



CN800

USB VGA KVM over IP Mini
User Manual

Compliance Statements

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.

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

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.

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.



KCC Statement:

우선 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.

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.

CAN ICES (A) / NMB (A)

VCCI Statement

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI - A

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.

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

Package Contents

Check to make sure that all the components are in working order. If you encounter any problem, please contact your dealer.

CN800

- ♦ 1 CN800 USB VGA KVM over IP Mini
- ♦ 1 user instructions

Contents

Compliance Statements	ii
User Information	iv
Online Registration	iv
Telephone Support	iv
User Notice	iv
Product Information	v
Package Contents	vi
CN800	vi
Contents	vii
About This Manual	xii
Conventions	xiii

1. Introduction

Overview	1
Features and Benefits	2
Hardware	2
Management	2
Easy-to-Use Interface	2
Advanced Security	3
Virtual Media	3
Virtual Remote Desktop	3
System Requirements	4
Remote User Computers	4
Servers	4
Cables	4
Supported Video Resolutions	5
Operating Systems	5
Browsers	6
Components	7
CN800	7

2. Hardware Setup

Rack Mounting	10
Securing the CN800 using a cable tie	10
Securing the CN800 using a screw and a cage nut	10
Securing the CN800 using a magic tape	11
Installation	12
Installation Diagram	12

3. Browser Login

Logging In	13
Main Screen	15

4. Configuration

Introduction	17
Basic Setting	18
User Management	18
User Information	18
Role	18
Permissions	19
Sessions	20
Maintenance	21
Upgrade Main Firmware	21
Update Display Information	22
Backup / Restore	23
Ping Host	25
Advanced Setting	26
Device Information	26
General	26
Network	27
IP Installer	28
Service Ports	28
IPv4 Settings	29
IPv6 Settings	30
Network Transfer Rate	30
DDNS	30
ANMS	31
Event Destination	31
Authentication	34
Security	38
Login Failures	38
Filter	39
Account Policy	42
Encryption	43
Working Mode	43
Private Certificate	45
Certificate Signing Request	46
Date/Time	48
Time Zone	48
Date / Time	48
Network Time	49
Customization	50
Mode	50
USB IO Settings	50
Multiuser Mode	51
Reset	51
Preferences	52
User Preferences	52
Logs	53
Remote Console	55

Remote Console Preview	55
Exit Macro	55
Download	56
About.	56
Viewer	57
Logout.	57
5. Accessing Remote Server	
Introduction	59
Web, Windows and Java Client Viewer	60
The Windows Client AP	61
Download	61
Starting Up	61
The Java Client AP	64
6. The Windows Client Viewer	
The Win / Java Client Control Panel	65
Control Panel Functions	66
Macros	69
Hotkeys	69
User Macros	71
System Macros	76
Video Settings	79
Advanced Video Settings	80
The Message Board	82
The Button Bar.	82
Message Display Panel	83
Compose Panel	83
User List Panel	83
Virtual Media	85
Virtual Media Icons	85
Virtual Media Redirection.	85
Zoom / Scale Window Size	89
The On-Screen Keyboard	90
Mouse Pointer Type	92
Mouse DynaSync Mode	93
Automatic Mouse Synchronization (DynaSync).	93
Manual Mouse Synchronization.	93
Mac and Linux Considerations	94
Customize Control Panel Configuration	95
7. The Log File	
The Log File Screen	97
8. The Log Server	
Installation.	99

Starting Up	99
The Menu Bar	100
Configure	101
Events	102
Search	102
Maintenance	103
Options	104
Help	104
The Log Server Main Screen	105
Overview	105
The List Panel	106
Panel Showing Logs of the Selected Units	106

Appendix

Safety Instructions	107
General	107
Rack Mounting	109
Technical Support	110
International	110
North America	110
IP Address Determination	111
IP Installer	111
Browser	112
AP Windows Client	113
IPv6	114
Link Local IPv6 Address	114
IPv6 Stateless Autoconfiguration	115
Port Forwarding	116
Keyboard Emulation	117
Trusted Certificates	118
Overview	118
Installing the Certificate	119
Certificate Trusted	120
Mismatch Considerations	120
Self-Signed Private Certificates	122
Examples	122
Importing the Files	122
Troubleshooting	123
General Operation	123
Windows	125
Java	126
Sun Systems	127
Mac Systems	128
The Log Server	128
Additional Mouse Synchronization Procedures	129
Windows:	129

Sun / Linux	130
Virtual Media Support	131
WinClient ActiveX Viewer / WinClient AP	131
Java Applet Viewer / Java Client AP	131
Administrator Login Failure	132
Specifications	133
CN800	133
ATEN Warranty Policy	134

About This Manual

This manual is provided to help you get the most out of your CN800. It covers all aspects of the device, including installation, configuration, and operation.

The models covered in this manual include:

Model	Product Name
CN800	USB VGA KVM over IP Mini

An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the CN800 KVM over IP Switch, its purpose, features and benefits, with its front and back panel components described.

Chapter 2, Hardware Setup, provides step-by-step instructions for setting up the device, and explains its basic operation procedures.

Chapter 3, Browser Login, describes how to log into the CN800 with a browser, and the various functions included.

Chapter 4, Configuration, explains the CN800's system settings that can be configured to suit its working environment.

Chapter 5, Accessing Remote Server, describes how to access the CN800 remotely.

Chapter 6, The Windows Client Viewer, explains how to remotely access the server connected to the CN800's port using a WinClient, Java Client, and Web Client viewer

Chapter 7, The Log File, shows how to use the log file utility to view the events that take place on the CN800.

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

Appendix, provides specifications and other technical information regarding the CN800.

Note:

- ♦ Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.

- ♦ The product may be updated with features and function added, improved or removed since the release of this manual. For an up-to-date user manual, visit <http://www.aten.com/global/en/>
-

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 consecutive selections, such as options on a menu or dialog box. For example, Start > Run means to open the <i>Start</i> menu, and then select <i>Run</i> .
	Indicates critical information.

This Page Intentionally Left Blank

Chapter 1

Introduction

Overview

The ATEN CN800 offers superior video quality with HD resolutions up to 1920 x 1200 @ 60 Hz, facilitating easier KVM access. The CN800 USB VGA KVM over IP Mini provides "over-IP" access control for conventional KVM switches lacking built-in over-IP functionality. It enables system operators to monitor and access computers remotely using Windows and Java-based application programs. The CN800 connects to an intranet, either LAN or WAN simply by using an industry-standard Cat 5e/6 cable and to a target computer or server. WinClient and JavaClient are available for remote access, enabling IP connection and login from anywhere over the internet.

The ATEN CN800 uses the standard TCP/IP protocols for communication. It allows the connected server or computer to be accessed from any computer over the internet – whether that computer is located down the hall, in other areas of the country, or branch offices in other parts of the world. The CN800 provides a fast, reliable, and cost-effective way to remotely access and manage widely distributed multiple computer installations.

Features and Benefits

Hardware

- ◆ Provides over-IP capability to KVM switches that do not have built in over-IP functionality
- ◆ Supports multi-platform server environments: Windows, Mac, Sun, Linux and VT100 based serial devices
- ◆ Virtual Media Support
- ◆ High video resolution — up to 1920 x 1200 @ 60 Hz with 24 bit color depth for remote sessions
- ◆ Enhanced FPS (frames per second) throughput for crisp responsive video display
- ◆ Bus-powered — no external power adapter required

Management

- ◆ Up to 64 user accounts
- ◆ Up to 32 users concurrent logins
- ◆ End session feature — administrators can terminate running sessions
- ◆ Event logging and Windows-based Log Server support
- ◆ Supports instant notification of critical system events via email, SNMP trap, and Syslog
- ◆ Remote firmware upgradable
- ◆ Multi-user Mode allows multiple users to gain access to a server simultaneously
- ◆ Integration with ATEN CC2000 Centralized Management Software
- ◆ Integration with ATEN CCVSR Video Session Recording Software
- ◆ DDNS (Dynamic Domain Name System)
- ◆ Enable / disable browser operation
- ◆ IPv6 capable

Easy-to-Use Interface

- ◆ Browser-based and AP GUIs offer a unified multi-language interface to minimize user training time and increase productivity
- ◆ Multi-platform client support (Windows, Mac OS X, Linux, Sun)
- ◆ Multi-browser supports (Chrome, Firefox, Safari, Opera)

- ♦ Browser-based UI in pure Web technology allows administrators to perform administrative tasks without pre-installed Java software package required
- ♦ Full-screen or sizable and scalable Virtual Remote Desktop

Advanced Security

- ♦ External authentication supports: RADIUS, LDAP, LDAPS, and MS Active Directory
- ♦ TLS 1.2 encryption to protect password when users log in
- ♦ Flexible design allows users to choose any combination of encryption algorithms (e.g. 256-bit AES) or system-generated random selection for independent keyboard / mouse, video, and virtual media data encryption
- ♦ Supports for 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 in operating system and BIOS level
- ♦ Supports USB 2.0 DVD / CD drives, USB mass storage devices, PC hard drives and ISO images
- ♦ Convenient to use without virtual media cable

Virtual Remote Desktop

- ♦ Video quality and video tolerance can be adjusted to optimize data transfer speed; monochrome color depth setting, threshold and noise settings 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 multi-language support
- ♦ Mouse Dynasync
- ♦ Exit Macros support
- ♦ 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 must have at least a P III 1 GHz processor, with their screen resolution set to 1024 x 768. It is recommended that your PC shall have P IV 2 GHz with 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:

- ♦ A VGA, SVGA or multisync port
- ♦ For USB KVM cable connections: a USB Type-A port and USB host controller
- ♦ For virtual media connection: an extra USB Type-A and USB host controller

Cables

- ♦ Cat 5e/6 or higher Ethernet cable(s) (not provided with this package), should be used to connect the CN800 to the LAN, WAN, or Internet.

Supported Video Resolutions

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

Note: The above table lists the device's supported video resolutions by default. For further supporting of other resolutions, please contact your dealer.

Operating Systems

- Supported operating systems for remote user computers that log into the CN800 include Windows 2000 or above, 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 CN800 are shown in the table below:

OS		Version
Windows		2000 or above
Linux	RedHat	9.0, Fedora or later RHEL AS 4, RHEL 5
	SUSE	10/ 11.1 or later
	Debian	3.1/ 4.0 or later
	Ubuntu	7.04 / 7.10 or later
UNIX	IBM AIX	5L / V6 or later
	FreeBSD	5.5/ 6.1 / 6.2 or later
Sun	Solaris	8/ 9 / 10 or later
Mac		OS 10.1 or later

Note: For Linux systems, Linux Kernel must be 2.6 or later to support USB 2.0.

Browsers

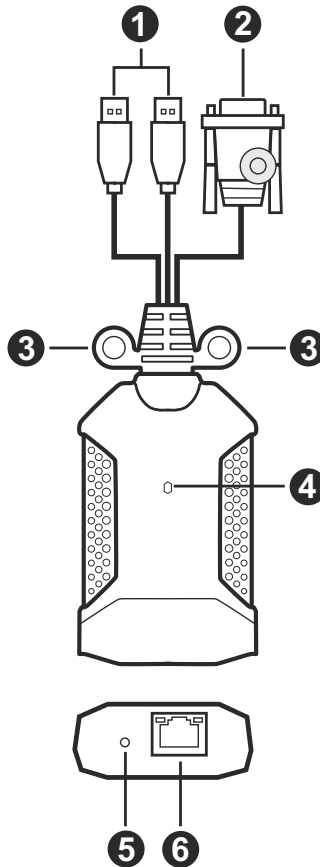
Supported browsers for users that log into the CN800 include the following:

Browser	Version
Chrome	45.0.2454.82, 51.0.270.103 or later
Firefox	33, 45.2.0, 47.0 or later
Safari	9.1.3 or later
Edge	25.10586.0.0 or later

Note: See *Mac Systems*, page 128, for further information regarding Safari.

Components

CN800



No.	Component	Description
1	USB Type-A ports	Connect the USB Type-A and VGA connectors to a PC / server you are installing.
2	VGA input port	
3	SR mounting hangers	Secures the CN800 to a rack, see <i>Rack Mounting</i> , page 10 for more information.
4	power LED	Lights green when the CN800 is powered on.

5	reset button	Press the reset button for more than 3 seconds to revert the unit back to factory default settings.
6	RJ-45 port	Connects to a Cat 5e/6 network cable for uplink connection.

Chapter 2

Hardware Setup



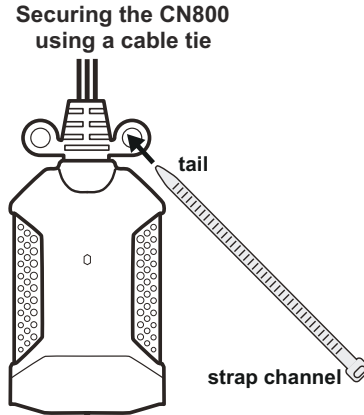
1. Important safety information regarding the placement of this device is provided on page 107. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
3. Any installation that does not follow the instructions in this guide may be hazardous or cause damage to the device.
4. Please operate the device with caution when under high environmental temperatures, as the surface of the device may become overheated under such conditions. For instance, the surface temperature of the device may reach 70 °C (158 °F) or higher when the environmental temperature reaches close to 50 °C (122 °F).

