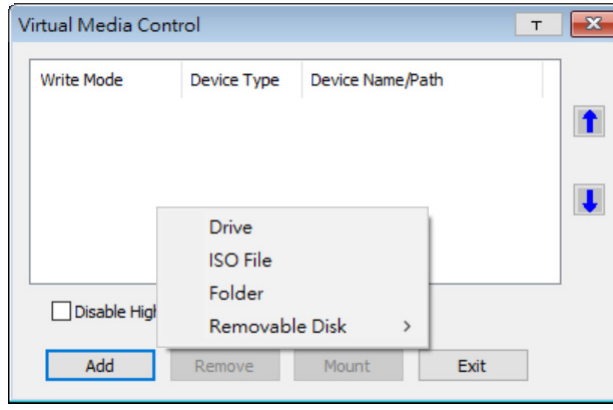
Virtual Media Redirection

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

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



2. Click **Add** and select the media source.



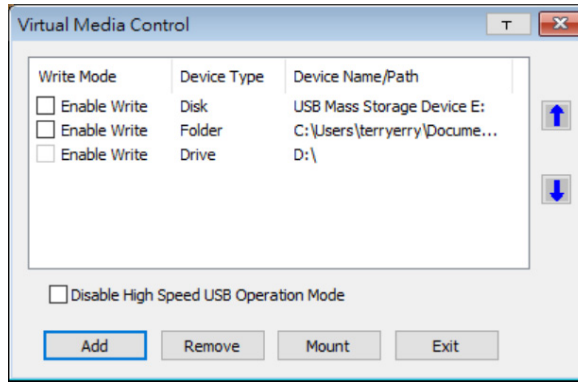
   Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 135 for details about mounting these media types.

3. To add additional media sources, click **Add**, and select the source as many times as you require.

   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, check the *Enable Write* checkbox:

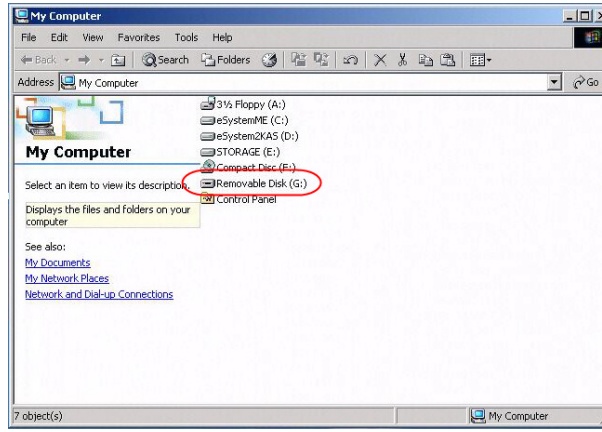


Note: 1. If a redirected device cannot be written to, or if a user does not have write permissions, it appears in gray and cannot be selected.

2. See *Virtual Media Support*, page 135, for a list of supported virtual media types.

5. To remove an entry from the list, highlight it and click **Remove**.

6. 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 system's file system.



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.

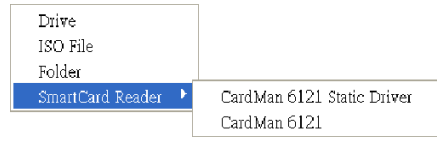
7. To end the redirection, bring up the *Control Panel* and click on the *Virtual Media* icon. All mounted devices are automatically unmounted.

Smart Card Reader

Note: This feature is only available when using the *WinClient Viewer* or the *Windows Client AP*.

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 and click **Mount** to complete the redirection.

Zoom

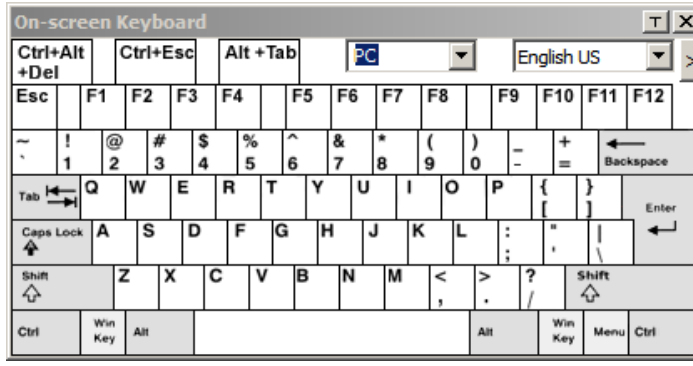
The *Zoom* icon controls the zoom factor for the remote view window. Settings are as follows:

Setting	Description
100%	Sizes and displays the remote view window at 100%.
75%	Sizes and displays the remote view window at 75%.
50%	Sizes and displays the remote view window at 50%.
25%	Sizes and displays the remote view window at 25%.
1:1	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.

The On-Screen Keyboard

The CN9600 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:

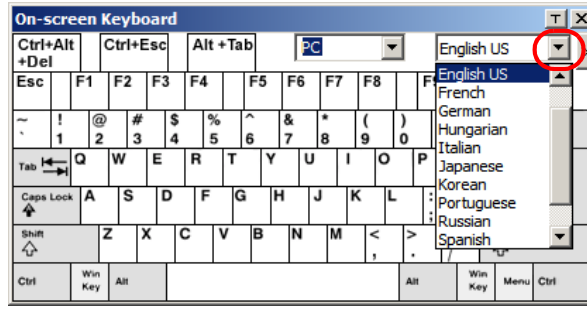


One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems are not the same, you do not have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer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

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

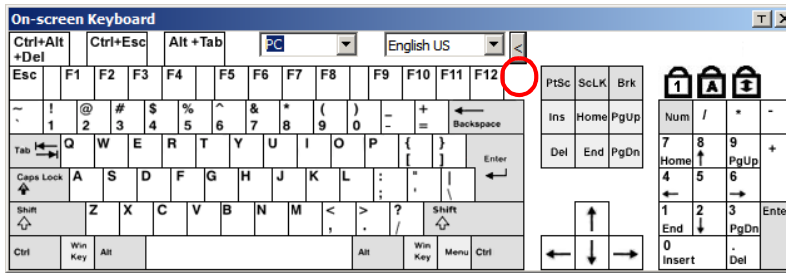
To change languages, do the following:

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



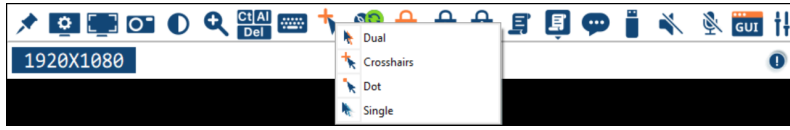
2. Select the new language from the list.

