



**Single Port KVM over IP Switch with Single Port Power Switch
KN1000A
User Manual**



EMC Information

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

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

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

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

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

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

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)

이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .



RoHS

This product is RoHS compliant.

User Information

Online Registration

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

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

Telephone Support

For telephone support, call this number:

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

User Notice

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

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

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

Package Contents

The basic KN1000A package consists of:

- ◆ 1 KN1000A
- ◆ 1 Custom KVM Cable Sets
- ◆ 1 Custom Console Cable Set
- ◆ 1 Mini USB to Type A USB Cable
- ◆ 1 Power Adapter
- ◆ 1 Outlet Power Cord
- ◆ 1 Mounting Kit
- ◆ 1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the KN1000A installation.

* Features may have been added to the KN1000A since this manual was published. Please visit our website to download the most up-to-date version.

Copyright © 2017 ATEN® International Co., Ltd.

Manual Date: 2018-06-15

Altusen and the Altusen 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.

Content

EMC Information	ii
RoHS	iii
User Information	iv
Online Registration	iv
Telephone Support	iv
User Notice	iv
Package Contents	v
Content	vi
About This Manual	xii
Conventions	xiii
Product Information	xiii
Terminology	xiv

1. Introduction

Overview	1
Features and Benefits	3
System Requirements	7
Remote User Computers	7
Servers	7
Cables	8
Video	9
Operating Systems	9
Browsers	10
Components	11
Front View	11
Rear View	12
Custom Console Cable	13

2. Hardware Setup

Mounting	15
Rack Mounting	15
DIN Rail Mounting	17
Installation	18

3. Browser Login

Introduction	21
Logging In	21

4. Configuration

Introduction	23
Basic Setting	24
User Management	24
Role	24
Permissions	25
Sessions	26
Maintenance	27
Upgrade Main Firmware	27
Backup / Restore	28
Ping Host	30
Advanced Setting	31
Device Information	31
General	31
Network	32
IP Installer	33
Service Ports	33
IPv4 Settings	34
IPv6 Settings	35
Network Transfer Rate	35
DDNS	35
ANMS	36
Event Destination	36
SMTP Settings	37
Log Server	38
SNMP Server	38
Syslog Server	38
Authentication	39
RADIUS Settings	39
LDAP Settings	40
The Permission Attribute Value (for RADIUS and LDAP)	41
Permission String Characters	41
CC Management Settings	42
Security	42
Login Failures	42
Filter	43
Account Policy	46
Encryption	46
Working Mode	48
Private Certificate	49
Obtaining a CA Signed SSL Server Certificate	49
Certificate Signing Request	50
Power Management	52
Outlet Settings	53
Schedule	55
Auto Ping	57

Serial Console (COM 2)	58
PON Device	58
Enable 2-Wire RS232	58
Console Management	60
OABC	60
Serial Console	63
Date/Time	64
Customization	66
Preferences	68
User Preferences	68
Settings	68
Password	69
Log	69
Remote Console	70
Download	71
About	71
View and Logout	71

5. The WinClient Viewer

Starting Up	73
Navigation	74
The WinClient Control Panel	74
Control Panel Functions	76
Macros	79
Hotkeys	79
User Macros	81
Search	85
System Macros	85
Video Settings	88
Gamma Adjustment	90
Message Board	91
The Button Bar	91
Message Display Panel	92
Compose Panel	92
User List Panel	92
Virtual Media	93
Virtual Media Icons	93
Virtual Media Redirection	93
Smart Card Reader	96
Zoom	97
The On-Screen Keyboard	98
Mouse Pointer Type	100
Mouse DynaSync Mode	100
Automatic Mouse Synchronization (DynaSync)	100
Mac Considerations	101

Manual Mouse Synchronization	101
Open GUI	102
Customize Control Panel	103

6. The JavaClient Viewer

Introduction	105
Navigation	106
The JavaClient Control Panel	107
Control Panel Functions	108
Macros	110
Hotkeys	110
User Macros	111
System Macros	111
Search	112
Video Settings	112
Message Board	113
Virtual Media	115
Zoom	115
The On-Screen Keyboard	117
Mouse Pointer Type	117
Mouse DynaSync Mode	118
Control Panel Configuration	118

7. Local Console

Introduction	119
Laptop USB Console	119
Laptop USB Console Main Page	120

8. The Log Server

Installation	121
Starting Up	122
The Menu Bar	123
Configure	123
Events	124
Search	124
Maintenance	125
Options	126
Help	126
The Log Server Main Screen	127
Overview	127
The List Panel	128
The Tick Panel	128

9. AP Operation

Introduction	129
The WinClient AP	130
Logging In	131
The File Menu	132
The Java Client AP	133
Starting Up	133
Logging In	135

Appendix

Safety Instructions	137
General	137
Rack Mounting	140
Consignes de sécurité	141
Général	141
Montage sur bâti	144
Technical Support	145
International	145
North America	145
IP Address Determination	146
Local IP Setup	146
IP Installer	149
Browser	150
AP Windows Client	150
IPv6	151
Link Local IPv6 Address	151
IPv6 Stateless Autoconfiguration	152
Port Forwarding	153
Keyboard Emulation	154
PPP Modem Operation	155
Basic Setup	155
Connection Setup Example (Windows XP)	156
Trusted Certificates	157
Overview	157
Installing the Certificate	158
Certificate Trusted	159
Mismatch Considerations	160
Self-Signed Private Certificates	161
Examples	161
Importing the Files	161
Troubleshooting	162
General Operation	162
Windows	164
Java	165

Sun Systems	166
Mac Systems.	167
The Log Server	167
Additional Mouse Synchronization Procedures.	168
Windows:	168
Sun / Linux	169
Supported KVM Switches	170
Virtual Media Support	170
WinClient ActiveX Viewer / WinClient AP	170
Java Applet Viewer / Java Client AP	171
Administrator Login Failure	172
Specifications	173
About SPHD Connectors	174
Limited Warranty	175

About This Manual

This User Manual is provided to help you get the most from your KN1000A system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the KN1000A System. Its purpose, features and benefits are presented, and its front and back panel components are described.

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

Chapter 3, Browser Login, describes how to log into the KN1000A with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 4, Configuration, explains the administrative procedures that are employed to configure the KN1000A's working environment, as well as how to operate the KN1000A from the local console.

Chapter 5, The WinClient Viewer, explains how to connect to the KN1000A with the Windows Client software, and describes how to use the OSD to access and control the computers connected to the unit.

Chapter 6, The JavaClient Viewer, describes how to connect to the KN1000A with the Java Applet software, and explains how to use the OSD to access and control the computers connected to the unit.

Chapter 7, Local Console, describes the use of the KN1000A from the local console and mini USB ports for console functionality.

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

Chapter 9, AP Operation, describes how to operate the KN1000A using Windows and Java programs, rather than with the browser method.

An Appendix, provides specifications and other technical information regarding the KN1000A.

Conventions


This manual uses the following conventions:

- Monospaced

Indicates text that you should key in.
- []

Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
- 1.

Numbered lists represent procedures with sequential steps.
- ◆

Bullet lists provide information, but do not involve sequential steps.
- Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
- 

Indicates critical information.

Product Information

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

International	http://www.aten.com
---------------	---

Terminology

Throughout the manual we make reference to the terms *Local* and *Remote* in regard to the operators and equipment deployed in a KN1000A installation. Depending on the point of view, users and servers can be considered *Local* under some circumstances, and *Remote* under others:

- ♦ Switch's Point of View
 - ♦ Remote users – We refer to a user as a *Remote* user when we think of him as someone who logs into the switch over the net from a location that is *remote from the switch*.
 - ♦ Local Console – The keyboard mouse and monitor connected directly to the switch.
 - ♦ Servers – The servers attached to the switch via custom KVM cables.
- ♦ User's Point of View
 - ♦ Local client users – We refer to a user as a *Local client user* when we think of him as sitting at his computer performing operations on the servers connected to the switch that is *remote from him*.
 - ♦ Remote servers – We refer to the servers as *Remote servers* when we think of them from the Local Client User's point of view – since, although they are locally attached to the switch, they are *remote from him*.