Rack Mounting

You can secure the CN800 to a rack using an of the following methods.

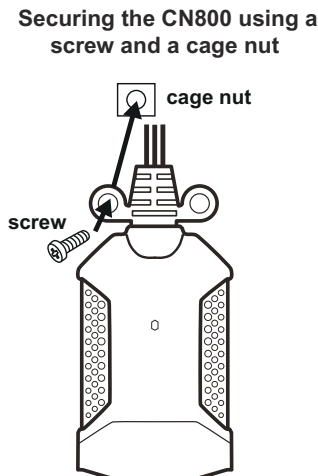
Securing the CN800 using a cable tie

Use a self-prepared cable tie, insert the tail through the SR mounting hanger, connect the tail to the strap channel and then tighten the strap to a rack.



Securing the CN800 using a screw and a cage nut

Use a self-prepared screw to screw through the SR mounting hanger to a self-prepared cage nut to secure the CN800 to a rack. Please make sure the cage nut is secured to the rack first.



Securing the CN800 using a magic tape

Use a self-prepared magic tape to hold the CN800 to a rack.

**Securing the CN800
using a magic tape**



Installation

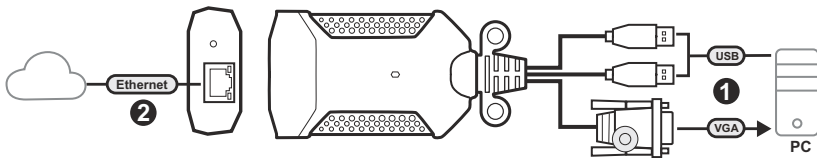
Follow the steps below and refer to the diagram on the following page (the steps and the numbers correspond to each other) to install.

1. Connect the USB and VGA connectors of the CN800 to the corresponding ports on the PC you are installing.

Note: The CN800 can be powered by the USB connectors, make sure to connect both USB connectors to the corresponding ports on the PC to power the CN800.

2. Connect the RJ-45 port of the CN800 to the LAN via a Cat 5e/6 cable for remote control.

Installation Diagram



Chapter 3

Browser Login

The CN800 can be accessed either from an Internet type browser, or via the following methods:

- ♦ Windows Client or Java Client (*Web, Windows and Java Client Viewer*, page 60);
- ♦ Windows or Java application (AP) program (*The Windows Client AP*, page 61 or *The Java Client AP*, page 64); and

The next several chapters describe browser-based operations.

Logging In

To operate the CN800 from a web browser, do the following:

1. Open your browser and enter the IP address of the CN800 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/CN800`

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 CN800's IP address are described in the Appendix on page 111.
-

2. If a **Security Alert** appears, click **Continue to this website** to accept the certificate — it can be trusted. (See *Trusted Certificates*, page 118, 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 CN800 login page appears:



3. Provide a valid **username** and **password** (set by the CN800 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 mindful of the username and password.

The main page appears after logging in successfully.

Main Screen

After you have successfully logged in, the CN800 main page appears:



The main page consists of the user menu on the left panel, with a *Viewer* icon (to launch the Java or WinClient Viewer) as well as a *Logout* icon displayed at 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 18, for permission details.

This Page Intentionally Left Blank

Chapter 4

Configuration

Introduction

The administration utilities, represented by the links and icons located on the left panel of the CN800 web page, are used to configure the device'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 CN800 is 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 18), the Administration configuration dialogs are not available.

Basic Setting

The following sections describe the screens under *Basic Setting*. Click the **User Management**, **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 CN800, 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.
- ♦ **Description:** Enter a descriptive word or phrase to describe the account.

Role

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

- ♦ **Administrator:** Gives Administrator level access. All permissions except *View Only* and *Force to Grayscale* are granted (see permissions below).
- ♦ **User:** Gives 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 CN800's operation.

- ♦ **Windows Client:** Checking this allows a user to access the CN800 via the Windows Client software.
- ♦ **Config:** Checking this allows the user to set up and modify the CN800's operating environment.
- ♦ **Enable Virtual Media:** Checking this allows a user to utilize the CN800's Virtual Media capabilities (see *Virtual Media*, page 85 for details). Use 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 CN800 via the Java Client software.
- ♦ **System Log:** Checking this allows a user to view the contents of the log file.
- ♦ **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 CN800 to apply:

- ♦ *Reset* - Click this to clear the fields.
- ♦ *Add* - Click this to add the new account to the CN800.
- ♦ *Update* - Click this to update the settings of an existing account.
- ♦ *Remove* - Click this to remove the selected account.

Sessions

The Sessions screen lets the administrator see all the users currently logged into the CN800, and provides information about each of their sessions.



Username	IP	Client	Category	Session	Logout
Administrator	192.168.1.100	Browser	Administrator	10:00:00	10:00:00



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 CN800 (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 56 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 CN800's firmware, backup/restore the CN800's configuration settings and allows you to configure the unit's setting using Terminal.

Upgrade Main Firmware

As new versions of the CN800 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 CN800; and click *Maintenance* in the left panel menu to bring up the *Firmware File* dialog box as follows:



3. Click **Choose File** 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.

Update Display Information

The Update Display Information screen displays the information of the video display and monitor used, as well as allows users to change its video resolution.



- ♦ **Display Information:** Click to display the information of the video display.
- ♦ **Update Display Info:** Click to change the resolution of the video display.
- ♦ **Save:** Click for the change to take effect.

Backup / Restore

The Backup / Restore screen gives you the ability to back up the CN800'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 CN800 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 CN800 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.

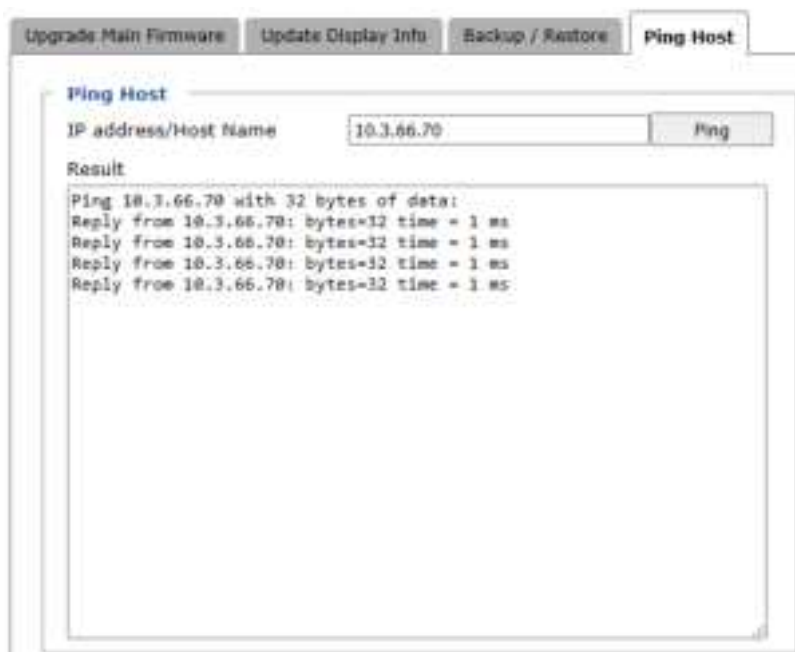
To restore a previous backup, do the following:

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 **Choose File** 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.

Ping Host

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



The screenshot shows a web interface with a top navigation bar containing four buttons: "Upgrade Main Firmware", "Update Display Info", "Backup / Restore", and "Ping Host". The "Ping Host" button is selected and highlighted. Below the navigation bar is a "Ping Host" section. It features a text input field labeled "IP address/Host Name" containing the value "10.3.66.70", followed by a "Ping" button. Below these is a "Result" section containing a text area with the following output:

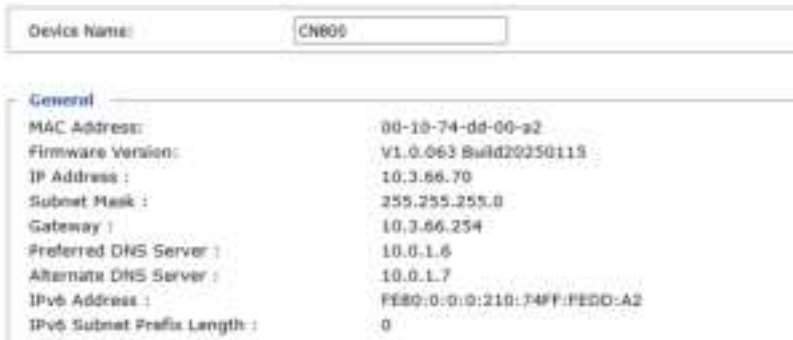
```
Ping 10.3.66.70 with 32 bytes of data:  
Reply from 10.3.66.70: bytes=32 time = 1 ms  
Reply from 10.3.66.70: bytes=32 time = 1 ms  
Reply from 10.3.66.70: bytes=32 time = 1 ms  
Reply from 10.3.66.70: bytes=32 time = 1 ms
```

Advanced Setting

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

Device Information

The Device Information screen provides information about the CN800's status. You can change the device name in this screen.



Device Name:		CN800
General		
MAC Address:	00-10-74-d8-00-a2	
Firmware Version:	V1.0.063 Build20250113	
IP Address :	10.3.66.70	
Subnet Mask :	255.255.255.0	
Gateway :	10.3.66.254	
Preferred DNS Server :	10.0.1.6	
Alternate DNS Server :	10.0.1.7	
IPv6 Address :	FE80:0:0:0:210:74FF:FE00:A2	
IPv6 Subnet Prefix Length :	0	

General

- ♦ **Device Name:** To make it easier to manage installations that have more than one CN800, each one can be given a name. Enter a name (16 characters max.) for the CN800 then click **Save**.
- ♦ **MAC (1, 2) Address:** The CN800's MAC Address displays here.
- ♦ **Firmware Version / FPGA:** Indicates the CN800's current firmware version and build date. New versions of the CN800's firmware can be downloaded from our website as they become available (see *Upgrade Main Firmware*, page 21). You can reference this number to see if there are newer versions available on the website.
- ♦ **IP Address:** Displays the CN800'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 CN800's gateway address.
- ♦ **IPv6 Address / IPv6 Subnet Prefix Length:** Displays the CN800's Internet Protocol Version 6 (128 bit) address (in the new format). See *IPv6*, page 114 for details.

Network

The Network screen is used to specify the CN800's network environment.

IP Installer

☒ Enabled ☐ View Only ☐ Disabled

Service Ports

Program:

HTTP:

HTTPS:

IPv4 Settings

IP Address:

☒ Obtain IP address automatically [DHCP]
☐ Set IP address manually [Fixed IP]

IP Address:

Subnet Mask:

Default Gateway:

DNS Server:

☒ Obtain DNS server address automatically
☐ Set DNS server address manually

Preferred DNS server:

Alternate DNS server:

IPv6 Settings

IP Address:

☒ Obtain IPv6 address automatically [DHCP]
☐ Set IPv6 address manually [Fixed IP]

IPv6 Address:

Subnet Prefix Length:

Default Gateway:

DNS Server:

☒ Obtain DNS server address automatically
☐ Set DNS server address manually

Preferred DNS server:

Alternate DNS server:

Network Transfer Rate: Kbps

DONOS

☐ Enable

Host Name:

DONOS:

Username:

Password:

DONOS Retry Time: hour

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the CN800. Click one of the radio buttons to select *Enabled*, *View Only*, or *Disabled* for the IP Installer utility. See p. 111 for IP Installer details.

-
- Note:** 1. If you select *View Only*, you will be able to see the CN800 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 CN800 uses for various network services.

- ♦ **Program:** This is the port number for connecting to the CN800 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.

-
- 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 CN800 will not be found.

IPv4 Settings

The CN800 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 CN800 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 111, for information.
-

The CN800 can either have its DNS server address assigned automatically, or a fixed address can be specified.

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

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

IPv6 Settings

The CN800 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 CN800 can either have its DNS server address assigned automatically, or a fixed address can be specified.

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

Note: Specifying for an 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 CN800 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 CN800 can update the DDNS server with its IP address at certain time intervals. To enable the DDNS capability for the CN800, 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 CN800 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 Server, and Syslog Server settings.