To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.



Mouse Pointer Type

The CN9600 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: 1. Before accessing a port, only Dual and Crosshairs are available for the Windows Viewers. Once the port is accessed, three pointers are available.

2. The Dot pointer is not available with the Java Client Viewer or the Java Client AP.

3. Selecting the Single pointer has the same effect as the *Toggle mouse display* hotkey function (see *Toggle Mouse Display*, page 75 for details).

4. 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.

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

Icon	Function
	The green mark on this icon indicates that Mouse DynaSync is available and is **enabled**. This is the default setting when Mouse DynaSync is available.
	The red mark on this icon indicates that Mouse DynaSync is available but is **not enabled**.

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

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.

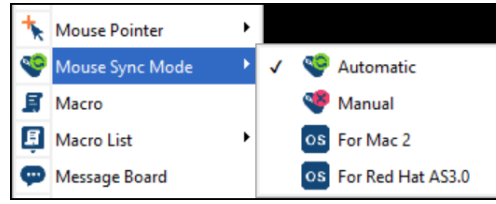
Manual Mouse Synchronization

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. Invoke the **Adjust Mouse** function with the *Adjust Mouse* hotkeys (see *Adjust mouse*, page 75, for details).
2. Move the pointer into all 4 corners of the screen (in any order).
3. Drag the Control Panel to a different position on the screen.
4. Set the mouse speed and acceleration for each problematic computer attached to the switch. See *Additional Mouse Synchronization Procedures*, page 133, for instructions.

Mac and Linux Considerations

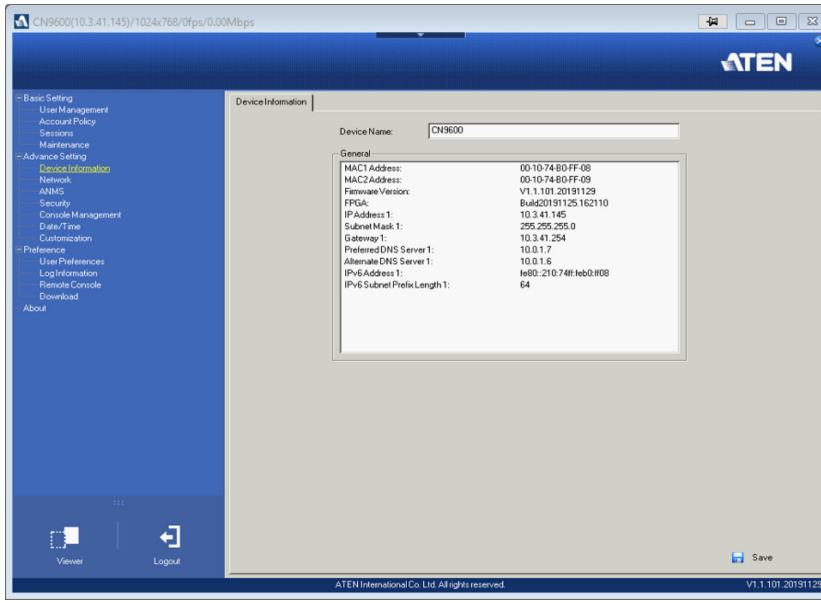
- For Mac OS versions 10.4.11 or later, there is a second DynaSync setting to choose from. If the default Mouse DynaSync result is not satisfactory, try the **Mac 2** setting. To select Mac 2, right click in the text area of the Control Panel and select *Mouse Sync Mode* → *Automatic for Mac 2*:



Linux does not support DynaSync Mode, but there is a setting on the Mouse Sync Mode menu for Redhat AS3.0 systems. If you are using a USB Adapter Cable with an AS3.0 system and the default mouse synchronization is not satisfactory, you can try the Redhat AS3.0 setting. In either case, you must perform the manual mouse synchronization procedures described in the previous section.

Open GUI (Configuration)

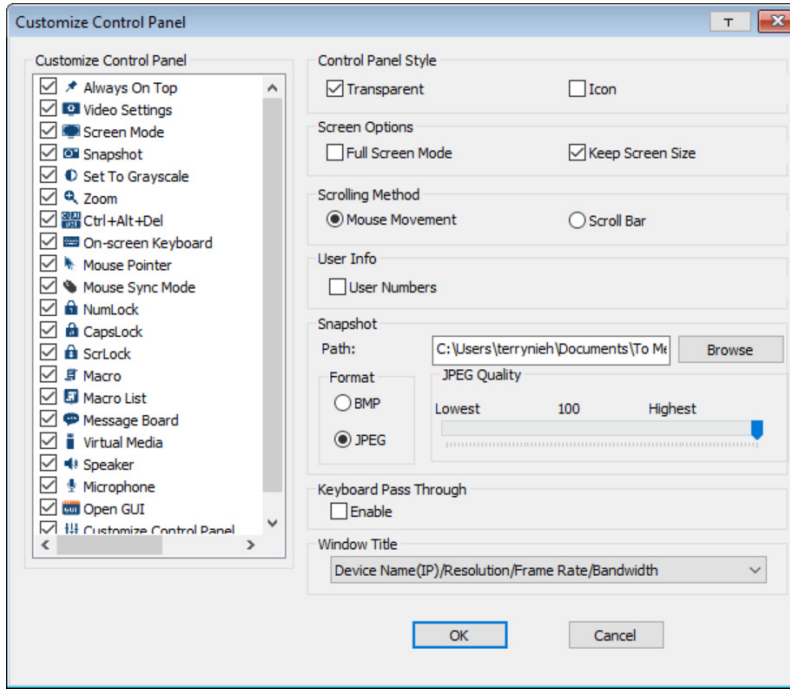
Clicking the *Open GUI* icon for viewer-based configuration.