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

Chapter 1

Introduction

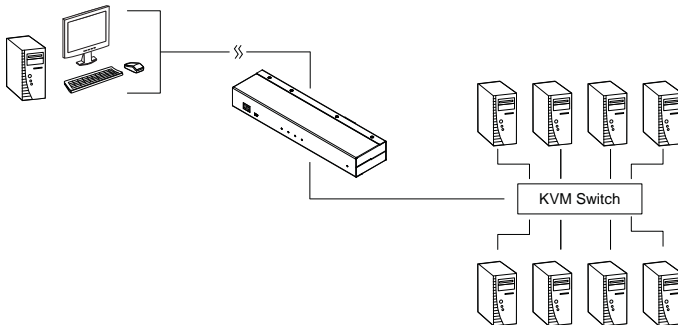
Overview

The KN1000A is a control unit that provides remote BIOS-level access to servers or “over-IP” capability to KVM switches that do not have built-in over-IP functionality. It allows operators to monitor and access their computers from remote locations using a standard Internet browser or Windows and Java based application. In addition, the KN1000A offers out-of-band access, including external modem support, and supports BIOS-level troubleshooting without the need for constant on-site IT maintenance.

To help you manage and control your entire data center environment, a built-in single-port power switch allows remote power management of a server/installation connected locally to the KN1000A. You can also add a PON* (Power Over the NET™) power management unit and remotely control the power status of devices in your installation, including monitoring their current status, as well as turning servers on, off, and rebooting them.

Note: Requires a separate purchase.

The KN1000A connects to the Internet, an Intranet, LAN, or WAN using industry-standard Cat 5e cable, then uses a custom KVM cable to connect to a local KVM switch or server. Because the KN1000A uses TCP/IP for its communications protocol, the server or KVM switch it is connected to can be accessed from any computer on the net – whether that computer is located down the hall, down the street, or half-way around the world.



(Continues on next page.)

Operators at remote locations connect to the KN1000A via its IP address. Once a connection has been established and authorization granted, the remote computer can exchange keyboard, video and mouse signals with the server (or servers on a KVM switch installation), just as if they were physically present and working on the equipment directly.

The KN1000A's Virtual Media function allows you to perform diagnostic testing, file transfers, and OS and application patches from a remote console. There is no need to physically load a CD directly to the server to perform data-related tasks – you can conveniently and efficiently troubleshoot and resolve problems at the BIOS level from anywhere.

The *Administrator* and *Client* software included with the KN1000A make it easy to install, maintain, and operate. System administrators can handle a multitude of tasks with ease – from installing and running GUI applications, to BIOS-level troubleshooting, routine monitoring, concurrent maintenance, system administration, rebooting and even pre-booting functions.

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

A *Windows Client Viewer* and a *Java Applet Viewer* are available for browser access, while *Windows Client AP* and *Java Client AP* programs are provided for non-browser GUI access. They allow IP connections and logins from anywhere on the net. Inclusion of a Java-based client ensures that the KN1000A is platform independent, and is able to work with practically all operating systems. The KN1000A also provides serial console management over the Internet, which can remotely control serial console devices such as a network switch.

The client software allows access to, and control of, the connected servers. Once an operator successfully connects and logs in, his screen displays what is running on the remote unit attached to the KN1000A (a KVM OSD display, a server's desktop, or a running program, for example) and he can control it from his console just as if he were there.

The *Log Server* records all the events that take place on selected KN1000A units for the administrator to analyze.

As an investment, the KN1000A is protected through the ability of its firmware to be upgraded over the Internet. You can stay current with the latest functionality improvements by downloading firmware update files from our website as they become available, and then using the utility to quickly and conveniently perform the upgrade.

Features and Benefits

The features and benefits provided by a KN1000A deployment are described in the following table:

Features	Benefits
Over-IP Capability for Legacy KVM Switches or KVM switches that do not have built-in over-IP functionality	<p>Protects your original KVM switch investment. No need to purchase new KVM switches to achieve the benefits of over-IP connectivity.</p> <p>Compatible KVM Switches include the following: ACS1208A, ACS1216A, CS1308, CS1316, CS1708A, CS1716A, CS1754*, CS1758*, CS9134, CS9138, KH1508A, KH1516A, KH2508A, KH2516A.</p> <p><small>*Some of the KN1000's features may not be supported, depending on the functionality of the connected KVM switch. (For example, some switches do not support virtual media.)</small></p> <p><small>*Some features found on the connected KVM switches may not be supported on the KN1000. (For example, the CS1754's audio.)</small></p>
Configuration and Operation	An easy-to-navigate graphical user interface makes for convenient, intuitive configuration and operation. Web-based Windows and Java implementations allow the remote equipment to be controlled from industry-standard web browsers. Windows and Java AP client software – using the same, convenient, GUI – are also included to provide access where a browser environment is not desired.
Remote Power Control with Wake on LAN	<p>1. A built-in single-port power switch allows remote power management of a server/installation connected locally to the KN1000A.</p> <p>2. In addition, you can also add a PON (Power Over the NET™) power management unit and remotely control the power status of devices on your installation, including monitoring their current status, as well as turning servers On, Off and Rebooting them.</p>
Superior Video	With its enhanced FPS throughput for crisp responsive video display, the KN1000A offers resolutions of up to 1920 x 1200 @ 60Hz and vibrant 24-bit color depth for rich remote session display. The remote desktop can appear full-screen, or in a window. In full-screen mode the remote desktop display scales to the user's monitor display size.
Virtual Media	USB 1.1 and 2.0 devices (floppy drives, CDROMs, flash drives, etc.), folders, and image files on a user's local system, appear and act as if they were installed on the remote server, for ease and convenience when performing software installation and system updates across the entire installation.
Virtual Remote Desktop	<ul style="list-style-type: none"> ◆ On-screen keyboard with multilanguage support ◆ Exit Macros support ◆ BIOS-level access

Features	Benefits
Smart Card / CAC Reader Support	To meet advanced security requirements, the KN1000A's Virtual Media function allows a Smart Card / CAC reader on a user's local system to be mapped to a remote server.
Built-in Single Port Power Switch	Allows remote power management of a server/installation connected locally to the KN1000A, including turning servers On, Off and Rebooting
Low Bandwidth Optimization	Bandwidth optimization via grayscale and video quality settings allow maximum data throughput in low bandwidth situations. PPP modem dialup support ensures reliable connectivity for out-of-band, and low bandwidth situations.
Multi-Platform / Multi-Protocol Support	Windows and Java client software ensures that the KN1000A and the equipment that connects to it can be accessed from most of the operating systems in use today (Windows, Linux, Unix, Sun, Mac). The KN1000A also supports a broad range of communication protocols, such as TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP, 10Base-T and 100Base-T.
Manage Browser Access Methods	Use either HTTP, HTTPS, or disable the browser.
Multi-Keyboard Language Support / On-Screen Keyboard	The KN1000A supports multiple keyboard language inputs – including English, French, German, Italian, Spanish, Japanese, Korean, and Traditional Chinese. There is no need to have a separate keyboard for each language – you can input key data in any of these languages with the KN1000A's convenient on-screen keyboard.
Multi-Users / Multi-Logins	The KN1000A supports up to 64 user accounts, and allows up to 32 concurrent user logins for single-bus access.
Message Board	To alleviate the possibility of access conflicts that may result from multiple user logins, and facilitate communication among the logged-in users, a message board – similar to an Internet chat program – allows users to communicate with each other, and provides mechanisms for a user to take exclusive control of the KVM functions.