The screenshot shows the 'Event Destination' configuration window. It has two tabs: 'Event Destination' and 'Authentication'. The 'Event Destination' tab is active. It contains four main sections:

- SMTP Settings:**
 - ☐ Enable report from the following SMTP Server
 - SMTP Server: [text field]
 - Service Port: [text field with value 25]
 - ☐ My server requires secure connection (SSL)
 - ☐ My server requires authentication
 - Account Name: [text field]
 - Password: [text field]
 - From: [text field]
 - To: [text field]
 - ☐ Report IP Address
 - ☐ Report system reboot
 - ☐ Report user login
 - ☐ Report user logout
- Log Server:**
 - ☐ Enable
 - MAC Address: [text field with value 000000000000]
 - Service Port: [text field with value 9991]
- SNMP Server:**
 - ☐ Enable SNMP Agent
 - Server IP: [text field]
 - Service Port: [text field with value 162]
- Syslog Server:**
 - ☐ Enable
 - Server IP: [text field]
 - Service Port: [text field with value 514]

■ SMTP Settings

To have the CN800 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 CN800, such as logins and internal status messages, are kept in an automatically generated log file in the Log Server. See Chapter 8, *The Log Server* for details on setting up the log server. The *Log File* is discussed on page 97.

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 be different than the one used for the *Program* port (see *Service Ports*, page 28).

■ SNMP Server

To be notified of SNMP server 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 server events. The valid port range is 1-65535. Default is 162.

Note: The SNMP server events such as System Power On, Login Failure, and System Reset are sent to the server.

■ Syslog Server

To record all the events that take place on the CN800 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 CN800 allows log in authentication and authorization through external programs.

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

The screenshot shows the 'Authentication' tab of a configuration interface. At the top, there are two tabs: 'Event Destination' and 'Authentication'. Below the tabs, there is a checkbox labeled 'Disable Device Authentication'. Underneath, there are three main sections: 'RADIUS Settings', 'AD/LDAP Settings', and 'CC Management'. The 'RADIUS Settings' section includes an 'Enable' checkbox, fields for 'Preferred RADIUS Server IP', 'Preferred RADIUS Service Port', 'Alternate RADIUS Server IP', 'Alternate RADIUS Service Port', 'Timeout' (with a 'sec' label), 'Retries', and a 'Shared Secret (at least 6 characters)'. The 'AD/LDAP Settings' section includes an 'Enable' checkbox, a 'Type' dropdown menu with 'LDAP' and 'LDAPS' options, and fields for 'LDAP Server', 'Admin DN', 'Admin Name', 'Password', 'Search DN', 'Port', and 'Timeout' (with a 'sec' label). The 'CC Management' section includes an 'Enable' checkbox and fields for 'CC Server IP' and 'CC Service Port'.

Authentication

☐ Disable Device Authentication

RADIUS Settings

☐ Enable

Preferred RADIUS Server IP:

Preferred RADIUS Service Port:

Alternate RADIUS Server IP:

Alternate RADIUS Service Port:

Timeout: sec

Retries:

Shared Secret (at least 6 characters):

AD/LDAP Settings

☐ Enable

Type: ☐ LDAP ☐ LDAPS

LDAP Server:

Admin DN:

Admin Name:

Password:

Search DN:

Port:

Timeout: sec

CC Management

☒ Enable

CC Server IP:

CC Service Port:

If you want to use a RADIUS, AD/LDAP, CC Authentication instead of the CN800 device authentication, check **Disable Device Authentication**. Selecting this option will disable login authentication locally on the CN800.

■ RADIUS Settings

To allow authentication and authorization for the CN800 through a RADIUS server, do the following:



The screenshot shows a configuration window titled "RADIUS Settings". It contains the following fields and controls:

- ☐ Enable
- Preferred RADIUS Server IP: [text input field]
- Preferred RADIUS Service Port: [text input field with "0" entered]
- Alternate RADIUS Server IP: [text input field]
- Alternate RADIUS Service Port: [text input field with "0" entered]
- Timeout: [text input field with "0" entered] sec
- Retries: [text input field with "0" entered]
- Shared Secret (at least 6 characters): [text input field]

1. Check **Enable**.
2. Fill in the IP addresses and port numbers for the Preferred and Alternate RADIUS servers.
3. In the **Timeout** field, set the time in seconds that the CN800 waits for a RADIUS server reply before it times out.
4. In the **Retries** field, set the number of allowed RADIUS retries.
5. In the **Shared Secret** field, enter the character string that you want to use for authentication between the CN800 and the RADIUS Server.

■ AD/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 *CN800 – iKVM50-userProfile* or *iKVM57-userProfile* – is added as an optional attribute to the person class.

Users can find the attribute name of CN800 by executing a **get** command on the Ping Host page, see page 25.

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 CN800 via LDAP / LDAPS, refer to the information in the following table.

Item	Action
Enable	Check <i>Enable</i> to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click a radio button to specify whether to use LDAP or LDAPS.
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 CN800 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=cn800,dc=aten,dc=com
Admin Name	Key in the Group Name for CN800 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. <i>If Enable Authorization is not checked, this field must include the entry where the CN800 Admin Group is created. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.</i>

- ◆ 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.
- ◆ For CN800, respectively use **iKVM50-userProfile** and **iKVM57-userProfile** as LDAP attribute and **su/[username]** as its attribute value.

■ CC Management Settings

To allow authorization for the CN800 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 CN800 and allows you configure the login failure policies, filter settings, account policies, encryption settings, 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 screenshot shows a configuration window titled "Login Failures". It contains the following elements:

- An "Enable" checkbox, which is currently unchecked.
- An "Allowed:" label followed by a text input field containing the number "5".
- A "Timeout:" label followed by a text input field containing the number "3", and a "min" label to its right.
- A "Lock Client PC" checkbox, which is checked.
- A "Lock Account" checkbox, which is unchecked.

The meanings of the entries are explained below.

- ♦ **Login Fail Policy:** Select the login failure policy that the CN800 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 CN800 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.

The screenshot shows a configuration window titled "Filter". It contains two main sections: "IP Filter" and "MAC Filter".

IP Filter Section:

- There are three radio buttons: "Enable IP Filter" (unchecked), "Include" (unchecked), and "Exclude" (checked).
- Below the radio buttons is a list box containing the IP range "192.168.0.100-192.168.0.101".
- To the right of the list box are three buttons: "Add", "Modify", and "Delete".
- Below the list box is a "Login String:" label followed by an empty text input field.

MAC Filter Section:

- There are three radio buttons: "Enable MAC Filter" (unchecked), "Include" (unchecked), and "Exclude" (checked).
- Below the radio buttons is a list box containing the MAC address "00-60-00-00-12-34".
- To the right of the list box are three buttons: "Add", "Modify", and "Delete".

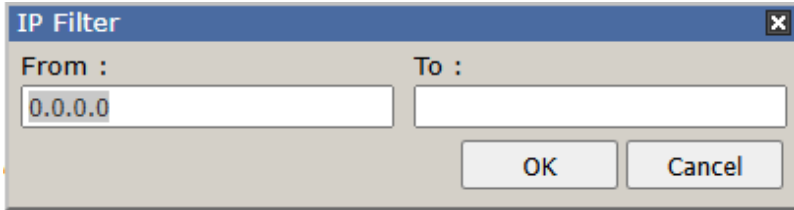
To enable IP and/or MAC filtering, check **Enable IP Filter** and/or **Enable MAC Filter**.

- ♦ 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:

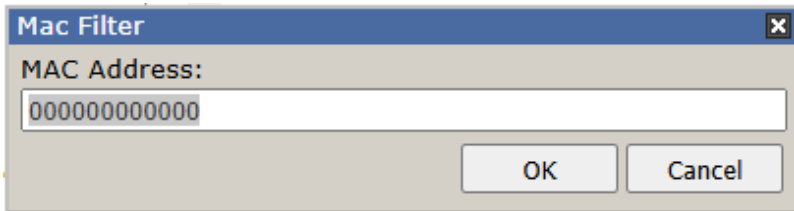
1. Click **Add**, enter the IP address range you want to filter and click **OK**.



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 CN800 with a browser. For example:

192.168.0.126/CN800

- ♦ 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 CN800 login page using the IP address alone. This makes your installation less secure.

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

Account Policy

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

Account Policy

Minimum Username Length:

Minimum Password Length:

Password Must Contain At Least

☐ One Upper Case

☐ One Lower Case

☐ One Number

☐ Disable Duplicate Login

☐ Enforce Password History

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

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

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.

Encryption					
Keyboard/Mouse					
☐ DES	☐ 3DES	☐ AES	☐ RC4	☐ Random	
Video					
☐ DES	☐ 3DES	☐ AES	☐ RC4	☐ Random	
Virtual Media					
☐ DES	☐ 3DES	☐ AES	☐ RC4	☐ Random	

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

Working Mode

Use this section to set the working mode parameters.

Working Mode	
☒	Enable ICMP
☒	Enable Multiuser Operation
☒	Enable Virtual Media Write
☐	Browser Service : Disable Browser
☒	Disable Authentication

- ♦ **Enable ICMP** so that the CN800 can be pinged. If it is not enabled, the device cannot be pinged. The default is **Enabled**.
- ♦ **Enable Multiuser Operation** to permit more than one user to log into the CN800 at the same time. The default is **Enabled**.

- ♦ **Enable Virtual Media Write** allows redirected virtual media devices on a user's system to send data to a remote server, as well as being able to have data from the remote server written to them. The default is **Enabled**.
- ♦ **Browser Service** allows the administrator to limit the scope of browser access to the CN800. Put a check in the checkbox to enable this function, then select the browser limitation in the drop-down menu. Choices are explained in the following table:

Item	Explanation
Disable Browser	If this is selected, the CN800 cannot be accessed via a browser. It can only be accessed from the AP programs (see <i>AP Operation</i> , page 133).
Disable HTTP	If this is selected, the CN800 can be accessed via a browser, but not from an ordinary (HTTP) login connection – it can only be accessed over a secure HTTPS (SSL) connection.
Disable HTTPS (SSL)	If this is selected, the CN800 can be accessed via a browser over an ordinary (HTTP) login connection, but not via a secure HTTPS (SSL) connection.

- ♦ If **Disable Authentication** is checked, no authentication procedures are used to check users attempting to log in. Users gain Administrator access to the CN800 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.

The screenshot shows a web interface titled "Private Certificate". It contains two rows of input fields. The first row is labeled "Private Key :" and the second row is labeled "Certificate :". To the right of each label is a "Choose File" button and the text "No file chosen". Below these rows are two buttons: "Upload" and "Restore default".

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 122 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 **Choose File** to the right of **Private Key**, navigate to where your private encryption key file is located and select it.
2. Click **Choose File** 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:

A screenshot of a "Certificate Signing Request" dialog box. It contains several text input fields for: "Country (2 letter code):", "State or Province:", "Locality:", "Organization:", "Unit:", "Common Name:", and "Email Address:". At the bottom of the dialog are two buttons: "Create" and "Close".

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

Information	Example
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 <i>www.mycompany.com</i> , and you only specify <i>mycompany.com</i> , the certificate will not be valid.
Email Address	administrator@yourcompany.com

- 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 CN800.
- 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.
- After the CA sends you the certificate, save it to a convenient location on your computer. Click **Choose File** to locate the file; then click **Upload** to store it on the CN800.

Note: When you upload the file, the CN800 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**.

Date/Time

The Date/Time dialog page sets the CN800 time parameters:

Time Zone

(GMT-12:00) Eniwetok Kwajalein ▾

☐ Daylight Savings Time

Date

March ▾ < 2025 >

March 2025

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Time

21 : 27 : 00

Set

Network Time

☐ Enable auto adjustment

Preferred time server

All | ntp.cs.msu.cz All ▾

☐ Preferred custom server IP

☐ Alternate time server

All | ntp.cs.msu.cz All ▾

☐ Alternate custom server IP

Adjust time every 1 days

Adjust Time Now

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.

Note: We recommend configuring a preferred custom server IP to avoid time issues due to the selected preferred time server becoming unserviceable.

3. If you want to configure an alternate time server, check **Alternate time server** and repeat step 2 for the alternate time server entries.

Note: We recommend configuring an alternate time server to avoid time issues due to the selected preferred time server becoming unserviceable.

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.

The screenshot shows a web-based configuration interface for the CN800 device. It is divided into four sections: **Mode**, **USB IO Settings**, **Multiusers Mode**, and **Reset**. In the **Mode** section, there are two checkboxes: 'Force All to Grayscale' (unchecked) and 'Enable Client AP Device List' (checked). The **USB IO Settings** section contains two dropdown menus: 'OS' set to 'Win' and 'Language' set to 'US English'. The **Multiusers Mode** section has a 'Multiusers Mode' dropdown set to 'Share' and an 'Occupy Timeout' field set to '3' seconds, with a range of '(0-255)' indicated. The **Reset** section includes a 'Reset on exit' checkbox (unchecked) and a 'Reset Default Values' button.

Mode

Check **Force All to Grayscale** to enable this function. When enabled, the remote displays of all clients connected to the CN800 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 *Starting Up*, page 61). 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.

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 82).

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

Reset

Click **Reset Default Values** to reset the CN800 to the default system 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.