The sidebar menu items available on this page are based on the user's permissions. For information on how to use these functions, refer to *Configuration* on page 21.

Control Panel Configuration

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 five main sections as described in the table below:

Item	Description
Customize Control Panel	Allows you to select which icons are displayed in the Control Panel.
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 display as an icon until you mouse over it. When you mouse over the icon, the full panel comes up.

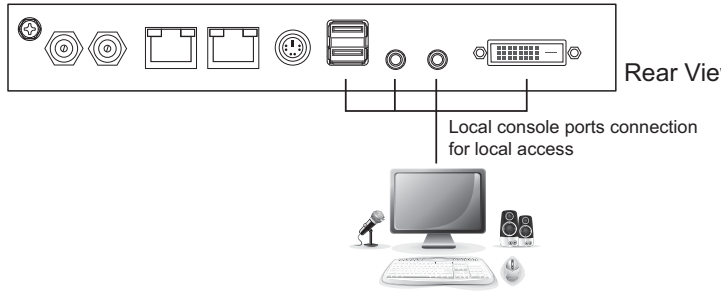
Item	Description
Screen Options	◆ If **Full Screen Mode** is enabled, the remote display fills the entire screen. ◆ If **Full Screen Mode** is not enabled, the remote display appears as a window on the client desktop. If the remote screen is larger than what is able to fit in the window, scroll bars will appear. ◆ If **Keep Screen Size** is enabled, the remote screen is not resized. ◆ If the remote resolution is smaller than that of the client monitor, its display appears like a window centered on the screen. ◆ If the remote resolution is larger than that of the client monitor, its display is scaled to the client monitor size. ◆ If **Keep Screen Size** is not enabled, the remote screen is resized to fit the client monitor's resolution.
Scrolling Method	In cases where the remote screen display is larger than your monitor, you can choose how to scroll to the areas that are off-screen. ◆ If you select *Mouse Movement*, the screen will scroll when you move the mouse pointer to your screen border. ◆ If you select *Scroll Bars*, scroll bars appear around the screen borders that you can use to scroll to the off-screen areas.
User Info	If *User Numbers* is enabled, the total number of users logged into the CN9600 displays beside the resolution on the second row of the Control Panel (See the *Control Panel* diagram on page 71 for an example.)
Snapshot	These settings let the user configure the CN9600's screen capture parameters (see the *Snapshot* description under *The WinClient Control Panel*, page 71): ◆ 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.
Window Title	Use the drop-down menu to select which remote server information is displayed on the window title.

Chapter 7
Local Access

The CN9600 can be accessed directly from a local console's keyboard/mouse/ monitor or via a laptop application (AP) program at the local site.

Local Console

You can directly access the server/computer the CN9600 is connected to by connecting a keyboard, mouse, and monitor to the local console ports of the CN9600.

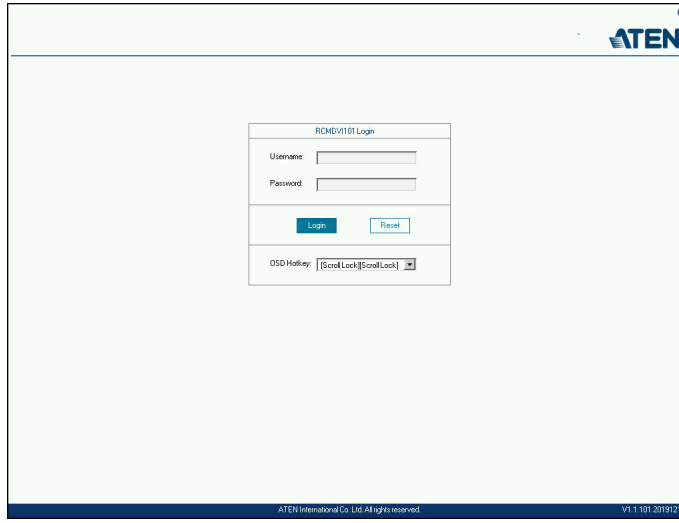


This access is like you using the server/computer directly. The CN9600 is able to split the signal to both the local and remote consoles.

- The local console has priority by default.
- To configure concurrent usage for the local console user and remote console user(s), refer to **Multiuser Mode** on page 57.

If you wish to configure the CN9600, you can press the OSD hot key (**[Scroll Lock] [Scroll Lock]** by default) for the configuration page.

A login page will first appear:



Enter the username and password to enter the configuration page.

The configuration page is the same as the web browser version, refer to *Configuration* on page 21 for more information.

Laptop USB Console (LUC)

The mini USB port can be used as a Laptop USB Console port for laptop access. This lets you conveniently configure the CN9600 directly at the local site simply by connecting a laptop to the port. With the laptop, you can then access and edit the CN9600 application.