Features	Benefits
Advanced Security	<ul style="list-style-type: none"> ◆ Advanced security features include password protection – whereby a valid username and password must be given before the client software will run – and advanced encryption technologies, such as secure 128-bit SSL. ◆ Supports SSL 128-bit data encryption and RSA 1024-bit certificates for secure users logging in from a browser. ◆ Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption. ◆ IP/MAC Filter for enhanced security protection ◆ Supports password protection ◆ Private CA
External Authentication Support	In addition to its own security protection, the KN1000A allows you to set up login authentication and authorization management from a external sources such as RADIUS, LDAP, LDAPS, and MS Active Directory.
Event Logging	The KN1000A can record all the events that take place on it and write them to a searchable database. Administrators and selected users can search for events containing specific words or strings and retrieve them according to date and order of significance.
Console Management	<ul style="list-style-type: none"> ◆ Serial console management – serial terminal access. Access the KN1000A via a built-in serial viewer, or via third-party software (such as PuTTY) for Telnet and SSH sessions. ◆ Out of Band Support – via dial up modem support. Access the KN1000A through its RS-232 port using a dial-up connection.
Upgradeable Firmware over the Internet	No need to add yet another cable to your installation – stay current with the latest functionality improvements and updates, all over the Internet.
Mouse DynaSync	No need to resync your mouse – Mouse DynaSync provides automatic locked-in synching of the remote and local mouse pointers – eliminating the need to constantly resync the two movements. Your local console mouse movement becomes the remote unit's mouse movement.
Auto-Ping	Pings a device to determine its status; if the ping test fails after a set amount of time it automatically takes an action assigned.
Supports Multiple Interfaces	<p>Supports PS/2, USB, Sun Legacy (13W3)* and serial (RS-232) connectivity</p> <p><small>*Requires CV130A converter purchase</small></p>

Features	Benefits
Full-Screen or Sizable Remote Desktop Window	Get a full screen even if your monitor's resolution is lower than the remote computer's resolution. In full-screen mode the remote desktop display scales to the user's monitor display size. Supports up to 1920 x 1200 @ 60Hz; 24-bit color depth for remote sessions.
DDNS	Allows the mapping of a dynamic IP address assigned by a DHCP server to a host name.
On/Off Scheduling for Power Outlets	Power management tasks can be scheduled on a daily, weekly, monthly or user-specified time basis
Safe Shutdown Support	IT administrators can control servers remotely and completely shut down servers before powering them off.
End Session	Administrators can terminate running sessions
Magic Panel	Special hideaway control panel with configurable function icons.

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 (see *Terminology*, page xiv). The following equipment must be installed on these computers:

- ♦ For best results, we recommend that the computers used to access the switch have at least a P III 1 GHz processor, with their screen resolution set to 1024 x 768.
- ♦ Browsers must support 128-bit SSL encryption.
- ♦ For best results, a network transfer speed of at least 128 kbps is recommended.
- ♦ For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.
- ♦ For Safe Shutdown:
 - ♦ The computer must be running Windows (2000 or higher), or Linux.
 - ♦ The *Safe Shutdown* program (available by download from our website), must be installed and running on the computer.

Servers

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

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

Cables

- ♦ One custom KVM cable set (1 USB, 1 PS/2) to link the KN1000A to a server or KVM switch are provided with this package.
- ♦ Custom KVM cable sets are available in various lengths, as shown in the table below:

Cable Type	Length	CS Part Number
PS/2	1.2 m	2L-5201P
	1.8 m	2L-5202P
	1.8 m	2L-5702P
	3.0 m	2L-5203P
	6.0 m	2L-5206P
USB	1.2 m	2L-5201U
	1.8 m	2L-5202U
	3.0 m	2L-5203U
	5.0 m	2L-5205U
PS/2-USB	1.2 m	2L-5301UP
	1.8 m	2L-5302UP
	3.0 m	2L-5303UP

To purchase additional cable sets, contact your dealer.

- ♦ One custom Console cable set to link the KN1000A to a local console is provided with this package.

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

- ♦ A USB 2.0 cable for use with the *Laptop USB Console* function (see *(LUC) Port*, page 11) is provided with this package.
- ♦ Cat 5e or higher Ethernet cable (not provided with this package), should be used to connect the KN1000A to the LAN, WAN, or Internet.
- ♦ One power cable to connect the KN1000A to the server for power management functionality is provided with this package.

Video

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

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

Operating Systems

- Supported operating systems for remote user computers that log in to the KN1000A include Windows XP (and higher), and other systems capable of running Sun's Java Runtime Environment (JRE) 6, Update 3, or higher (Linux, Mac, Sun, etc.).
- Supported operating systems for servers that connect to the KN1000A are shown in the table, below:

OS		Version
Windows		XP and higher
Linux	RedHat	7.1 and higher
	Fedora	Core12 and higher
	SuSE	11.1 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	7.1 and higher
	FreeBSD	10.1 and higher
	Sun	Solaris 10 and higher
Novell	Netware	6.5 and higher
Mac		OS X 10.7 and higher
DOS		6.2 and higher

Browsers

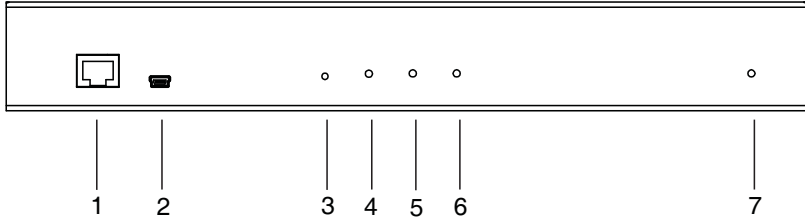
The browsers and the versions shown in the table below have been tested to support KN1000A login for the users:

Browser	Version
IE	8, 10, 11
Firefox	33, 45.2.0, 47.0
Safari*	9.1.3
Opera	38.0.2220.31
Chrome	45.0.2454.82, 51.0.270.103
Edge	25.10586.0.0

* See *Mac Systems*, page 167, for further information regarding Safari.

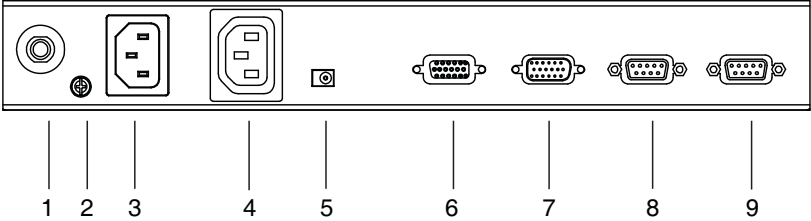
Components

Front View



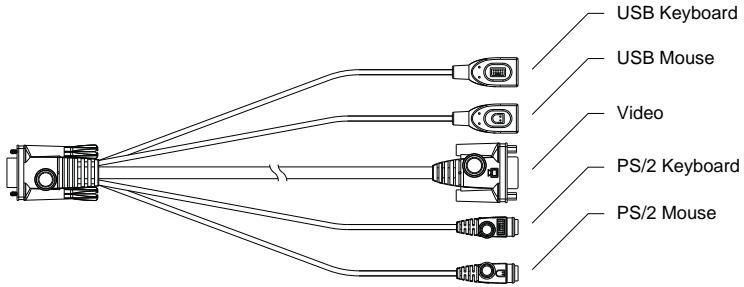
No.	Component	Description
1	LAN Port	The Cat 5e cable that connects the KN1000A to the LAN, WAN, or Internet plugs in here.
2	Laptop USB Console (LUC) Port	This port is used to connect a laptop to the KN1000A for KVM access to the computers or switch.
3	Firmware Upgrade / Reset Switch	This semi-recessed pushbutton can be used to reset the switch, or to upgrade the firmware.
4	10/100/1000 Mbps LED	The LED lights ORANGE to indicate a 10 Mbps data transmission speed. It lights ORANGE+GREEN to indicate a 100 Mbps data transmission speed. It lights GREEN to indicate a 1000 Mbps data transmission speed.
5	Link LED	Flashes GREEN to indicate that a Client program is accessing the device.
6	Power LED	Lights ORANGE when the KN1000A is powered up and ready to operate.
7	Power Outlet LED	Lights ORANGE when the server attached to the KN1000A's power outlet is powered on

Rear View



No.	Component	Description
1	Circuit Breaker	As a safety measure, if there is an overcurrent situation, the circuit breaker will trip. Press this button to recover normal operation.
2	Grounding Terminal	The wire used to ground the unit connects here.
3	Power Inlet	The power cord that connects the KN1000A to an AC power source for power management functionality plugs in here.
4	Power Outlet	The power cord provided with the KN1000A package that connects to the server for power management plugs in here. See <i>Power Management</i> , page 52.
5	Power Jack	The power adapter cable plugs in here.
6	PC/KVM Port	The KVM cable provided with this package that links the KN1000A to your server / KVM switch plugs in here.
7	PS/2 – USB Console Port	The cable for the local console (keyboard, monitor, and mouse) plugs in here. The console can use either a PS/2 or USB keyboard and mouse. Each connector is color coded and marked with an appropriate icon.
8	PON Port	This port is made available for use with a Power over the NET™ remote power management module. Refer to the User Manual that came with the PON device for operation details.
9	RS-232 Port	This serial port is provided for: 1. Serial console management (see <i>Serial Console</i> , page 63 for details); or 2. Out-of-band modem operation (see <i>OOB</i> , page 60 for details).