The screenshot shows a 'Settings' window with the following fields and controls:

- Language:** A drop-down menu currently set to 'English'.
- OSD Hotkey:** A drop-down menu currently set to '[Scroll Lock] [Scroll Lock]'.
- Logout Timeout:** A text input field containing '0' followed by a 'min' unit label.
- Launch viewer after login:** An unchecked checkbox.
- Viewer:** A list box containing two items: '#1 Win Client' (highlighted) and '#2 Java Client'. To the right of the list are green up and down arrow buttons for reordering.
- Save:** A button located below the Viewer list.
- Old Password:** A text input field.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Change Password...:** A button located below the password fields.

■ Language

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

■ OSD Hotkey

Select the keyboard combination to call the OSD function.

Note: This OSD Hotkey is not supported on WebClient, and is only supported on local console, WinClient, and JavaClient.

■ Logout Timeout

When the session is idling, the time set here determines how long the CN800 will wait for before terminating the session.

■ Launch Viewer after Login

Checking this checkbox will automatically launch the Viewer application after a user logs in to the CN800.

■ Viewer

Choose the detection order for the viewer you would like to use when viewing the remote server's display.

- Click **Save** for the changes to take effect.

■ 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 CN800 logs all the events that take place on it. Following a reset, all logs are cleared. Click **Log Information** to view the logs:

Time	Security	User	Log Information
2025/03/07 18:38:30	Event	222	OP: User 222 changed to [01].
2025/03/07 18:38:39	Event	222	OP: User 222 logged in.
2025/03/07 18:38:50	Event	System	OP: User 222 (10.3.86.131) attempting to login.
2025/03/07 18:38:50	Event	System	SYS: Access via windows client 10.3.86.131.
2025/03/07 18:38:58	Event	System	SYS: Connected to 10.3.86.131 [ID: 00-00-01-FE-45].
2025/03/07 18:17:38	Event	System	OP: User 222 from 10.3.86.131 [DE-00-00-01-FE-63] attempting to login via browser.
2025/03/07 18:17:37	Event	System	OP: User administrator from 10.3.86.98 (94-C8-81-1F-ED-08) attempting to login via browser.
2025/03/07 08:36:56	Event	System	SYS: Accept new IP address 10.3.86.76 to network interface.
2025/03/07 08:36:51	Event	System	SYS: System startup.
2025/03/07 08:36:11	Event	System	SYS: Loading system setting. Firmware version=V1.0.005.20250225.

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 99.

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:



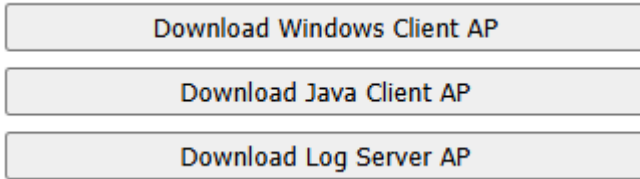
Clicking **Refresh** updates the snapshot of the remote display.

Exit Macro

The Exit Macro panel contains a drop-down list box of user created System macros: Select the Exit Macro you would like to use and click Save. See *System Macros*, page 76, for details on creating exit macros.

Download

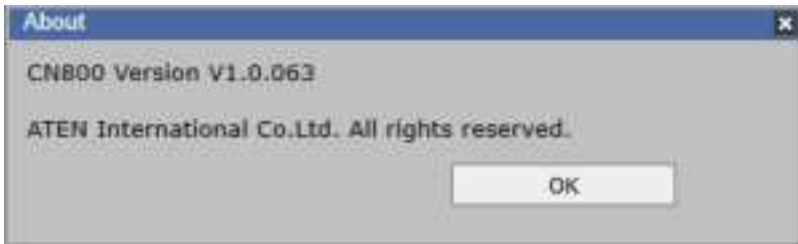
The Download page lets you download the standalone *Windows Client AP*, *Java client AP* and *Log Server AP*.



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 59.
 - ♦ For details on the *Log Server AP*, refer to Chapter 8 on page 99.

About

Click *About* to see the current firmware version and copyright information of your CN800.



Viewer

Click the Viewer icon to call the remote client (Web Client, WinClient or Java Client) to view the remote server in a separate window.

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

Logout

Click the Logout icon when you are done configuring the CN800's operating environment. This logs you out of the CN800 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. **Web Client viewer** accessed directly from the web browser GUI. Refer to *Web, Windows and Java Client Viewer* on page 60 for more information.
2. **Windows viewer** accessed directly from the web browser GUI. Refer to *Web, Windows and Java Client Viewer* on page 60 for more information.
3. **Java viewer** accessed directly from the web browser GUI. Refer to *Web, Windows and Java Client Viewer* on page 60 for more information.
4. **Windows Client Viewer AP** (without browser). Refer to *The Windows Client AP* on page 61 and *The Windows Client Viewer* on page 65 respectively on how to access the remote server and how to utilize the viewer.
5. **Java Client Viewer AP** (without browser). Refer to *The Java Client AP* on page 64 on how to access the remote server. Since the control is identical to the windows client viewer, refer to *The Windows Client Viewer* on page 65 on the control of the viewer interface.

To download the Windows Client AP and the Java Client AP from the web GUI. Refer to *Download*, page 56 for more details.

Web, Windows and Java Client Viewer

The Web, Windows and Java Client Viewer is accessible via a web browser. After you log into the web configuration page (see *Logging In*, page 13), click the **Viewer** icon on the left panel menu. A second or two after, the remote server's desktop appears as a window on your desktop:



The control/access of the remote server is laid out in the control panel. Refer to *The Win / Java Client Control Panel* on page 65 for access/control information.

By default, the Web Client viewer is used.

If you rearrange the preference order (see *User Preferences*, page 52), a different Client viewer may be 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 56 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 CN800 Windows Client program, it automatically searches the user's local LAN segment for CN800 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 CN800 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 CN800.
Disconnect	These buttons become active once you log into the CN800. See page 63 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.

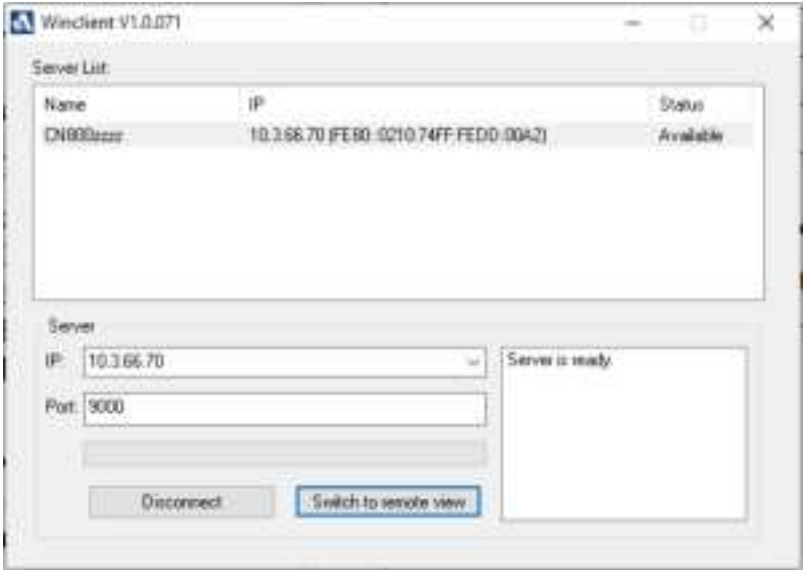
1. Double-click the unit. When the CN800 is connected to the unit, a login window appears:



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 CN800.
Switch to remote view	In some cases, administrators do not wish to have users connect to the CN800 with a browser. <i>Switch to remote view</i> solves this problem as it opens a window on the user's desktop containing the remote server's desktop that is the same as the one that appears with the browser-based Windows client. Refer to Chapter 6, <i>The Windows Client Viewer</i> , for operation details.

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

Refer to *The Win / Java Client Control Panel* on page 65 for information about the remote access interface.

The Java Client AP

The Java Client AP is an AP program provided to make the CN800 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 61 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 Win / Java Client Control Panel* on page 65 for access/control information.

Chapter 6

The Windows Client Viewer

The Win / Java Client Control Panel

The control panels of the WinClient and Java Client are similar, with their differences explained below:

- ♦ In the Macros dialog box, *Toggle Mouse Display* is only available on WinClient.
- ♦ The *Dot* mouse pointer type is only available on WinClient.
- ♦ There is *Show/Hide* button to show or hide the user list and message panel in the Message Board function on the Java Client Viewer. This function is achieved by clicking the arrows at the top of the bar that separates the User List panel from the Main panel.
- ♦ In Virtual Media, only ISO and Folder are supported for Java Client.

The control panel may be 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 *Customize Control Panel Configuration*, page 95, 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 consists of two rows.
- ♦ The second row shows the video resolution of the remote desktop, 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*. The below image shows the complete menu-style control panel and the 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.
	Under an accessed port, click to recall the GUI.
	Click to bring up the Video Options dialog box. (See <i>Video Settings</i> , page 79, for details).
	Toggles the display between <i>Full Screen Mode</i> and <i>Windowed Mode</i> .
	Click to adjust the zoom factor of the remote display window or adjust the windows size. Note: This feature is only available in windowed mode (Full Screen Mode is off). See <i>Zoom / Scale Window Size</i> , page 89 for details.

Icon	Function
	Click to toggle the remote display between color and grayscale.
	Click to perform a video and mouse autosync operation.
	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is <i>Automatic</i>, a green mark appears on the icon. ◆ When the selection is <i>Manual</i>, a red mark appears on the icon. See <i>Mouse DynaSync Mode</i>, page 93 for a complete explanation of this feature.
	Click to select the mouse pointer type. Note: This icon changes depending on which mouse pointer type is selected (see <i>Mouse Pointer Type</i>, page 92).
	Click to bring up the on-screen keyboard (see <i>The On-Screen Keyboard</i> , page 90).
	Click to take a snapshot (screen capture) of the remote display. To configure the Snapshot parameters, refer to <i>Snapshot</i> on page 96.
	Click to send a <i>Ctrl+Alt+Del</i> signal to the remote system.
	Click to bring up the Macro dialog box (see <i>Macros</i> , page 69 for more details).
	Click to display a dropdown list of <i>User</i> macros in order to access and run macros more conveniently than using the Macro dialog box (see the <i>Macro</i> icon in the table above, and the <i>Macro</i> section on page 69)
	Click to bring up the <i>Virtual Media</i> dialog box. The icon changes when a virtual media device is mounted on the port. See <i>Virtual Media</i>, page 85, for specific details. Note: This icon displays in gray when the function is disabled or not available to the user.
	Click to bring up the Message Board (see <i>The Message Board</i> , page 82).

Icon	Function
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is <i>On</i>, the LED is bright orange. ◆ When the lock state is <i>Off</i>, 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 Control Panel Configuration dialog box. See <i>Customize Control Panel Configuration</i>, page 95, for details on configuring the Control Panel.

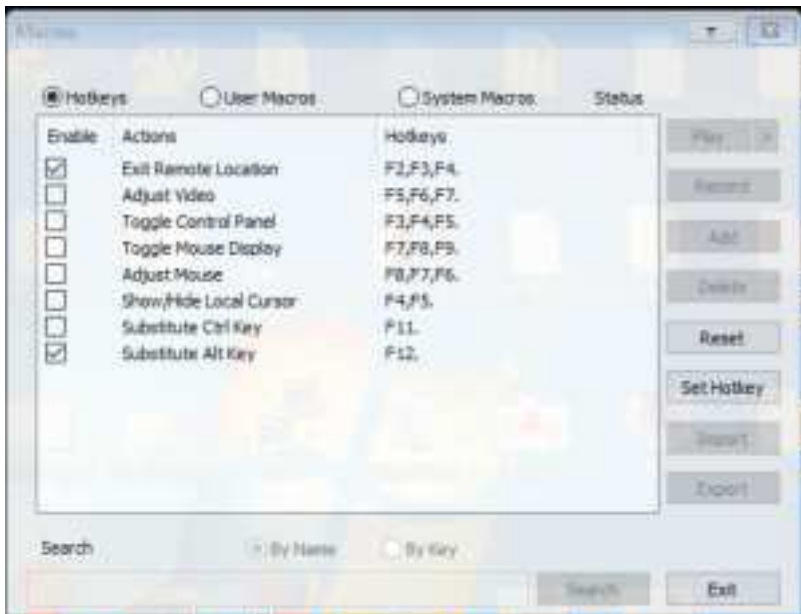


Macros

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**.