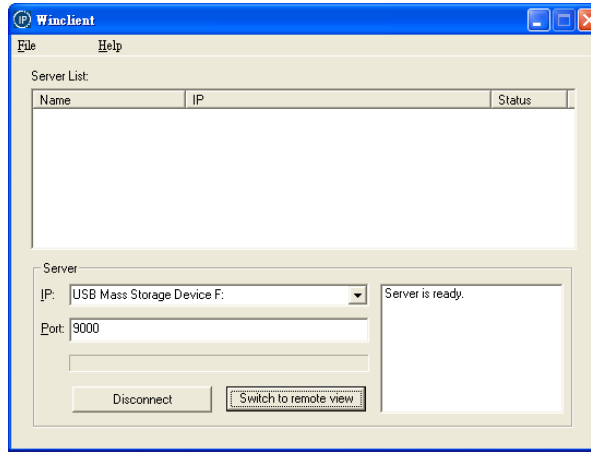
To enable this function, you have to set the *USB IO settings* of CN9600 to LUC mode first. Click the drop-down menu in the CN9600 browser configuration (Configuration location: *Advanced Settings* --> *Customization* --> *USB IO Settings* --> *Mode*) and select Laptop USB Console (LUC) Port.

The laptop application (AP) program for operating the LUC is built into the CN9600's firmware and does not require a download. To access the switch, do the following:

1. Connect your laptop to the CN9600's mini USB port using the USB 2.0 cable (type-A to mini USB) included in the package (see *Hardware Installation*, page 14).

2. The CN9600 appears as a virtual drive in the laptop's file system. Locate the Laptop AP on the virtual CD ROM and double-click the icon. The login screen appears.

3. At the login screen, enter the Username and Password and click **OK**. Once you have connected successfully, the **Switch to Remote View** button becomes active.



4. Click **Switch to Remote View** for the Laptop Console Main Page.

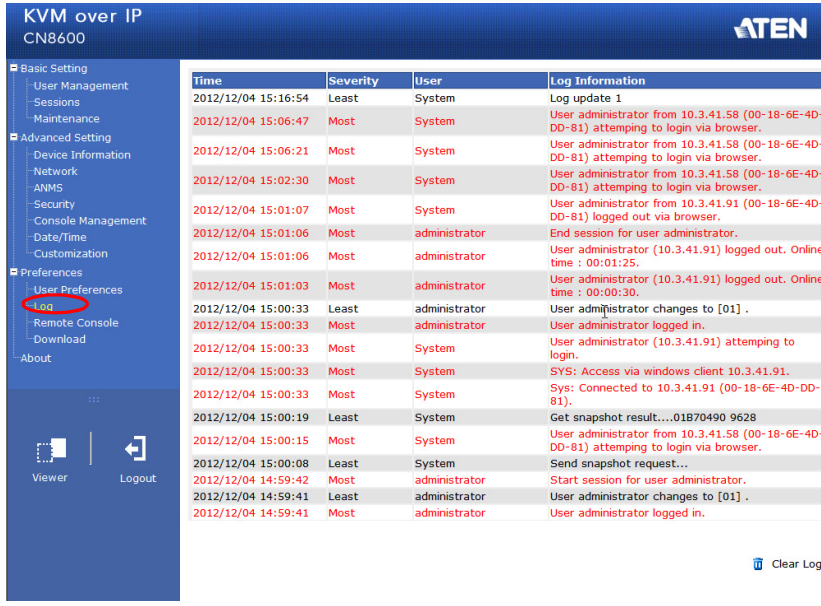
The Laptop Console Main Page is similar to the Web Browser, WinClient and Java Client Main Pages. See *The Windows Client AP*, page 67, for further details, and refer to the AP GUI sections throughout the rest of the manual regarding operations.

This Page Intentionally Left Blank

Chapter 8
The Log File

The Log File Screen

The CN9600 logs all the events that take place on it. Following a reset, all logs are cleared. To view the contents of the log file, click the *Log* icon at the center left of the page. A screen similar to the one below appears:



A maximum of 1024 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 1024 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 1024), set up the Log Server AP program. see *The Log Server*, page 105.

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

This Page Intentionally Left Blank

Chapter 9
The Log Server

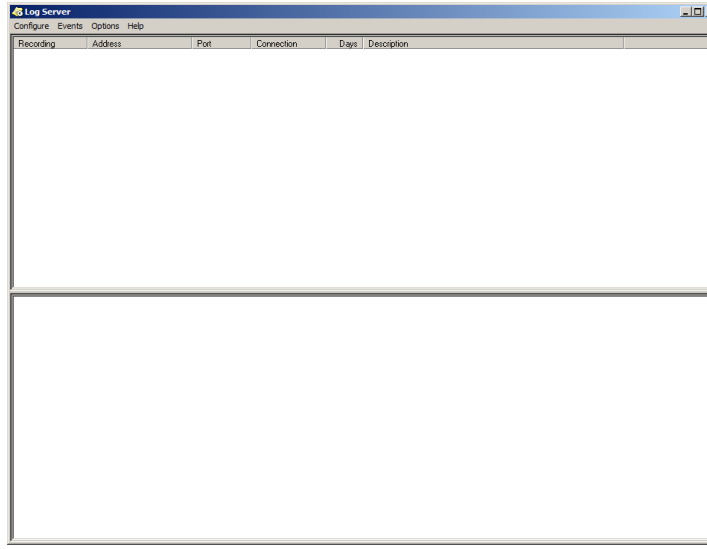
The Log Server is a Windows-based administrative utility that records all the events that take place on selected CN9600 units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. In the web GUI, go to the Download page. Refer to *Download*, page 62 for more details.
2. Click the **Download Log Server AP** button.
3. Follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.

Starting Up

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



Note: 1. The MAC address of the Log Server computer must be specified in the *ANMS* settings – see *Log Server*, page 37 for details.

2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server*, page 132 if the program does not start.