Custom Console Cable



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

This Page Intentionally Left Blank

Chapter 2

Hardware Setup



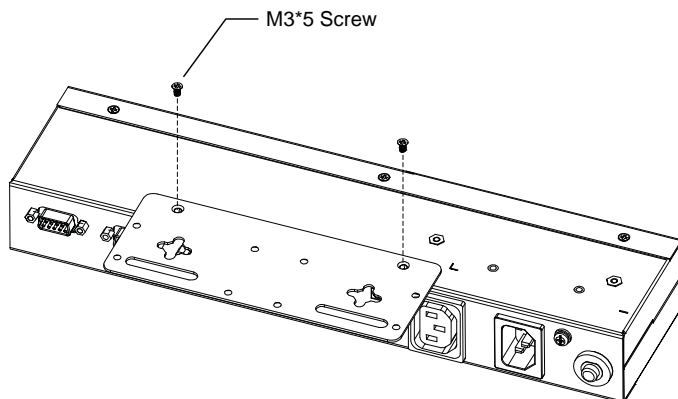
1. Important safety information regarding the placement of this device is provided on page 137. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
3. Any installation that does not follow the instructions in this guide may be hazardous.

Mounting

Rack Mounting

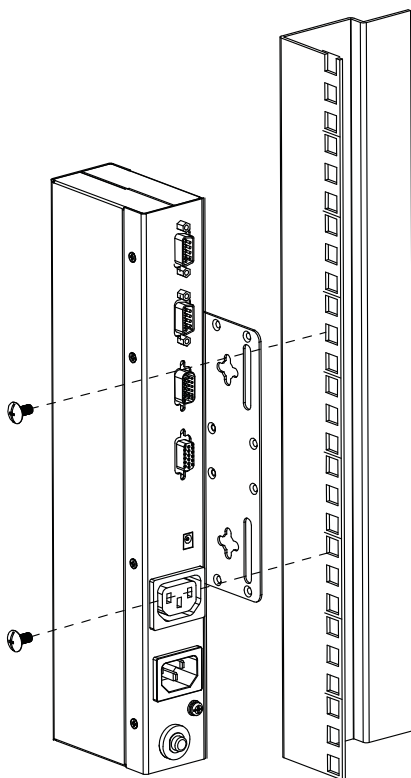
For convenience and flexibility, the KN1000A can be mounted on a system rack. To rack-mount the unit, do the following:

1. Remove the two original screws from the top/bottom of the unit (near the rear of the unit).
2. Using the screws provided with the Rack Mount kit, screw the mounting bracket into the KN1000A – as shown in the diagram below:



Note: The illustrations show the mounting bracket attached to the bottom of the unit; it can also be attached to the top.

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

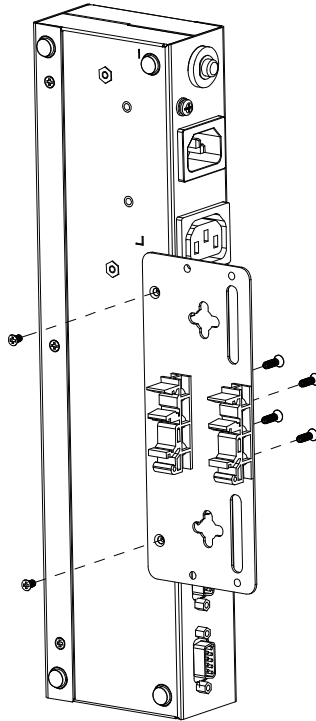


Note: Rack screws are not provided. Use screws that are appropriate for your rack.

DIN Rail Mounting

To mount the KN1000A on a DIN rail:

1. Screw the mounting bracket to the back of the KN1000A, as described in steps 1 and 2 of the rack mounting procedure.
2. Use the larger screws supplied with the Rack Mount Kit to screw the DIN rail brackets to the mounting bracket – as shown in the diagram, below:



3. Hang the unit on the DIN rail.

Installation

To install the KN1000A, refer to the installation diagrams on the following pages (the numbers correspond to the numbers of the steps), and do the following:

1. Ground the unit using a grounding wire.
2. Use the Console cable provided with this package to connect the KN1000A's *Console* port, to the local console keyboard, monitor and mouse.

Note: 1. The Console cable comes with connectors for both PS/2 and USB mice and keyboards – use the ones appropriate for your installation. See *Console Cables*, page 20 for details.

2. You can use any combination of keyboard and mouse connections. For example, you can use a PS/2 keyboard with a USB mouse. See *Console Cables*, page 20 for details.
-

3. Use the KVM cable provided with this package to connect the KN1000A's *PC/KVM* port, to the keyboard, video and mouse ports of the server or KVM switch that you are installing.

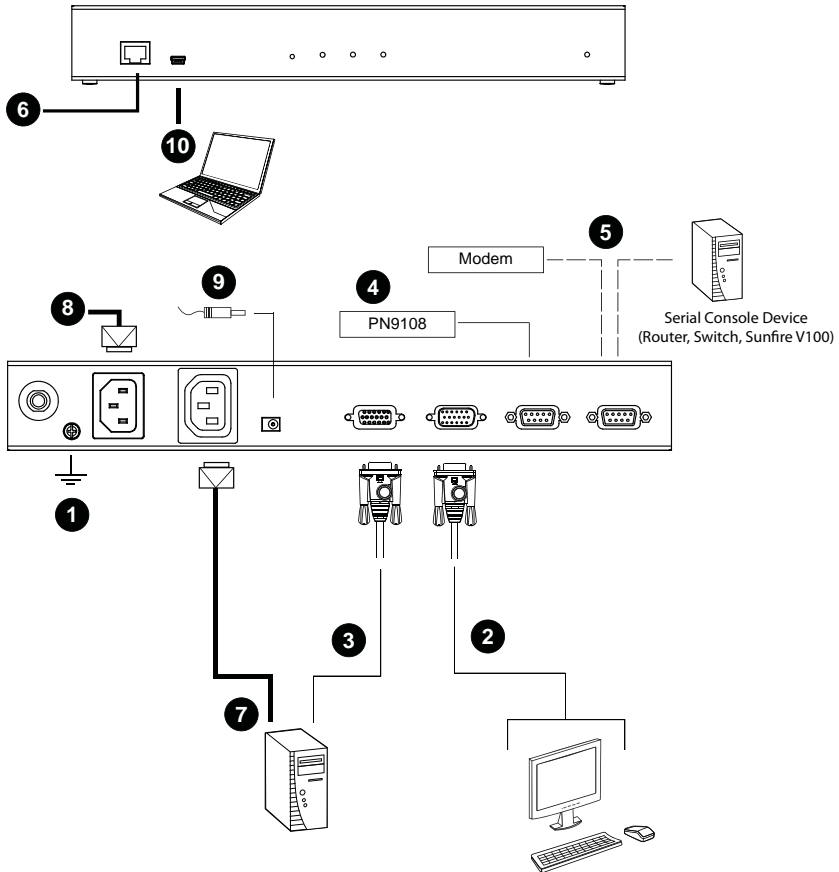
Note: The KN1000A's virtual media features may not be supported, depending on the functionality of the cascaded KVM switch (see *Supported KVM Switches*, page 170).