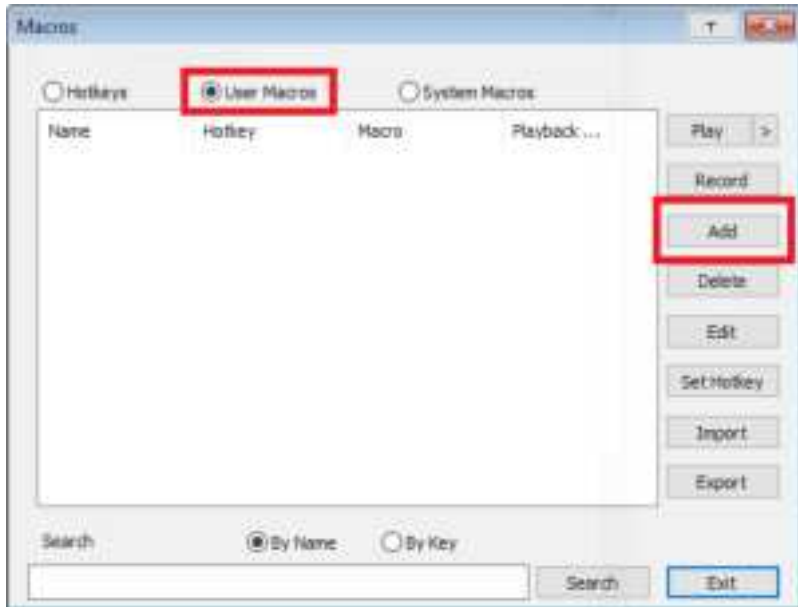
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit remote location	Exits the remote view. This is equivalent to clicking the <i>Exit</i> icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	Brings up the <i>Video Settings</i> dialog box. This is equivalent to clicking the <i>Video Settings</i> 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 <i>Dot</i> pointer type from the <i>Mouse Pointer</i> 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.
Show/Hide Local Cursor	Toggles the display of your local mouse pointer off and on. This is equivalent to selecting the <i>Null</i> pointer type from the <i>Mouse Pointer</i> 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 F12.

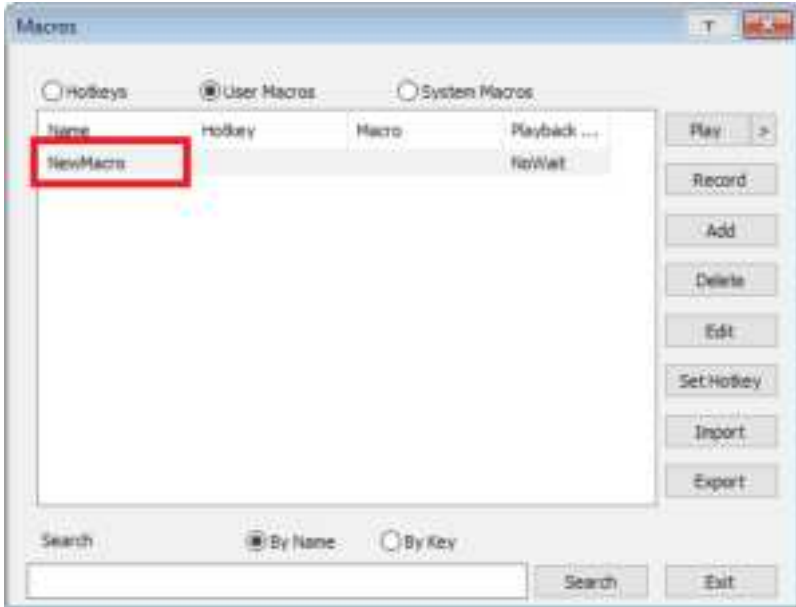
User Macros

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**.

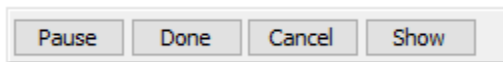


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:

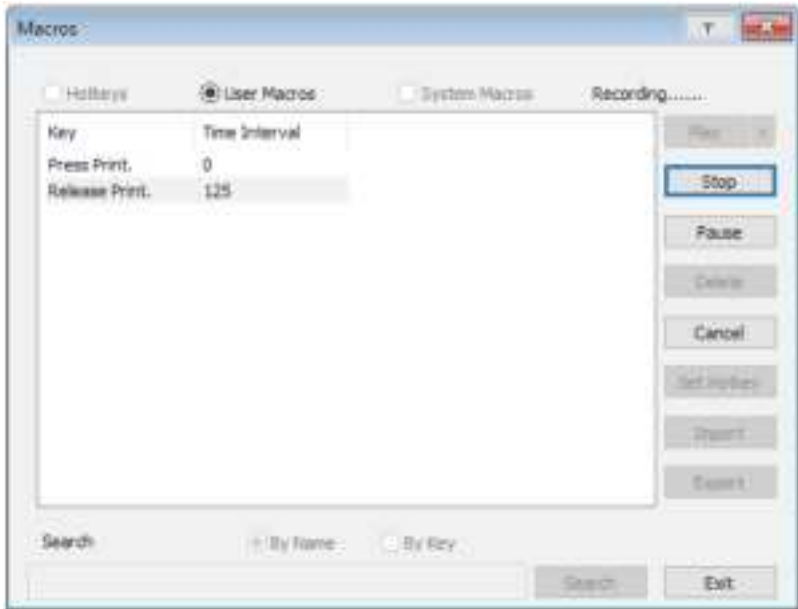


3. Click **Record**.

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:

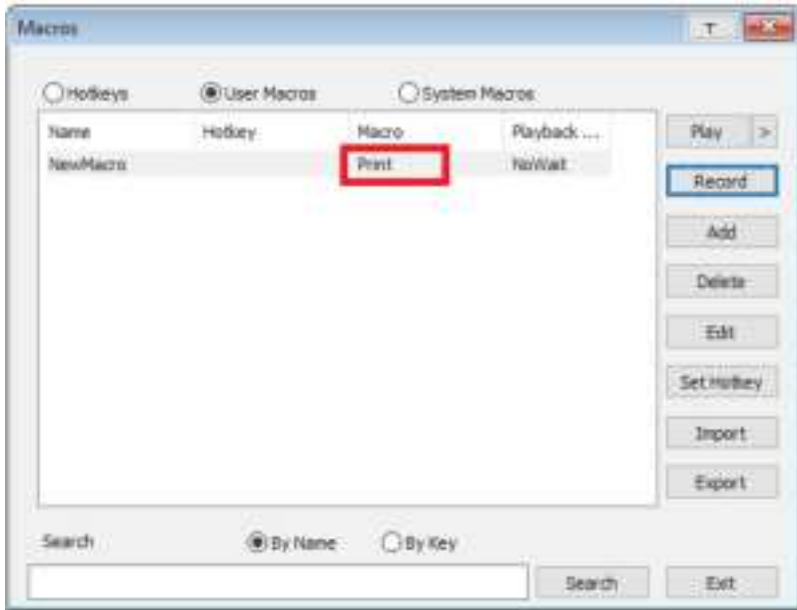


- ♦ Clicking **Cancel** cancels all keystrokes.
- ♦ When you have finished, click **Stop**. This is the equivalent of clicking *Done* in Step 5.

Note:

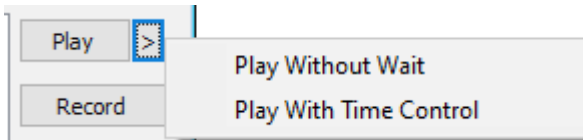
- ♦ Case is not considered – typing **A** or **a** has the same effect.
- ♦ When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
- ♦ Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is 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 69.
7. You can also assign the playback mode and select either **Play Without Wait** (*Nowait*) or **Play with Time Control**.

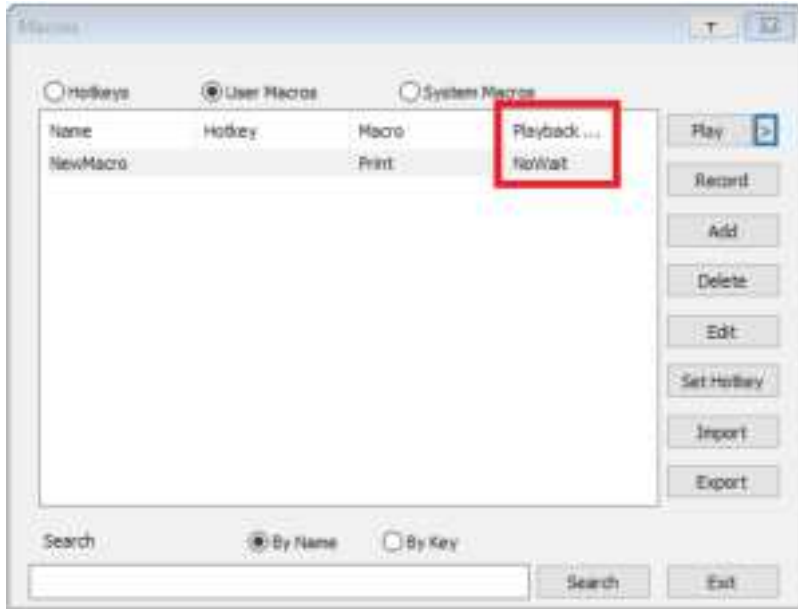
If you run the macro from this dialog box, you have the option of specifying how the macro runs.



- ♦ 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 67).
3. By opening this dialog box and clicking **Play**.

Note: User Macros are stored on the Local Client computer of each user.

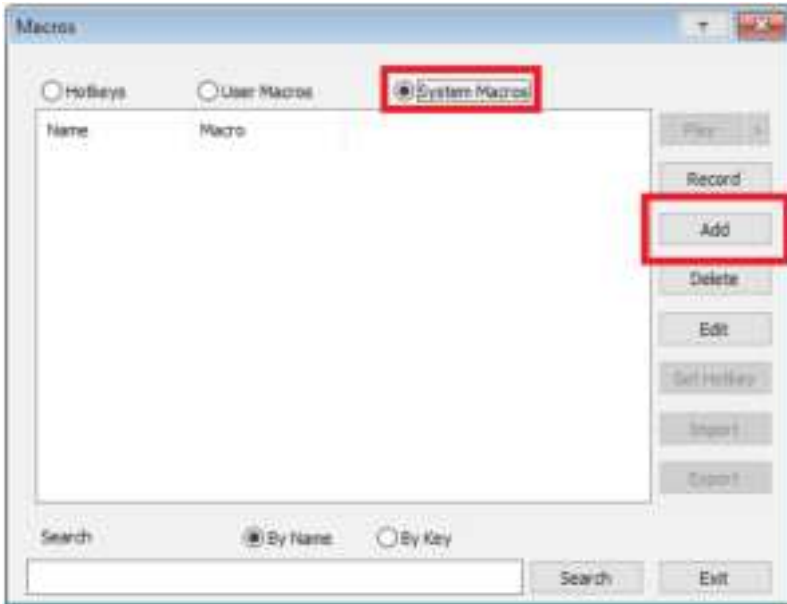
Therefore there is no limitation on the number of macros, the size of the macro names, or makeup of the hotkey combinations that invoke them.

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.

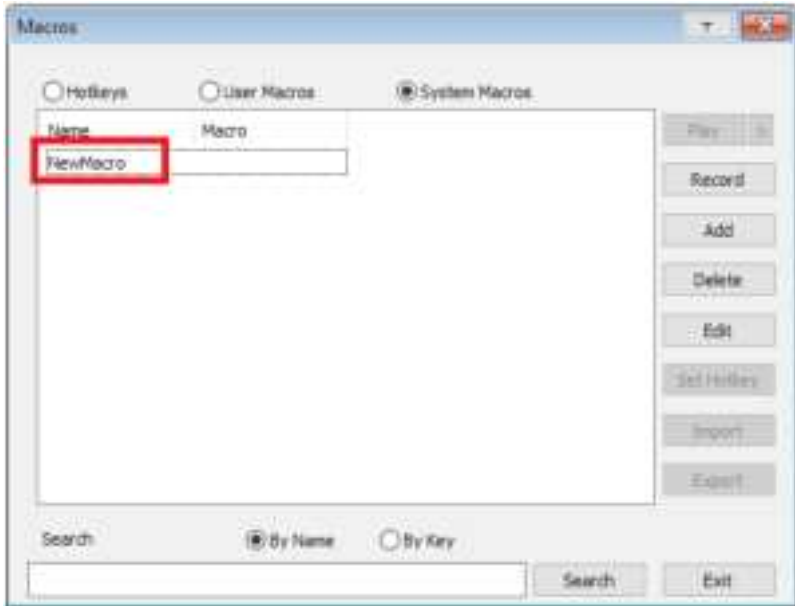
System Macros

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**.