The screen is divided into three components:

- A *Menu Bar* at the top
- A panel that will contain a list of CN9600 units in the middle (see *The Log Server Main Screen*, page 110, for details).
- A panel that will contain an *Events List* at the bottom

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

The Menu Bar

The Menu bar consists of four items:

- Configure
- Events
- Options
- Help

These are discussed in the sections that follow.

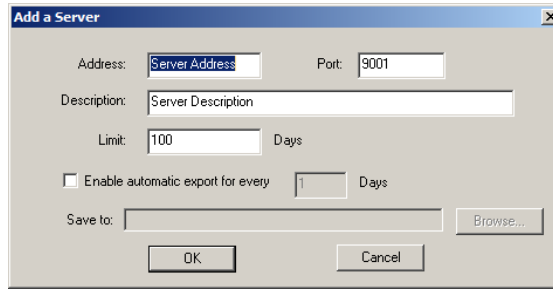
Note: If the Menu Bar appears to be disabled, click in the CN9600 List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new CN9600 units to the CN9600 List, edit the information for units already on the list, or delete CN9600 units from the list.

- To add a CN9600 to the CN9600 List, click **Add**.
- To edit or delete a listed CN9600, first select the one you want in the CN9600 List window, then open this menu and click **Edit** or **Delete**.

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



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

Field	Explanation
Address	This can either be the IP address of the CN9600 or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the CN9600 in the *ANMS* settings (see *ANMS*, page 35).
Port	Key in the port number that was specified for the Log Server's *Service Port* in the *ANMS* settings (see *Log Server*, page 37).
Description	This field is provided so that you can put in a descriptive reference for the unit to help identify it.
Limit	This specifies the number of days that an event should be kept in the Log Server's database before it expires and it is cleared out.
Enable automatic export for every (*) Days	Check this to have the server create a log file at specific intervals (in Days), and save it to your specified location. Click the **Browse...** button and navigate to the file folder where you want the log file to be stored.

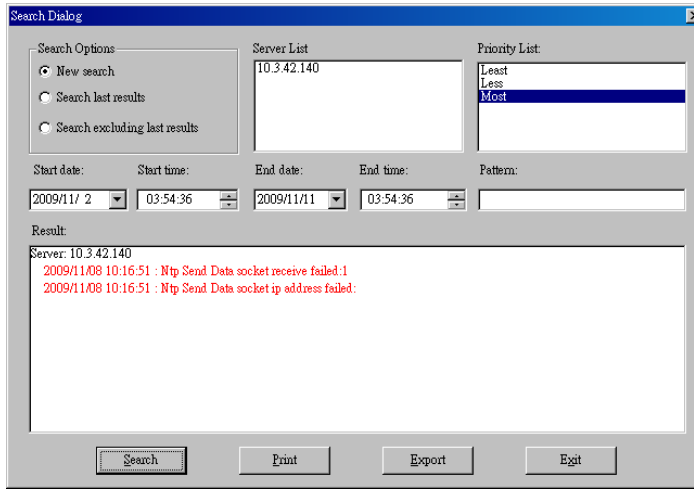
Fill in or modify the fields, then click **OK** to finish.

Events

The Events Menu has two items: *Search* and *Maintenance*.

Search

Search allows you to search for events containing specific words or strings. When you access this function, a screen similar to the one below appears:



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

Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected CN9600.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected CN9600 *excluding* the events that resulted from the last search.
Server List	CN9600 units are listed according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority List	Sets the level for how detailed the search results display should be. *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.

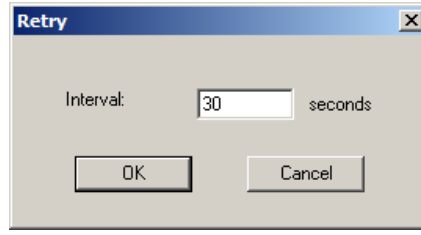
Start Date	Select the date that you want the search to start from. The format follows the YYYY/MM/DD convention, as follows: 2009/11/04
Start Time	Select the time that you want the search to start from.
End Date	Select the date that you want the search to end at.
End Time	Select the time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (*) is supported. E.g., h*ds would match *hands* and *hoods*.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to write the search results to a .txt file.
Exit	Click this button to exit the Search dialog box.

Maintenance

This function allows the administrator to perform manual maintenance of the database, such as erasing specified records before the expiration time that was set with the *Limit* setting of the Edit function (see page 107).

Options

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



Key in the number of seconds, then click **OK** to finish.

Help

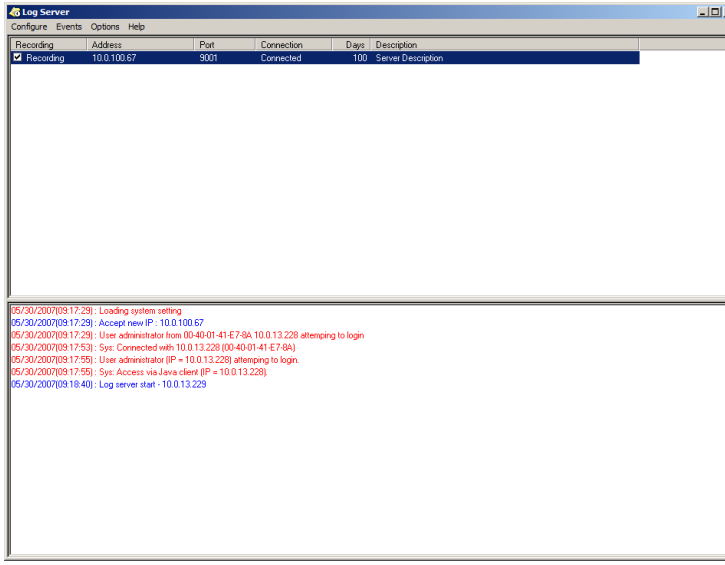
From the Help Menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

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

- The upper (List) panel lists the CN9600 units that have been selected for the Log Server to track (see *Configure*, page 107).
- The lower (Event) panel displays the log events for the currently selected CN9600 (the highlighted one - if there are more than one). To select a CN9600 unit in the list, simply click on it.