4. (Optional) If you want to connect a PON device for remote power management, plug its cable into the PON port.
5. (Optional) If you want to connect a serial console device or modem, plug its cable into the RS-232 port.
6. Plug the LAN or WAN cable into the KN1000A's LAN port.
7. Use the outlet power cord provided with the KN1000A package to connect the KN1000A's Power Outlet to the attached server for power management.
8. Use the power cord from the server to connect the KN1000A's Power Inlet to an AC power source.
9. Plug the power adapter cable into the KN1000A's power jack, then plug the power adapter into an AC power source.

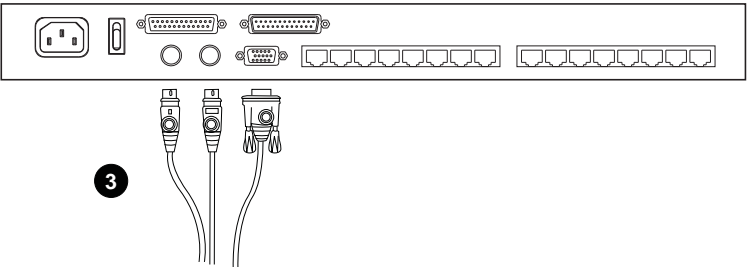
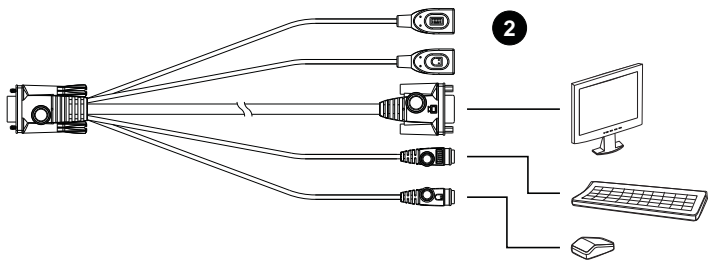
10. (Optional) If you want to use a Laptop USB Console, connect the laptop's USB to this port.

This completes the hardware installation.

Note: When starting up, be sure to first power on the KN1000A, before powering on the server or KVM switch.



Console Cables



Chapter 3

Browser Login

Introduction

The KN1000A can be accessed either from an Internet browser, Windows or Java AP (page 129), Java Applet viewer (page 105), Local Console (page 119), or by PPP modem dial-in (page 155).

Note: Windows Vista/7 users who want to use the KN1000A's Virtual Media feature must run the Internet browser as an Administrator. See *Virtual Media*, page 93, for details.

Logging In

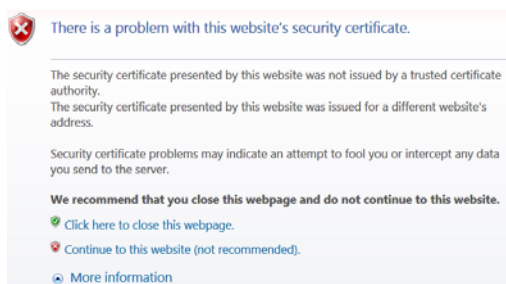
To operate the KN1000A from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the KN1000A you want to access in the browser's URL location bar.

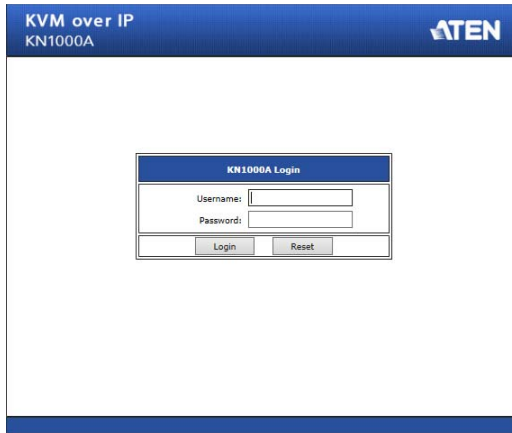
Note: 1. For security purposes, a login string may have been set by the administrator. If so, you must include a forward slash and the login string along with the IP address when you log in. For example: 192.168.0.100/KN1000A.

2. If you are the administrator, and are logging in for the first time, the various ways to determine the KN1000A's IP address are described in the Appendix on page 146.
-

2. If a *Security Alert* dialog box appears, Accept the certificate – it can be trusted. (See *Trusted Certificates*, page 157, for details.)



The KN1000A login page appears:

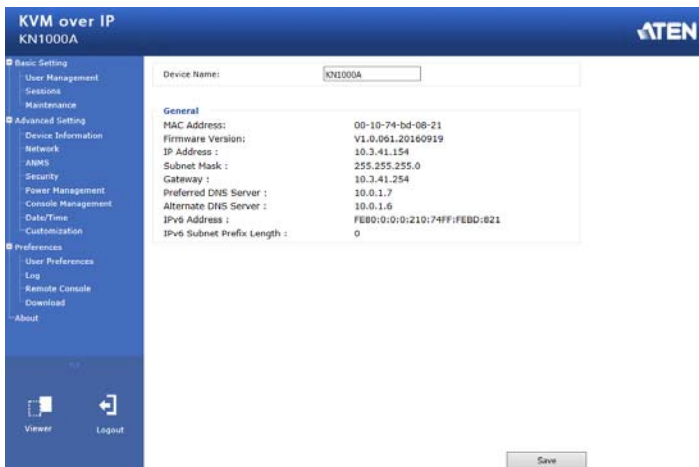
The screenshot shows the KN1000A login interface. At the top, a blue header bar contains the text 'KVM over IP' and 'KN1000A' on the left, and the 'ATEN' logo on the right. In the center of the page is a white box titled 'KN1000A Login'. Inside this box, there are two input fields: 'Username:' and 'Password:'. Below these fields are two buttons: 'Login' and 'Reset'.

3. Provide a valid Username and Password, then click **Login** to continue.

Note: 1. If you are logging in for the first time, use the default Username: *administrator*; and Password: *password*. For security purposes, we strongly recommend that you change these to something unique (see *User Management*, page 24).

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

After you have successfully logged in, the KN1000A Main Screen appears:

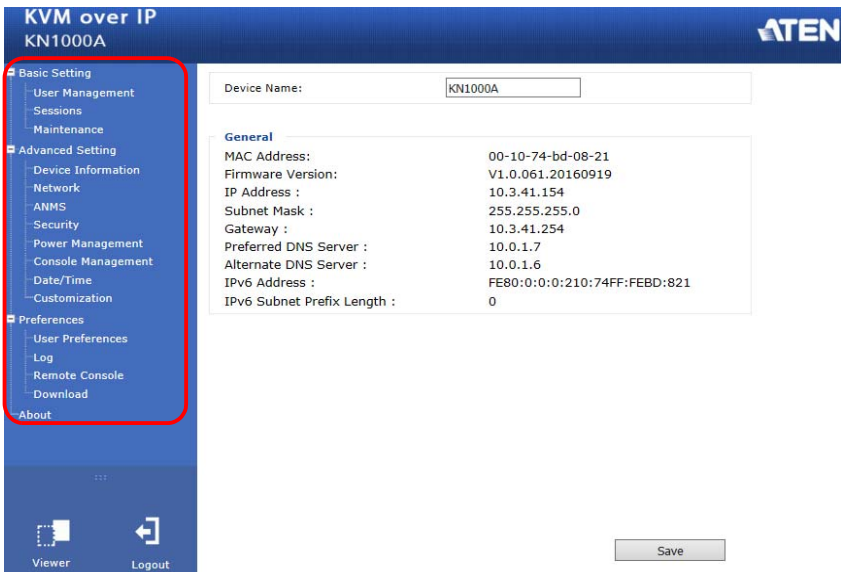
The screenshot shows the KN1000A Main Screen. It has a blue header bar with 'KVM over IP' and 'KN1000A' on the left, and the 'ATEN' logo on the right. On the left side, there is a vertical navigation menu with the following items: 'Basic Setting', 'User Management', 'Sessions', 'Maintenance', 'Advanced Setting', 'Device Information', 'Network', 'Alerts', 'Security', 'Power Management', 'Console Management', 'Date/Time', 'Customization', 'Preferences', 'User Preferences', 'Log', 'Remote Console', 'Download', and 'About'. The main area of the screen displays the 'Device Name' as 'KN1000A'. Below this, there is a 'General' section with the following information: 'MAC Address: 00-10-74-bd-08-21', 'Firmware Version: V1.0.061.20160919', 'IP Address: 10.3.41.154', 'Subnet Mask: 255.255.255.0', 'Gateway: 10.3.41.254', 'Preferred DNS Server: 10.0.1.7', 'Alternate DNS Server: 10.0.1.6', 'IPv6 Address: FE80::0:0:210:74FF:FE8D::621', and 'IPv6 Subnet Prefix Length: 0'. At the bottom left, there are two buttons: 'Viewer' and 'Logout'. At the bottom right, there is a 'Save' button.