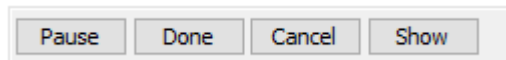


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



3. Click **Record**.

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



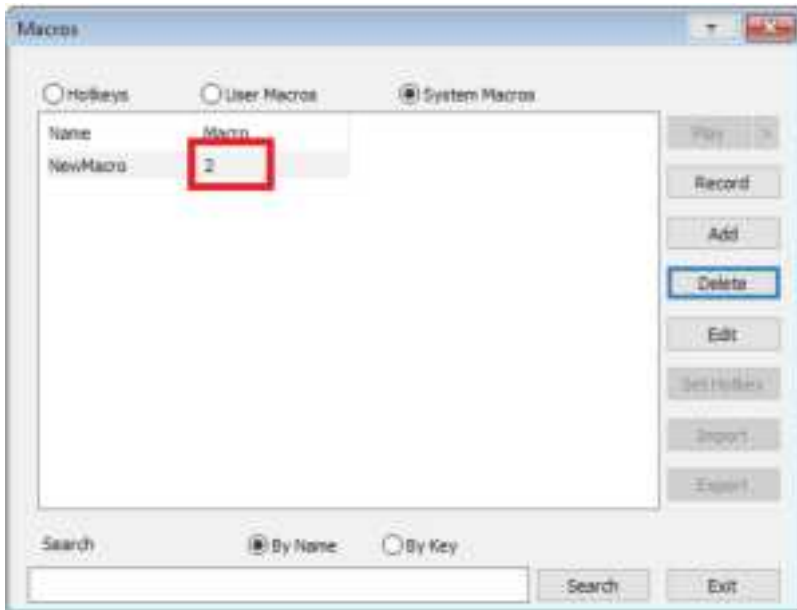
4. Press the keys for the macro.
 - ♦ To pause macro recording, click **Pause**. To resume, click **Pause** again.
 - ♦ Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 77).

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 of them upon logging out of the CN800 (see *Customization*, page 50 for details).

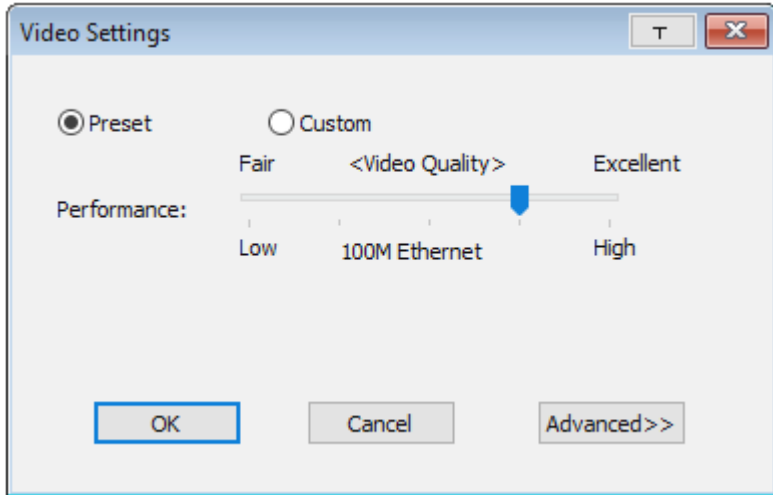
Note: 1. Information about the Search function is given on page 75.

2. Systems macros are stored on the CN800, 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.

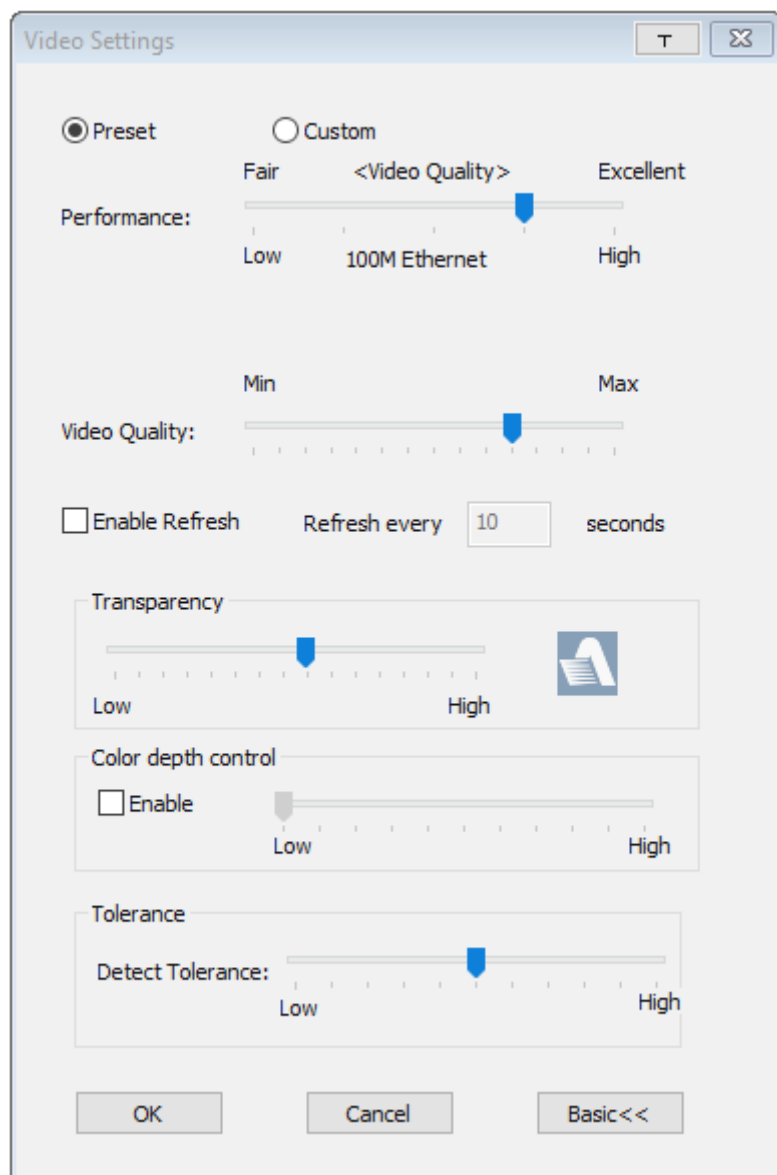


The adjustment options are as follows:

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 CN800. The CN800 will use that selection to automatically adjust the <i>Video Quality</i> and <i>Detect Tolerance</i> 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 <i>Customize</i> and use the Video Quality and Detect Tolerance slider bars to adjust the settings to suit your conditions.
Advanced	See page 80 for details.

Advanced Video Settings

For greater control and if it is necessary to modify the remote video display, use the **Advanced** Video Settings by clicking the **Advanced** button.



The additional options in the Advanced screen are as follows:

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 CN800 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 CN800 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 <i>Enable Refresh</i> 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 control panel.
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.
Tolerance	This setting also relates to video quality. It governs detecting or ignoring pixel changes. A high setting can result in a low quality display due to less data transfer. A lower setting will result in better video quality, but setting the threshold too low may allow too much data to be transferred, negatively impacting network performance.

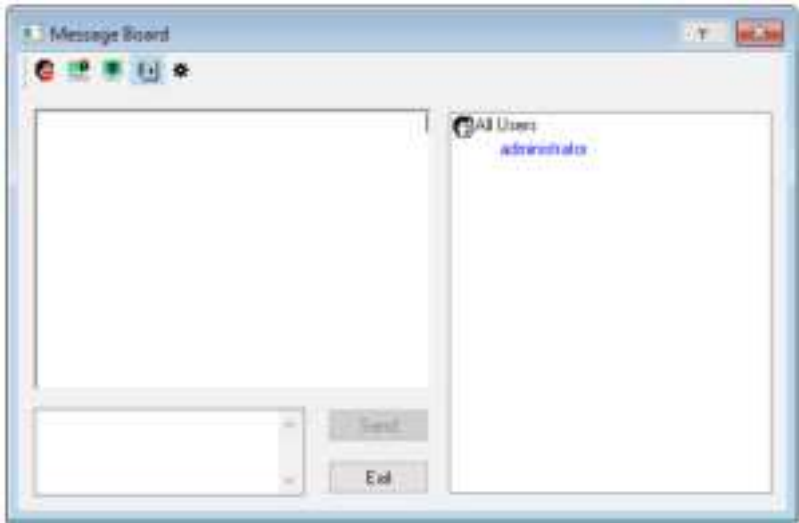
Click **OK** to save your changes and close the dialog box.

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 CN800 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 <i>Share</i> mode (see <i>Working Mode</i> , page 43), 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 Board Pop Up Settings. A checkbox is available to enable / disable message pop-up when a message is received.

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.

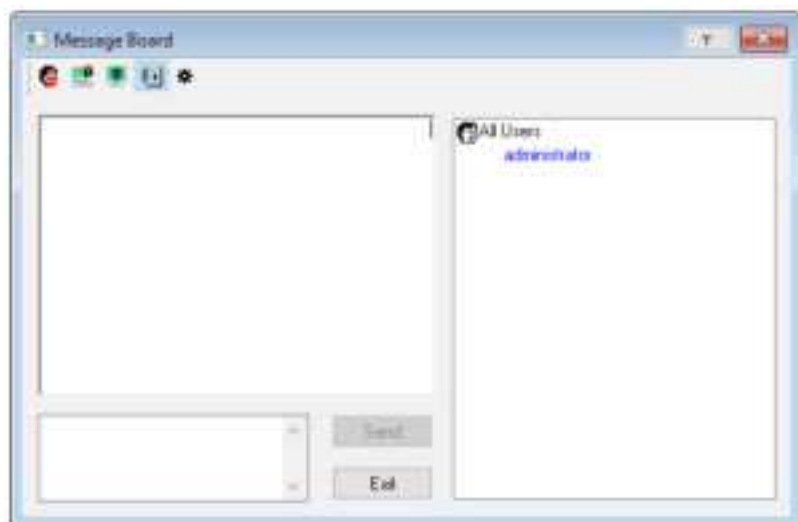
Compose Panel

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, the Disable icon displays before the user's name to indicate so.
- ◆ If a user has occupied the KVM or the KM, the Occupy 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 50 to “Virtual Media” first.

Virtual Media also supports smart card reader function, allowing a reader connected to the client PC to appear as if plugged into the remote server.

Virtual Media Icons

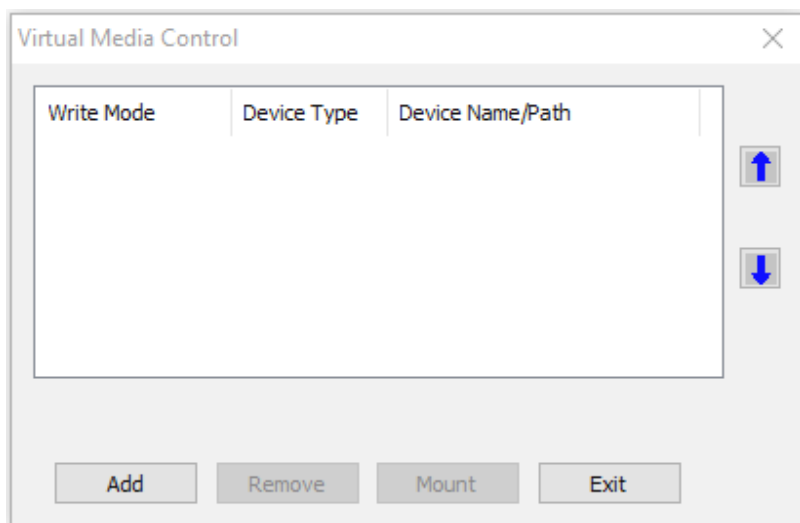
The *Virtual Media* icon on the **Control Panel** changes to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

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.

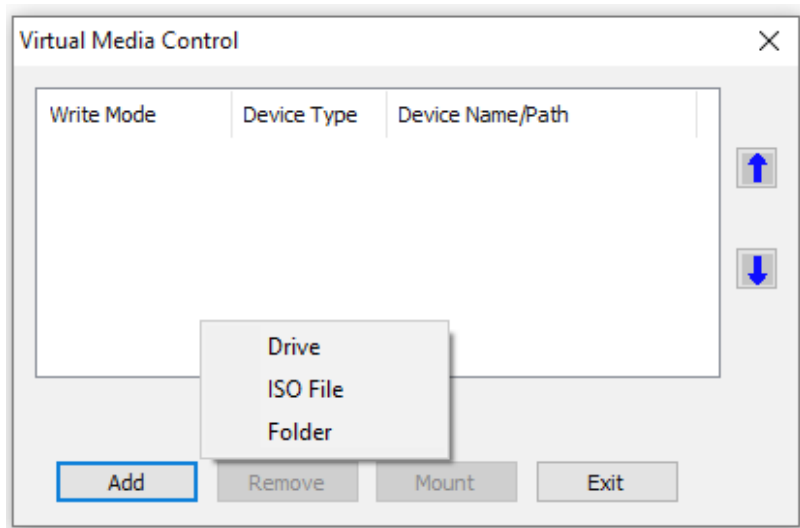
Virtual Media Redirection

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.