The List Panel

The List panel contains six fields:

Field	Explanation
Recording	Determines whether the Log Server records log events for this CN9600 or not. If the Recording check box is checked, the field displays *Recording*, and log events are recorded. If the Recording check box is not checked, the field displays *Paused*, and log events are not recorded. **Note:** Even though a CN9600 is not the currently selected one, if its Recording check box is checked, the Log Server will still record its log events.
Address	This is the IP Address or DNS name that was given to the CN9600 when it was added to the Log Server (see *Configure*, page 107).
Port	This is the port number that was assigned to the CN9600 when it was added to the Log Server (see *Configure*, page 107).
Connection	If the Log Server is connected to the CN9600, this field displays *Connected*. If it is not connected, this field displays *Waiting*. This means that the Log Server's MAC address and/or port number has not been set properly. It needs to be set in the *ANMS* settings (see page 35) and specified in the *Configure* dialog box (see *Configure*, page 107).
Days	This field displays the number of days that the CN9600's log events are to be kept in the Log Server's database before expiration (see *Configure*, page 107).
Description	This field displays the descriptive information given for the CN9600 when it was added to the Log Server (see *Configure*, page 107).

Panel Showing Logs of the Selected Units

The lower panel displays tick information for the currently selected CN9600. Note that if the installation contains more than one switch, even though a switch is not currently selected, if its *Recording* checkbox is checked, the Log Server records its tick information and keeps it in its database.

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.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Inlet power cord selection: Detachable, maximum 2.0 m long, 18 AWG, flexible cord (125V, 10A, 3C, NEMA 5-15P). Or, 0.75mm^2, 3G, flexible cord (E.g.: H05VV-F, 250V 10A).

Rack Mounting

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

Technical Support

International

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

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://eservice.aten.com
Telephone Support		1-888-999-ATEN ext 4988 1-949-428-1111

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.

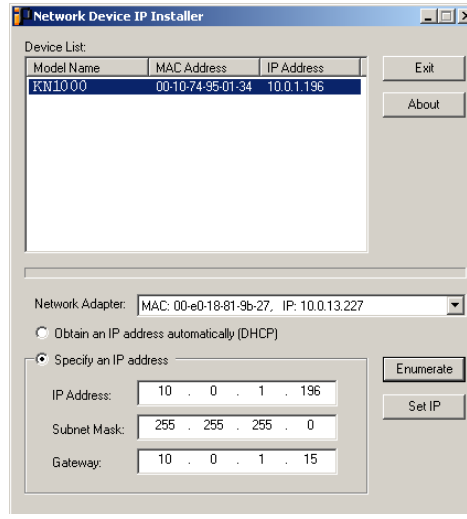
IP Address Determination

If you are an administrator logging in for the first time, you need to access the CN9600 in order to give it an IP address that users can connect to. There are several methods to choose from. In each case, your computer must be on the same network segment as the CN9600. After you have connected and logged in you can give the CN9600 its fixed network address. (See *Network*, page 31.)

IP Installer

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

1. On the CN9600 ATEN website, download the **IP Installer** in the *Support and Downloads* tab.
2. Execute the downloaded file (*IPInstaller.exe*). A dialog box similar to the one below appears:



3. Select the CN9600 in the *Device List*.

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

2. If there is more than one device in the list, use the MAC address to pick the one you want. The CN9600's MAC address is located on its bottom panel.

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

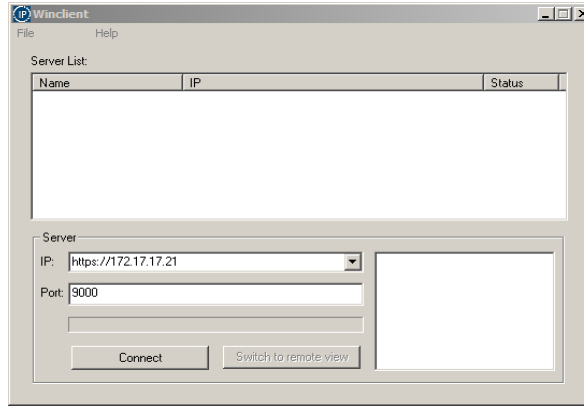
Browser

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

   Where *XXX* represents any number or numbers except 60. (192.168.0.60 is the default address of the CN9600.)
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 CN9600 that is suitable for the network segment that it resides on.
4. After you log out, reset your computer's IP address to its original value.

AP Windows Client

For computers running Windows, the CN9600's IP address can be determined with the Windows AP program (see *The Windows Client AP*, page 67). When you run the program it searches the network segment for CN9600 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 in the **Network** menu. See page 33 for details.

IPv6

At present, the CN9600 supports two IPv6 address protocols: *Link Local IPv6 Address*, and *IPv6 Stateless Autoconfiguration*

Link Local IPv6 Address

At power on, the CN9600 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 CN9600's IPv4 address and click the *Basic Setting* icon. The address is displayed at the bottom of the *Basic Setting* page (see page 22).

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 p. 67).

Note: 1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the CN9600

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 CN9600's network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the CN9600 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 Setting* 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 is shown below and each components are described in the table.*, page 67).

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 CN9600 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.