Chapter 4

Configuration

Introduction

The administration utilities, represented by the links and icons located at the left panel of the KN1000A web page, are used to configure the KN1000A'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 KN1000A reset. To have the changes take effect, log out and then log back in again.
 3. If you do not have configuration privileges (see *User Management*, page 24), the Administration configuration dialogs are not available.
-

Basic Setting

The following sections describe the screens under *Basic Setting*, which enable users to view or edit user information and device settings, including sessions, firmware version, configuration backup/restore and EDID. 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 KN1000A, as well as modify the role and permissions of each account:

The screenshot shows the 'User Management' interface. On the left is a sidebar with a list of users, currently showing 'administrator'. The main area is titled 'User Information' and contains several input fields: 'Username:', 'Password:', 'Confirm Password:', and 'Description:'. Below these is a 'Role' section with three radio buttons: 'Administrator', 'User', and 'Select' (which is selected). Underneath is a 'Permissions' section with a grid of checkboxes for various functions: Windows Client, Config, Telnet Client, Enable Virtual Media, Java Client, System Log, SSH Client, View only, Force to Grayscale, and Power Management. There is also a 'Read Only' dropdown menu. At the bottom of the form are four buttons: 'Reset', 'Add', 'Update', and 'Remove'.

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

Role

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

- ♦ **Administrator:** Gives the user Administrator level access to the KN1000A. All permissions (except *View Only*) are granted (see permissions below).
- ♦ **User:** Gives the user User level access to the KN1000A. Windows Client, Power Manager, and Java Client permissions are granted (see permissions below).
- ♦ **Select:** This allows you to manually select the access rights of the user by selecting them in the *Permissions* section.

Permissions

Click to place/remove a check mark next to an item to grant/withhold access to that aspect of the KN1000A's operation.

- ♦ **Windows Client:** Checking this allows a user to access the KN1000A via the Windows Client software.
- ♦ **Config:** Checking this allows the user to set up and modify the KN1000A's operating environment.
- ♦ **Telnet:** Checking this allows a user to access the KN1000A via the network protocol of the same name.
- ♦ **Enable Virtual Media:** Checking this allows a user to utilize the KN1000A's Virtual Media capabilities (see *Virtual Media*, page 93 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 KN1000A via the Java Client software.
- ♦ **System Log:** Checking this allows a user to view the contents of the log file.
- ♦ **SSH Client:** Checking this allows a user to access the KN1000A via SSH sessions.
- ♦ **View Only:** Checking this restricts a user from configuring the KN1000A.
- ♦ **Power Management:** Checking this gives a user privileges to access the Power on the Net™ device being implemented on the KN1000A.
- ♦ **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 KN1000A to apply:

- ♦ *Reset* - Click this to clear the fields.
- ♦ *Add* - Click this to add the new account to the KN1000A.
- ♦ *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 at a glance all the users currently logged into the KN1000A and provides information about each of their sessions.

Username	IP	Login Time	Client	Category	Devices	Ports
administrator	10.3.41.57	2016/10/28 16:33:40	Browser	Administrator	None	
				End Session	Refresh	

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 KN1000A (Browser, WinClient AP, JavaClient AP, etc.).
- ♦ The *Category* heading lists the type of user who has logged in: Admin (Administrator), User, or Select. (See *Download*, page 71 for details about user types.)

This screen also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session**.

Click **Refresh** to update the screen.

Maintenance

The Maintenance screen allows the Administrator to upgrade the KN1000A's firmware, backup/restore the KN1000A's configuration settings and ping an IP address.

Upgrade Main Firmware

As new versions of the KN1000A 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 KN1000A; and click *Maintenance* in the left panel menu to bring up the *Upgrade Main Firmware* dialog box as follows:

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

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

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

5. After the upload completes, a message appears on the screen to inform you that the operations succeeded. Click **Logout** at the bottom left of the Main web page.
6. In the screen that comes up click **Yes** to confirm that you want to exit and reset the KN1000A.

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

Backup / Restore

The Backup / Restore screen gives you the ability to back up the KN1000A'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 KN1000A will be replaced with the information that you restore.

The image shows two web forms. The top form, titled 'Backup', has a 'Password:' label and a text input field, followed by a 'Backup' button. The bottom form, titled 'Restore', has a 'Filename:' label with a text input field and a 'Browse...' button. Below this is a 'Password:' label with a text input field. Then there are three radio buttons: 'Select All' (selected), 'User Account', and 'User Select'. Below the radio buttons is a section titled 'Options' containing two columns of checkboxes, all of which are checked: 'Device Information', 'ANMS', 'OBC', 'Customization' in the first column, and 'Network', 'Security', 'Date/Time', 'Account' in the second column. At the bottom of the 'Restore' form is a 'Restore' button.

To perform a backup, do the following:

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

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

2. Click **Backup**.

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

Note: The KN1000A saves all its backup files as *sysconfig.cfg*. If you want to save more than one backup file, simply rename the file to something convenient when you save it.

To restore a previous backup, do the following:

1. If a password was set when the backup was made, key the same password that you used to save the backup file in the *Password* field. If a password was not set, you can leave this field blank.
2. Click **Browse**; navigate to the file and select it.

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

3. Select which parts of the backup you wish to restore:
 - ♦ Select the *All* to restore both User Account and all Configuration information
 - ♦ Select the *User Account* radio button to only restore User Account information
 - ♦ Select the *User Select* radio button to choose which parts of the backed up information you wish to restore, then click the checkboxes to select/deselect the restore elements.
4. When you have made your selections, click **Restore**.

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

Ping Host

The Ping Host section enables you to ping an IP address. Enter the IP address/Hostname then click *Ping*.

Ping Host

IP address/Host Name

Ping

Result

Advanced Setting

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

Device Information

The Device Information screen provides information about the KN1000A's status. You can change the device name in this screen.

Device Name:

KN1000A

General

MAC Address:

00-10-74-bd-08-21

Firmware Version:

V1.0.061.20160919

IP Address :

10.3.41.154

Subnet Mask :

255.255.255.0

Gateway :

10.3.41.254

Preferred DNS Server :

10.0.1.7

Alternate DNS Server :

10.0.1.6

IPv6 Address :

FE80:0:0:0:210:74FF:FEBD:821

IPv6 Subnet Prefix Length :

0

General

- ◆ **Device Name:** To make it easier to manage installations that have more than one KN1000A, each one can be given a name. Enter a name (16 characters max.) for the KN1000A then click **Save**.
- ◆ **MAC Address:** The KN1000A's MAC Address displays here.
- ◆ **Firmware Version:** Indicates the KN1000A's current firmware version level and build. New versions of the KN1000A's firmware can be downloaded from our website as they become available (see *Upgrade Main Firmware*, page 27). You can reference this number to see if there are newer versions available on the website.
- ◆ **IP Address:** Displays the KN1000A'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 KN1000A's gateway address.
- ◆ **Preferred DNS Server / Alternate DNS Server:** This is the Preferred and Alternate DNS server configured for the KN1000A.
- ◆ **IPv6 Address / IPv6 Subnet Prefix Length:** Displays the KN1000A's Internet Protocol Version 6 (128 bit) address (in the new format). See *IPv6*, page 151 for details.

Network

The Network screen is used to specify the KN1000A's network environment.