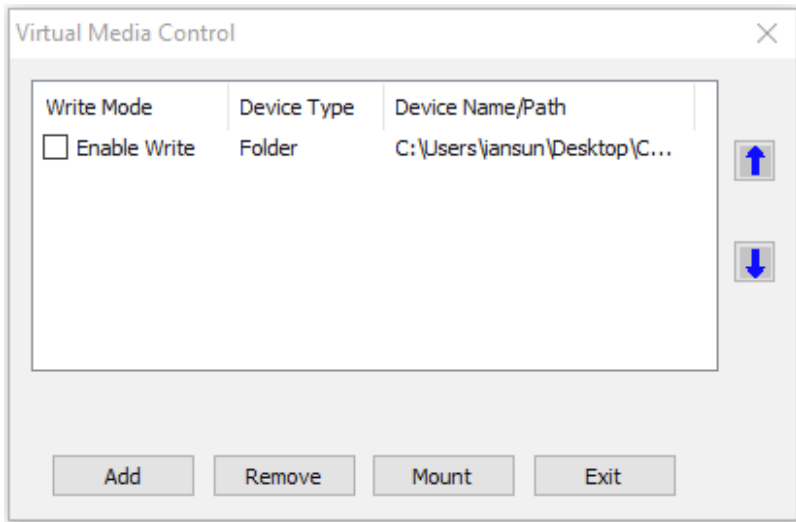


Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 131 for details about mounting these media types.

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 131, 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.



Zoom / Scale Window Size

The *Zoom* icon controls the zoom factor of the remote view window and the size of the window, as explained below:

Setting	Option	Description
Scale Window Size	100%	Sizes and displays the window at the percentage set.
	75%	
	50%	
	25%	
Zoom		Sets the zoom factor of the contents displayed as according to the server's video resolution.
		Sets the zoom factor of the contents displayed so that they're fitted to the size of the window.
		Sets the zoom factor of the contents displayed so that they're fitted to the width of the window.
		Sets the zoom factor of the contents displayed so that they're fitted to the height of the window.



The On-Screen Keyboard

The CN800 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:

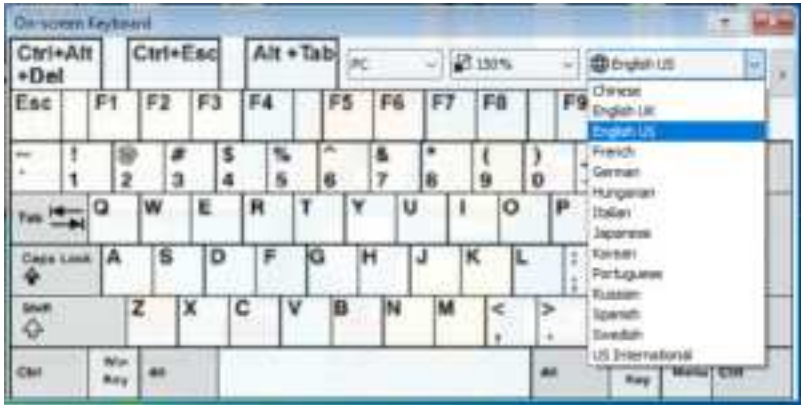


One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems are not the same, you do not have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer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

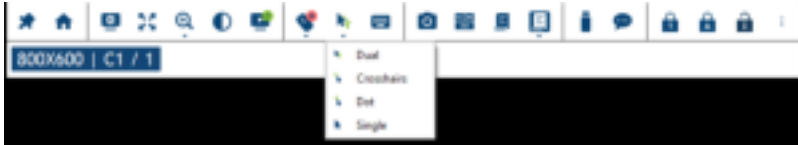
To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.





Mouse Pointer Type

The CN800 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 70 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 syncing of the remote and local mouse pointers – eliminating the need to constantly resync the two movements.

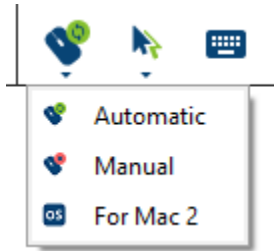
Manual Mouse Synchronization

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 70, 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 129, for instructions.

Mac and Linux Considerations

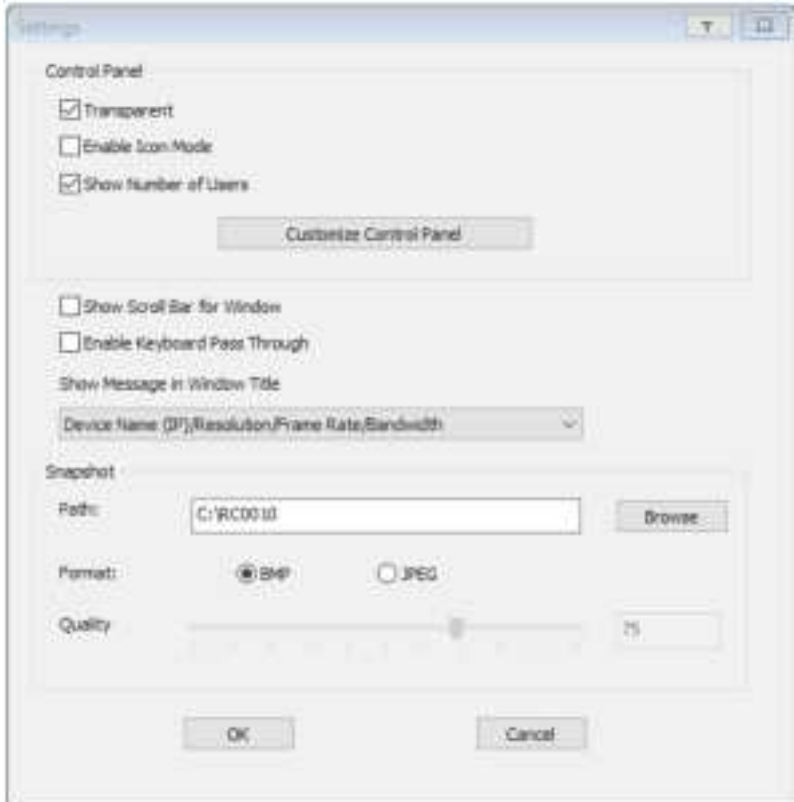
- ♦ For Mac OS versions 10.4.11 or later, there is a second DynaSync setting to choose from. If the default Mouse DynaSync result is not satisfactory, try the **Mac 2** setting. To select Mac 2, right click in the text area of the Control Panel and select *Mouse Sync Mode* → *Automatic for Mac 2*:



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.

⋮ Customize 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
Control Panel Style	◆ Enabling <i>Transparent</i> makes the Control Panel semi-transparent, so that you can see through it to the display underneath. ◆ Enabling <i>Enable Icon Mode</i> 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. ◆ Enabling <i>Show Number of Users</i> shows the number of the bus you are on, as well as the total number of users on the bus, displays on the bottom row center of the Control Panel as follows: Bus No./ Total Users. (see the Control Panel diagram on page 65 for an example.)
Customize Control Panel	Allows you to select which icons are displayed in the Control Panel. Check the ones you wish to see, uncheck the ones you don't want.
Show Scroll Bar for Window	In case where the remote screen display is larger than your monitor, you can choose how to scroll to the areas that are off-screen. When this is enabled, the show bar for windows allows scroll bars to appear around the screen borders that you can use to scroll to the off-screen areas.
Enable 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.
Show Message in Window Title	Use the drop-down menu to select which remote server information is displayed on the window title such as port name, device name, resolution, frame rate, and bandwidth.
Snapshot	These settings let the user configure the CN800's screen capture parameters (see the <i>Snapshot</i> description under <i>The Win / Java Client Control Panel</i>, page 65): ◆ 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.

Chapter 7

The Log File

The Log File Screen

The CN800 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 99.

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

This Page Intentionally Left Blank

Chapter 8

The Log Server

The Log Server is a Windows-based administrative utility that records all the events that take place on selected CN800 units and writes them to a searchable database.

Installation

1. In the web GUI, go to the Download page. Refer to *Download*, page 56 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 33 for details.

2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver.
See *The Log Server*, page 128 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 CN800 units in the middle (see *The Log Server Main Screen*, page 105, 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 CN800 List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new device units to the CN800 List, edit the information for units already on the list, or delete device units from the list.

- ◆ To add a CN800 to the List, click **Add**.
- ◆ To edit or delete a listed CN800, first select the one you want in the 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:

The screenshot shows a standard Windows-style dialog box titled "Add a Server". It includes a close button (X) in the top right corner. The form contains the following elements: an "Address" field with a blue placeholder text "Server Address"; a "Port" field with the value "9001"; two empty text boxes for "Username" and "Password"; a "Description" field with the placeholder "Server Description"; a "Limit" field with the value "100" followed by the text "Days"; a "Save to:" label followed by a text box and a "Browse..." button; two checkboxes, "Enable username/password authentication" and "Enable automatic export for every" (the latter followed by a "Days" field); and "OK" and "Cancel" buttons at the bottom.

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

Field	Explanation
Address	This can either be the IP address of the CN800 or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the CN800 in the ANMS settings (see <i>ANMS</i> , page 31).
Port	Key in the port number that was specified for the Log Server's <i>Service Port</i> in the ANMS settings (see <i>Log Server</i> , page 33).
Enable Username/ Password Authentication	Check this to enable username and password authentication.

Username	Enter the username here for authentication.
Password	Enter the password here for authentication.
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:

Search Dialog

Search Options

- ☒ New search
- ☐ Search last results
- ☐ Search excluding last results

Device List

Priority List

Start date: 1/1/2005 Start time: 2:34:40 PM End date: 1/1/2005 End time: 2:34:40 PM Pattern:

Result:

Search Print Export Exit

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

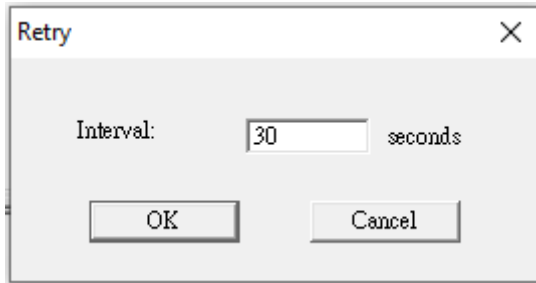
Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected CN800.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected CN800 <i>excluding</i> the events that resulted from the last search.
Server List	CN800 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. <i>Least</i> is the most general; <i>Most</i> 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 <i>hands</i> and <i>hoods</i> .
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 102).

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. Click About LogServer to see the LogServer version information.

- The upper (List) panel lists the CN800 units that have been selected for the Log Server to track (see *Configure*, page 101).
- The lower (Event) panel displays the log events for the currently selected CN800 (the highlighted one - if there are more than one). To select a CN800 unit in the list, simply click on it.



The List Panel

The List panel contains six fields:

Field	Explanation
ID / State	Shows the ID number of the device and determines whether the Log Server records the ticks for this unit, or not. If the ID checkbox is checked, the State field displays <i>Recording</i> , and the ticks are recorded. If the ID checkbox is not checked, the State field displays <i>Paused</i> , and the ticks are not recorded. Note: Even though a unit is not the currently selected one, if its Recording checkbox is checked, the Log Server will still record its ticks.
Address	This is the IP Address or DNS name that was given to the CN800 when it was added to the Log Server (see <i>Configure</i> , page 101).
Port	This is the port number that was assigned to the CN800 when it was added to the Log Server (see <i>Configure</i> , page 101).
Connection	If the Log Server is connected to the CN800, this field displays <i>Connected</i> . If it is not connected, this field displays <i>Waiting</i> . 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 31) and specified in the <i>Configure</i> dialog box (see <i>Configure</i> , page 101).
Days	This field displays the number of days that the CN800's log events are to be kept in the Log Server's database before expiration (see <i>Configure</i> , page 101).
Description	This field displays the descriptive information given for the CN800 when it was added to the Log Server (see <i>Configure</i> , page 101).

Panel Showing Logs of the Selected Units

The lower panel displays tick information for the currently selected CN800. 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.

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.
- ♦ 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.
- ♦ 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, 0.75mm², 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 iv.

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.

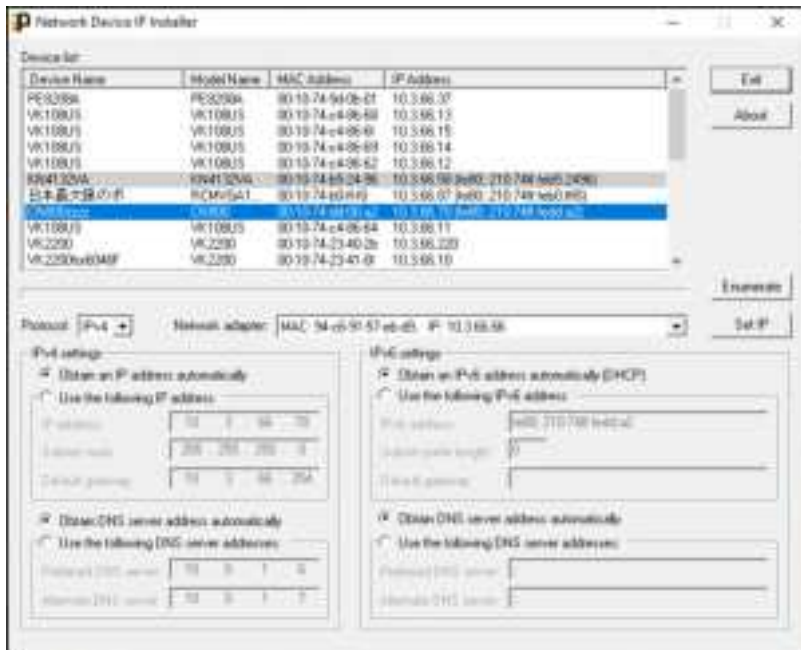
IP Address Determination

If you are an administrator logging in for the first time, you need to access the CN800 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 CN800. After you have connected and logged in you can give the CN800 its fixed network address. (See *Network*, page 27.)