PC Keyboard	Sun Keyboard	PC Keyboard	Mac Keyboard
[Ctrl] [T]	Stop	[Shift]	Shift
[Ctrl] [F2]	Again	[Ctrl]	Ctrl
[Ctrl] [F3]	Props		
[Ctrl] [F4]	Undo	[Ctrl] [1]	
[Ctrl] [F5]	Front	[Ctrl] [2]	
[Ctrl] [F6]	Copy	[Ctrl] [3]	
[Ctrl] [F7]	Open	[Ctrl] [4]	
[Ctrl] [F8]	Paste	[Alt]	Alt
[Ctrl] [F9]	Find	[Print Screen]	F13
[Ctrl] [F10]	Cut	[Scroll Lock]	F14
[Ctrl] [1]			=
[Ctrl] [2]		[Enter]	Return
[Ctrl] [3]		[Backspace]	Delete
[Ctrl] [4]		[Insert]	Help
[Ctrl] [H]	Help	[Ctrl] 	F15
	Compose		
	◆		

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

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.

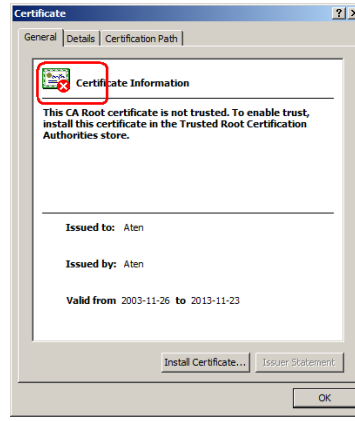
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- 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:

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



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

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

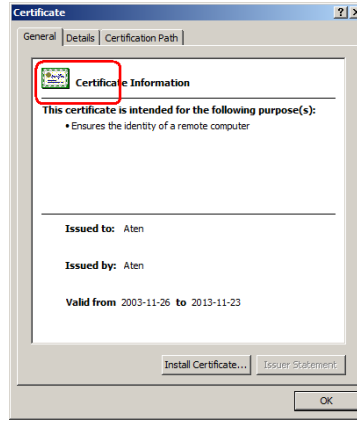
Click **Yes**.

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

Certificate Trusted

The certificate is now trusted:

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



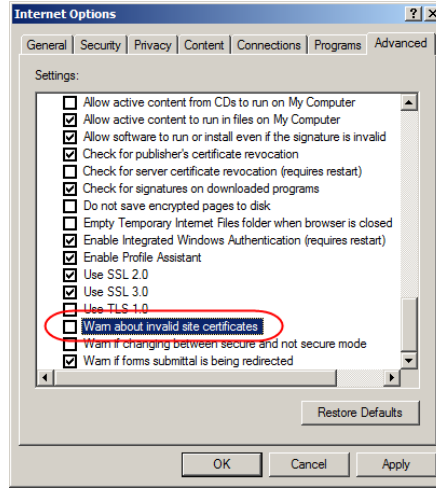
Mismatch Considerations

If the site name or IP address used for generating the certificate no longer matches the current address of the CN9600 a mismatch warning occurs:

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*:



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:

```
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

```
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=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
```

```
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 46).

Troubleshooting

General Operation

Problem	Resolution
Erratic operation	The CN9600 needs to be started before the KVM switch 1. If the CN9600 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 CN9600, reset or restart the KVM switch.
	The CN9600 needs to be reset (see *Upgrade Main Firmware*, page 26, point 1).
I can't access the CN9600, even though I have specified the IP address and port number correctly.	If the CN9600 is behind a router, the router's *Port Forwarding* (also referred to as *Virtual Server*) feature must be configured. See *Port Forwarding*, page 121, 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 75 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 82) so that less video data is transmitted.
Changing Mouse Sync Mode to Manual makes the CN9600 crash.	The CN9600 has not crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the CN9600 to get it going right away (see *Upgrade Main Firmware*, page 26, point 1).
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 do not click **Apply**, the CN9600 is not 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 CN9600 and reset the timeout counter.
The Windows Client link does not appear in the *Remote Console Display* when I log in with Firefox.	The Windows Client link requires ActiveX. Since Firefox does not 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 CN9600 with a browser; open a viewer; on the control panel set *Mouse DynaSync* to **Manual**. See page 93 for details.

Windows

Problem	Resolution
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 123, 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 46).
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 126 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 93). 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 82), to sync the local and remote monitors. 3. If that does not resolve the problem, use the *Adjust Mouse* feature (see *Adjust mouse*, page 75) to bring the pointers back in step. 4. If the above fails to resolve the problem, refer to *Additional Mouse Synchronization Procedures*, page 133, for further steps to take.
Part of remote window is off my monitor.	Use the *AutoSync* feature (see *Video Settings*, page 82), to sync the local and remote monitors.
Virtual Media does not 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 CN9600 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 100, *Mouse DynaSync Mode*, page 107, and *Sun / Linux*, page 134. For other problems, see the table below:

Problem	Resolution
Java Applet won't connect to the CN9600	1. Java 6 Update 3 or higher must be installed on your computer. 2. Make sure to include the correct login string when you specify the CN9600's IP address. 3. Close the Java Applet, reopen it, and try again.
I have installed the latest Java JRE, but I am having performance and stability problems.	There may be issues with the latest version because it is so new. Try using a Java version that is one or two updates earlier than the latest one.
Java Applet performance deteriorates.	Exit the program and start again.
National language characters don't appear.	Use the CN9600'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 106.)
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 123, for details.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g., Sun Blade 1000 servers).[1]	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to **OK mode** and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
Video display problems with 13W3 interface systems (e.g., Sun Ultra servers).*	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to **OK mode** and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
The local and remote mouse pointers do not sync	The default configuration is for the local and remote mouse pointers to automatically sync when you connect. Automatic mouse sync only supports USB mice on Windows and Mac (G4 or higher) systems, however. You must select *Manual* as the *Mouse DynaSync Mode* choice, and sync the pointers manually. See *Mouse DynaSync Mode*, page 93 for further details.

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

Mac Systems

Problem	Resolution
The local and remote mouse pointers do not sync.	There are two USB I/O settings for the Mac: Mac 1, and Mac 2 (see *Customization*, page 56). 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.
When I log in to the switch with my Safari browser, it hangs when I use the Snapshot feature.	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.