IP Installer	
<input type="radio"/> Enabled	<input checked="" type="radio"/> View Only
<input type="radio"/> Disabled	

Service Ports	
Program:	9000
HTTP:	80
HTTPS:	443
SSH:	22
Telnet:	23

IPv4 Settings	
IP Address:	
<input checked="" type="radio"/> Obtain IP address automatically [DHCP]	
<input type="radio"/> Set IP address manually [Fixed IP]	
IP Address:	0,0,0,0
Subnet Mask:	0,0,0,0
Default Gateway:	0,0,0,0
DNS Server:	
<input checked="" type="radio"/> Obtain DNS server address automatically	
<input type="radio"/> Set DNS server address manually	
Preferred DNS server:	0,0,0,0
Alternate DNS server:	0,0,0,0

IPv6 Settings	
IP Address:	
<input checked="" type="radio"/> Obtain IPv6 address automatically [DHCP]	
<input type="radio"/> Set IPv6 address manually [Fixed IP]	
IPv6 Address:	
Subnet Prefix Length:	64
Default Gateway:	
DNS Server:	
<input checked="" type="radio"/> Obtain DNS server address automatically	
<input type="radio"/> Set DNS server address manually	
Preferred DNS server:	
Alternate DNS server:	

Network Transfer Rate:	99999	KBps
------------------------	-------	------

DDNS		
<input type="checkbox"/> Enable		
Host Name:		
DDNS:	dyndns.org	
Username:		
Password:		
DDNS Retry Time:	0	hour

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the KN1000A. Click one of the radio buttons to select *Enabled*, *View Only*, or *Disabled* for the IP Installer utility. See p. 149 for IP Installer details.

-
- Note:** 1. If you select *View Only*, you will be able to see the KN1000A 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 KN1000A uses for various network services.

- ♦ **Program:** This is the port number for connecting to the KN1000A from the Windows Client and Java Applet Viewers, and from the Windows and Java Client AP programs. The default is 9000.
- ♦ **HTTP:** The port number for a browser login. The default is 80.
- ♦ **HTTPS:** The port number for a secure browser login. The default is 443.
- ♦ **SSH:** The port number for a secure shell login. The default is 22.
- ♦ **Telnet:** The port number for a secure console login. The default is 23.

-
- Note:** 1. Valid entries for all of the Service Ports are from 1–65535.
2. The service ports cannot have the same value. You must set a different value for each one.
3. If there is no firewall (on an Intranet, for example), it does not matter what these numbers are set to, since they have no effect.
-

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). If a port other than the default is set, users must specify the port number as part of the IP address when they log in. If not, an invalid port number (or no port number) is specified, the KN1000A will not be found.

IPv4 Settings

The KN1000A 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 IP address automatically [DHCP]**, radio button. (This is the default setting.)
- ♦ To specify a fixed IP address, select the **Set IP address manually [Fixed IP]**, radio button and fill in the IP address, Subnet Mask, and Default Gateway.

Note: 1. If you choose *Obtain IP address automatically*, 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 KN1000A 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 146, for information.

The KN1000A 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 at the alternate DNS Server address is optional.

IPv6 Settings

The KN1000A 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 IPv6 address automatically [DHCP]**, radio button. (This is the default setting.)
- ♦ To specify a fixed IP address, select the **Set IPv6 address manually [Fixed IP]**, radio button and fill in the, IPv6 address, Subnet Prefix Length, and Default Gateway.

The KN1000A can either have its DNS server address assigned automatically, or a fixed address can be specified.

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

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

Network Transfer Rate

This setting allows you to tailor the size of the data transfer stream to match network traffic conditions by setting the rate at which the KN1000A 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 KN1000A can update the DDNS server with its IP address at certain time intervals. To enable the DDNS capability for the KN1000A, 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 KN1000A 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 and syslog server settings.

Event Destination **Authentication**

SMTP Settings

☐ Enable report from the following SMTP Server

SMTP Server:

Service Port:

☐ My server requires secure connection (SSL)

☐ My server requires authentication

Account Name:

Password:

From:

To:

☐ Report IP Address

☐ Report system reboot

☐ Report user login

☐ Report user logout

Log Server

☐ Enable

MAC Address:

Service Port:

SNMP Server

☐ Enable SNMP Agent

Server IP:

Service Port:

Syslog Server

☐ Enable

Server IP:

Service Port:

Save

SMTP Settings

To have the KN1000A 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 are connecting to a secure server, check **My server requires secure connection (SSL)**.
3. If your server requires authentication, put a check in the **My server requires authentication** checkbox, 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. Put a check on the kind of information that you want to be included in the report email:
 - ◆ Report IP Address
 - ◆ Report system reboot
 - ◆ Report user login
 - ◆ Report user logout

Log Server

Important transactions that occur on the KN1000A, such as logins and internal status messages, are kept in an automatically generated log file

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

Note: The port number must be different than the one used for the *Program* port (see *Service Ports*, page 33).

See Chapter 8, *The Log Server*, for details on setting up the log server. The *Log* is discussed on page 69.

SNMP Server

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

1. Check *Enable SNMP Agent*.
2. Key in the IP address and the port number of the computer to be notified of SNMP trap events. The valid port range is 1-65535. Default is 162.

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

Syslog Server

To record all the events that take place on the KN1000A and write them to a Syslog server, do the following:

1. Check **Enable**.
2. Key in the IP address and the port number of the Syslog server. The valid port range is 1-65535. Default is 514.

Authentication

The KN1000A allows login authentication and authorization through external programs.

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

If you want to use a RADIUS, LDAP, CC Authentication instead of the KN1000A device authentication, check **Disable Device Authentication**. Selecting this option will disable login authentication locally on the KN1000A.

RADIUS Settings

To allow authentication and authorization for the KN1000A through a RADIUS server, do the following:

☐ 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):

1. Check **Enable**.
2. Fill in the IP addresses and service port numbers for the Preferred and Alternate RADIUS servers.
3. In the *Timeout* field, set the time in seconds that the KN1000A waits for a RADIUS server reply before it times out.
4. In the *Retries* field, set the number of allowed RADIUS retries.
5. In the **Shared Secret** field, key in the character string that you want to use for authentication between the KN1000A and the RADIUS Server.

LDAP Settings

To allow authentication and authorization via LDAP or LDAPS, the Active Directory’s LDAP Schema must be extended so that an extended attribute name for the KN1000A – *KN1000A-iKVM32-userProfile* – is added as an optional attribute to the person class.

In order to configure the LDAP server, you will have to complete the following procedures: 1) Install the Windows Server Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema. Refer to the *LDAP Server Configuration Example* for further information, please see the ATEN website at www.aten.com and navigate to the Download page.

The image shows two overlapping configuration windows. The top window, titled 'AD/LDAP Settings', has an 'Enable' checkbox and a 'Type' section with radio buttons for 'LDAP' (selected) and 'LDAPS'. Below these are input fields for 'LDAP Server', 'Port', 'Admin DN', 'Timeout' (with a 'sec' unit), 'Admin Name', 'Password', and 'Search DN'. The bottom window, titled 'CC Management', has an 'Enable' checkbox (checked) and input fields for 'CC Server IP' and 'CC Service Port'.

To allow authentication and authorization for the KN1000A via LDAP / LDAPS, refer to the information in the following table.

Item	Action
Enable	Put a check in the <i>Enable</i> checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click a radio button to specify whether to use LDAP or LDAPS.
LDAP Server	Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Port	
Timeout (seconds)	Set the time in seconds that the KN1000A 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=cn8600,dc=aten,dc=com
Admin Name	Key in the Group Name for KN1000A administrator users.
Password	Key in the LDAP administrator’s password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. <i>If Enable Authorization is not checked, this field must include the entry where the KN1000A Admin Group is created. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.</i>

The Permission Attribute Value (for RADIUS and LDAP)

The attribute value for *permission* is made up of two parts: 1) the IP address of the KN1000A a user will access; and 2) a string that indicates the access rights the user has on the KN1000A at that IP address. For example:

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

The makeup of the permission entry is as follows:

- ♦ An ampersand (&) connects the KN1000A's IP with the access rights string.
- ♦ The access rights string is made up of various combinations of the following characters: c w j p l v s. The characters can be entered in upper or lower case. See *Permitted String Characters* table below.
- ♦ The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- ♦ If a user has access rights to more than one KN1000A, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.
- ♦ Use the following keyword for Radius and LDAP setting: **su/[username]** – the username must be a real user account that exists in the system.
- ♦ LDAP should use **CN8600-userProfile**, or can waive this. The login name must exist in the local account.