IP Installer

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

1. On the CN800 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 CN800 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 CN800'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 CN800.)
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 CN800 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 CN800's IP address can be determined with the Windows AP program (see *The Windows Client AP*, page 61). When you run the program it searches the network segment for CN800 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 29 for details.

IPv6

At present, the CN800 supports two IPv6 address protocols: *Link Local IPv6 Address*, and *IPv6 Stateless Autoconfiguration*

Link Local IPv6 Address

At power on, the CN800 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 CN800's IPv4 address and click the *Basic Setting* icon. The address is displayed at the bottom of the *Basic Setting* page (see page 18).

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. 62).

-
- Note:**
1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the CN800
 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 CN800's network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the CN800 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 61).

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 CN800 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

PC compatible (101/104 key) keyboards 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.





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

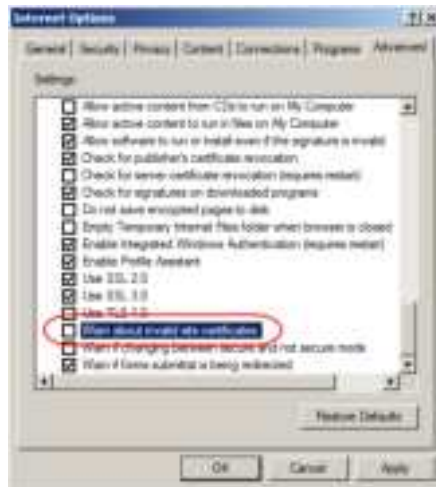
If the site name or IP address used for generating the certificate no longer matches the current address of the CN800 a mismatch warning occurs:



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=yourorganization/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 45).

Troubleshooting

General Operation

Problem	Resolution
Erratic operation	The CN800 needs to be started before the KVM switch 1. If the CN800 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 CN800, reset or restart the KVM switch. The CN800 needs to be reset (see <i>Upgrade Main Firmware</i>, page 21, point 1).
I can't access the CN800, even though I have specified the IP address and port number correctly.	If the CN800 is behind a router, the router's <i>Port Forwarding</i> (also referred to as <i>Virtual Server</i>) feature must be configured. See <i>Port Forwarding</i> , page 116, 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 <i>Toggle Mouse Display</i> function to shrink the non-functioning pointer. See page 70 for details.
Mouse movement unsynchronized	If you find the mouse pointer movement of a connected PC/server using PS/2 control (CN9000) is not in sync with your remote mouse operation, you can do the following: 1. On the connected PC/server, turn off "Enhance pointer precision" in its mouse settings. If the problem persists, go to Step 2. 2. On the web browser of the CN9000, execute terminal command "<i>setportatt 1 <n></i>" to set mouse delay time by 'n' milliseconds. You can start with n = 10, and then adjust as needed. See <i>Ping Host</i>, page 25. 1. This problem may also occur on connected PC/server using USB mouse control without absolute coordinate support (CN9600/CN9950). 2. To reset the mouse delay time back to default, execute terminal command "<i>setportatt 1 0</i>".
Mouse movement extremely slow	There is too much data being transferred for your connection to keep up with. Lower the video quality (see <i>Video Settings</i> , page 79) so that less video data is transmitted.
Changing Mouse Sync Mode to Manual makes the CN800 crash.	The CN800 has not crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the CN800 to get it going right away (see <i>Upgrade Main Firmware</i> , page 21, point 1).

Problem	Resolution
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 CN800 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 CN800.
The Windows Client link does not appear in the <i>Remote Console Display</i> 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 CN800 with a browser; open a viewer; on the control panel set <i>Mouse DynaSync</i> to Manual . See page 93 for details.
My ATEN over IP unit is not listed in the Device List of IP Installer.	◆ Make sure the Broadcast function is enabled from your switch or router in order for the auto-discover to work properly. ◆ Make sure to turn off your firewall and/or antivirus software temporarily in order for the audio-discover to work properly. ◆ Make sure the ATEN over IP unit and the PC are under the same network segment.
When connecting the CN800 to certain computers or devices with specific resolutions, the display may experience flickering or ripple effects.	If you find the display is having flickering or ripple issues, you can do the following: 1. Access the Web GUI and navigate to Maintenance > Ping Host. See <i>Ping Host</i>, page 25 for details. 2. Enter the command: "tc setvideo 1" and execute it to enable fine-tune function. 3. Log in to the WinClient to display the video output. 4. Use Alt + Left Arrow or Alt + Right Arrow on the keyboard to fine-tune the display settings and eliminate flickering or ripple issues. 5. To close this fine-tune function, access the Web GUI and navigate to Maintenance > Ping Host. See <i>Ping Host</i>, page 25 for details. Enter the command: "tc set-video 0" and execute it.

Windows

Problem	Resolution
When I log in, the browser generates a <i>CA Root certificate is not trusted</i> , or a <i>Certificate Error</i> response.	1. The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See <i>Trusted Certificates</i>, page 118, for details. 2. You can eliminate this message by importing a certificate issued by a recognized third party certificate authority (see <i>Obtaining a CA Signed SSL Server Certificate</i>, page 45).
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 <i>Continue to the website (not recommended)</i> to go on, or you can disable mismatch checking. See <i>Mismatch Considerations</i> , page 120 for a complete explanation of this topic.
Remote mouse pointer is out of step.	1. Check the status of the <i>Mouse DynaSync Mode</i> setting (see <i>Mouse DynaSync Mode</i>, page 93). If it is set to <i>Automatic</i>, change the setting to <i>Manual</i> and refer to the information provided. 2. If you are in Manual mode, use the <i>AutoSync</i> feature (see <i>Video Settings</i>, page 79), to sync the local and remote monitors. 3. If that does not resolve the problem, use the <i>Adjust Mouse</i> feature (see <i>Adjust mouse</i>, page 70) to bring the pointers back in step. 4. If the above fails to resolve the problem, refer to <i>Additional Mouse Synchronization Procedures</i>, page 129, for further steps to take.
Part of remote window is off my monitor.	Use the <i>AutoSync</i> feature (see <i>Video Settings</i> , page 79), 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.
My anti-virus program reports that there is a Trojan after I access the CN800 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 69, *Mouse DynaSync Mode*, page 93, and *Sun / Linux*, page 130. For other problems, see the table below:

Problem	Resolution
Java Applet won't connect to the CN800	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 CN800'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 CN800's <i>On-Screen Keyboard</i> and be sure that the local and remote computers are set to the same language. (See <i>The On-Screen Keyboard</i> , page 90.)
When I log in, the browser generates a <i>CA Root certificate is not trusted</i> , or a <i>Certificate Error</i> response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See <i>Trusted Certificates</i> , page 118, 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: - Go to OK mode and issue the following commands: <pre>setenv output-device screen:r1024x768x60</pre> <pre>reset-all</pre> Under XWindow: - Open a console and issue the following command: <pre>m64config -res 1024x768x60</pre> - Log out - 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: - Go to OK mode and issue the following commands: <pre>setenv output-device screen:r1024x768x60</pre> <pre>reset-all</pre> Under XWindow: - Open a console and issue the following command: <pre>m64config -res 1024x768x60</pre> - Log out - 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 <i>Manual</i> as the <i>Mouse DynaSync Mode</i> choice, and sync the pointers manually. See <i>Mouse DynaSync Mode</i>, 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 <i>Customization</i> , page 50). 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.

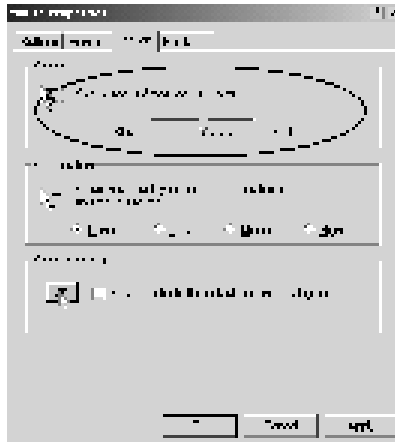
Additional Mouse Synchronization Procedures

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

Windows:

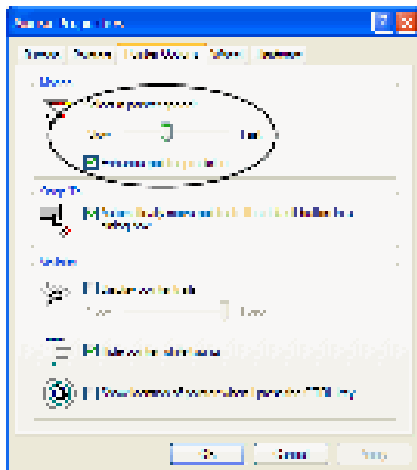
Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

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)

- Click the *Pointer Options* tab
- Bring the mouse speed to the middle position (6 units in from the left)
- 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 CD ROM/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 85). 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 2-GB limitation.

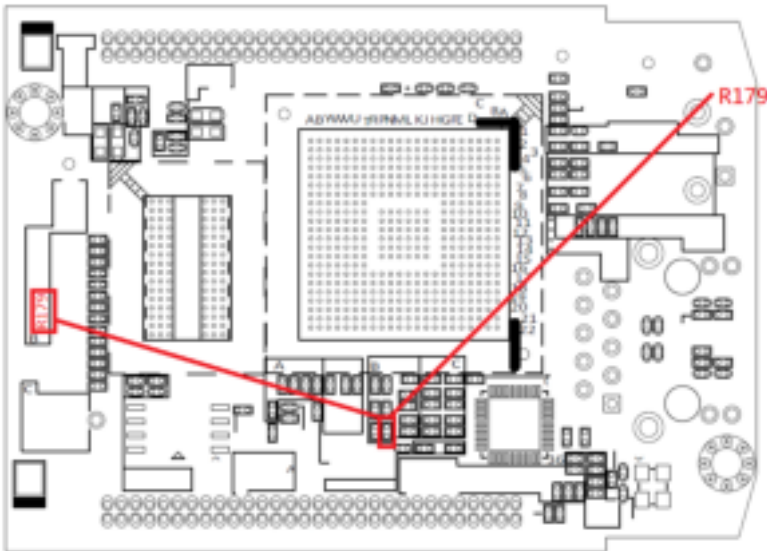
Administrator Login Failure

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 system database information.

Note: Disassembling the device will void the warranty. Improper handling may also cause permanent damage. Please contact your local service center or ATEN technical support before attempting this procedure.

To clear the system database information, do the following:

1. Power off the CN800 by disconnecting all the USB Type-A connectors.
2. Use a jumper cap to short the jumper on the mainboard as shown below.



3. Power on the CN800 by connecting all the USB Type-A connectors.
4. When the power LED flashes, power off the CN800.
5. Remove the jumper cap.
6. Close the housing and power on the CN800.

After you clear and reset the system database, you can use the default Username and Password (see page 14, and page 62) to log in.

Specifications

CN800

Connectors	
KVM (Computer) Ports	1 x USB Type-A Male (Purple) 1 x USB Type-A Male (Black) 1 x VGA Male (Blue)
LAN Ports	1 x RJ-45 Female
Switches	
Reset	1 x Semi-recessed Pushbutton
LEDs	
Power	1 (Green)
Link	1 x Link (Orange / Green) 1 x Active (Green)
Emulation	
Keyboard / Mouse	USB
Video	
Remote	up to 1920 x 1200 @ 60 Hz
Power Consumption	
DC5V:3.47W:16BTU/h	
Note:	
♦ The measurement in Watts indicates the typical power consumption of the device with no external loading. ♦ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Environment	
Operating Temperature	0 – 50 °C
Storage Temperature	–20 – 60 °C
Humidity	0 – 80% RH, Non-condensing
Physical Properties	
Housing	Plastic
Weight	0.17 kg (0.37 lb)
Dimensions (L x W x H)	9.32 x 5.66 x 2.44 cm (3.67 x 2.23 x 0.96 in)

ATEN Warranty Policy

The warranty policy may vary by product category and region of purchase. For details, please visit ATEN's official website, select your purchase counties/regions and then go to the Support Center, or contact your local ATEN sales representative for further assistance.

© Copyright 2025 ATEN® International Co., Ltd.
Released: 2025-07-01

ATEN and the ATEN logo are registered trademarks of ATEN International Co., Ltd. All rights reserved. All other brand names and trademarks are the registered property of their respective owners.