The Log Server

Problem	Resolution
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows ME, 2000 and XP. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com/data/download.htm to retrieve the driver file: MDAC 2.7 RTM Refresh (2.70.9001.0) Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Additional Mouse Synchronization Procedures

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

Windows:

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

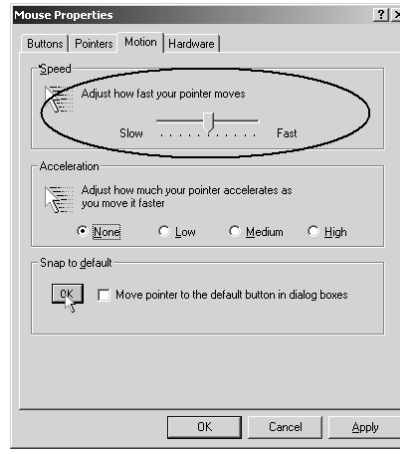
1. Windows 2000:

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

   b) Click the *Motion* tab

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

   d) Set the mouse acceleration to *None*



2. Windows XP / Windows Server 2003 / Windows 7 / Windows 8 / Windows 10:

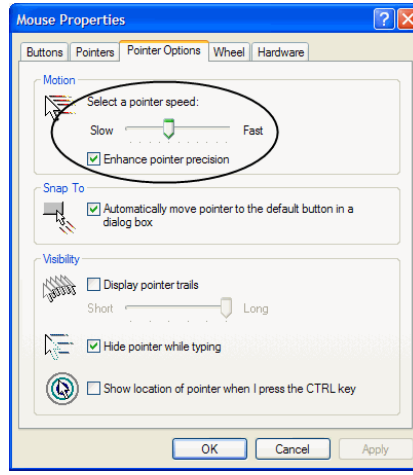
   a) Open the Mouse Properties dialog box (Control Panel → Mouse)

   (For Windows 10, click Start → Devices → Mouse → Additional mouse options)

b) Click the *Pointer Options* tab

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

d) Disable *Enhance Pointer Precision*



3. Windows ME:

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

4. Windows NT / Windows 98 / Windows 95:

   Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`
`or`
`xset m 1`

(If one does not help, try the other.)

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 87). 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

Note: 1. The Java Client supports Virtual Media in the same way as WinClient does – however, the account should have Administrator level privilege.

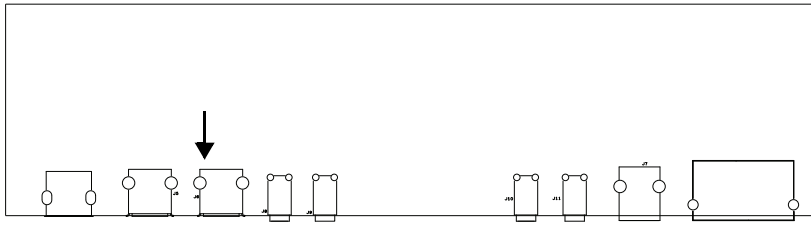
2. Folder mapping uses a FAT16 file system, so there is a 2G limitation. Virtual Media only supports ISO files less than 4G.

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 CN9600, disconnect the power cord from its inlet, and remove its housing.
2. Use a jumper cap to short the jumper on the mainboard labeled **J15**.



3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from **J15**.
6. Close the housing and power on the CN9600.

   After you start back up, you can use the default Username and Password (see page 18, and page 68) to log in.

Specifications

Connectors	
Console Ports	2 x USB Type A Female (White) 1 x DVI-D Female (White) 1 x 3.5mm Audio Jack Female (Green) 1 x 3.5mm Audio Jack Female (Pink)
KVM Ports	1 x USB Type B Female (White) 1 x DVI-D Female (White) 1 x 3.5mm Audio Jack Female (Green) 1 x 3.5mm Audio Jack Female (Pink)
LAN Ports	2 x RJ-45 Female
Virtual Media	1 x USB Mini-B Female
Power	2 x DC Jack
Serial Port	2 x RJ-45 Female
Control Port	1 x PS/2 Female
Switches	
Reset	1 x Semi-recessed pushbutton (Black)
Emulation	
Keyboard/Mouse	USB
LEDs	
Power	1 (Green)
Video	
Local Console & Remote	1920 x 1200 @ 60Hz
Power Consumption	
DC 5V: 5.55W: 30BTU	
Environment	
Operating Temperature	0–50ºC (CN9600) 0–40ºC (Power Adapter)
Storage Temperature	–20–60ºC
Humidity	0–80% RH, Non-condensing
Physical Properties	

Housing	Metal
Weight	0.84 kg (1.85 lb)
Dimensions (L x W x H)	20.00 x 15.49 x 2.85 cm (7.87 x 6.1 x 1.12 in.)

Limited Warranty

ATEN warrants its hardware in the country of purchase against flaws in materials and workmanship for a Warranty Period of two [2] years (warranty period may vary in certain regions/countries) commencing on the date of original purchase. This warranty period includes the LCD panel of ATEN LCD KVM switches. Select products are warranted for an additional year (see *A+ Warranty* for further details). Cables and accessories are not covered by the Standard Warranty.

What is covered by the Limited Hardware Warranty

ATEN will provide a repair service, without charge, during the Warranty Period. If a product is detective, ATEN will, at its discretion, have the option to (1) repair said product with new or repaired components, or (2) replace the entire product with an identical product or with a similar product which fulfills the same function as the defective product. Replaced products assume the warranty of the original product for the remaining period or a period of 90 days, whichever is longer. When the products or components are replaced, the replacing articles shall become customer property and the replaced articles shall become the property of ATEN.

To learn more about our warranty policies, please visit our website:

http://www.aten.com/global/en/legal/policies/warranty-policy/