Permission String Characters

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
M	Allows the user to use the Virtual Media function – Read / Write

CC Management Settings

To allow authorization for the KN1000A 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.



CC Management

☒ Enable

CC Server IP: CC Service Port:

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 KN1000A, and lets you configure the login failure policies, login string, security settings, and so on.

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.



Login Failures

☒ Enable

Allowed:

Timeout: min

☒ Lock Client PC ☐ Lock Account

The meanings of the entries are explained below.

- ♦ **Login Fail Policy:** Select the login failure policy that the KN1000A 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 enabled. 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 enabled.

- ♦ **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 log in again after it has exceeded the number of allowed failures. The default is 3 minutes.

Note: If you do not enable **Login Failures**, 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 KN1000A 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 sections for IP and MAC filtering. Each section has an "Enable" checkbox, radio buttons for "Include" and "Exclude", a list box for filter entries, and "Add", "Modify", and "Delete" buttons. In the IP Filter section, the "Exclude" radio button is selected. In the MAC Filter section, the "Exclude" radio button is also selected. The "Login String:" label is positioned above a text input field.

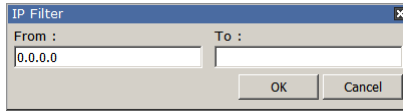
To enable IP and/or MAC filtering, put a check mark in the *IP Filter Enable* and/or *MAC Filter Enable* checkbox.

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

Adding Filters

To add an IP filter, do the following:

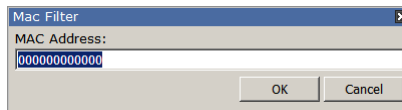
1. Click **Add**. Key in the IP address range you want to filter, and click **OK**:



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, then 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 IP Filter or MAC Filter list box and click **Modify**. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

Deleting Filters

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

The Filter section also lets administrators specify a *Login String* that users must include (in addition to the IP address) when they access the KN1000A with a browser. For example:

192.168.0.126/KN1000A

- ♦ 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 KN1000A 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

Set the parameters for the username and password.

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

- ◆ **Minimum Username Length:** Enter the minimum number (0 - 16) of characters required for a username (default is 6).
- ◆ **Minimum Password Length:** Enter the minimum number (0 - 16) of characters required for a password (default is 6).
- ◆ Check whether the password must contain at least: *One Upper Case*, *One Lower Case*, and/or *One Number* character.

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

Check *Disable Duplicate Login* to ensure that only one session for each user account is active. This prevents users from logging in with the same account at the same time.

Check *Enforce Password History* to prevent users from using the same password repeatedly. Enter the number of password changes that must occur before a previous password can be used again.

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; the greater the encryption, the greater the adverse effect. If you enable encryption, the performance considerations (going from best to worst) are as follows:

- ♦ RC4 offers the least performance impact; DES is next; then 3DES or AES.
- ♦ The RC4 + DES combination offers the least impact of any combination.

Working Mode

Use this section to set the working mode parameters.

Working Mode

- ☒ Enable ICMP
- ☒ Enable Multiuser Operation
- ☒ Enable Virtual Media Write
- ☐ Browser Service : Disable Browser ▼
- ☐ Disable Authentication

- ◆ *Enable ICMP* so that the KN1000A 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 KN1000A 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 KN1000A. Put a check in the checkbox to enable this function, then select the browser limitation in the drop down list box. Choices are explained in the following table:

Item	Explanation
Disable Browser	If this is selected, the KN1000A cannot be accessed via a browser. It can only be accessed from the AP programs (see <i>AP Operation</i> , page 129).
Disable HTTP	If this is selected, the KN1000A 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 KN1000A 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 KN1000A switch simply by entering combination of username and password.

Note: Enabling this setting creates an extremely dangerous result as far as security goes, and should only be used under very special circumstances.

Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the Private Certificate section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.

Private Certificate

Private Key :

Certificate :

Certificate Signing Request

Certificate :

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

Generating a Self-Signed Certificate

If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 161 for details about using OpenSSL to generate your own private key and SSL certificate.

Obtaining a CA Signed SSL Server Certificate

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

Importing the Private Certificate

To import the private certificate, do the following:

1. Click **Browse** to the right of **Private Key**; browse to where your private encryption key file is located; and select it.
2. Click **Browse** to the right of **Certificate**; browse to where your certificate file is located; and select it.
3. Click **Upload** to complete the procedure.

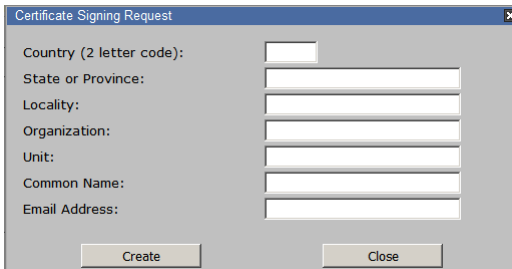
Note: Both the private encryption key and the signed certificate must be imported at the same time.

Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.

To perform this operation do the following:

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

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, there are 'Create' and 'Close' buttons.

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

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department
Common Name	mycompany.com This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is <i>www.mycompany.com</i> , and you only specify <i>mycompany.com</i> , the certificate will not be valid.

Information	Example
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 KN1000A.
- 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 **Browse** to locate the file; then click **Upload** to store it on the KN1000A.

Note: When you upload the file, the KN1000A 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**.

Power Management

The *Power Management* page has two tabs that allow you to configure the Outlet Settings and Serial Console (COM 2) settings which let you set up power management through the KN1000A.


To help you manage and control your entire data center environment, a built-in single-port power switch allows remote power management of a server/ installation connected locally to the KN1000A. You can also add a PON (Power Over the NET™) power management unit and remotely control the power status of devices in your installation, as well as turning servers on and off.

If you have the proper permission (See *User Management*, page 24), the Power Management page will bring up the KN1000A's power control interface, allowing you to reset power over the network, use the Wake on LAN feature, schedule routines, and use the Auto Ping function. These are all detailed in the sections that follow:

Outlet Settings

Serial Console (COM2)

Settings



Confirmation Required

☐ Enable

Power On Delay:

0

sec

Power Off Delay:

0

sec

Shutdown Method:

Wake on LAN

MAC:

000000000000

Schedule

Routine Type	Start Date	End Date	Day	Shutdown Time (HH:MM)	Restart Time (HH:MM)
Add				Delete	

Auto Ping

☐ Enable

Ping Address:

IP Address of device to be test

Interval:

0

(1-255)seconds

Fail Count:

0

1-99


Action:

Send Email

Outlet Settings

This section lets you set up the power management for the KN1000's power switch.

Settings




Confirmation Required ☐ Enable

Power On Delay: sec

Power Off Delay: sec

Shutdown Method: ▼

MAC:

Item	Description
	Click the Outlet icon to turn the KN1000A's power on or off. A red outlet icon indicates the power outlet is Off and a green outlet icon indicates that the power outlet is On.
Confirmation Required	If this option is enabled a dialog box comes up asking you to confirm a power operation before it is performed. If it is disabled (no check in the checkbox), the operation is performed without confirmation.
Power On Delay	Sets the amount of time the KN1000A waits after the Power Button is clicked before it turns on the power to the outlet. Note: The default delay time is 0 seconds. The maximum delay time is 999 seconds.
Power Off Delay	Sets the amount of time the KN1000A waits after the Power Button is clicked before it turns off the power to the outlet. For the System after AC Back option (see below), after the delay time expires, the KN1000A waits another fifteen seconds, then shuts the computer down. Note: The default delay time is 15 seconds. The maximum delay time is 999 seconds.

Item	Description
Shutdown Method	<p>There are three choices for the Shutdown method. Drop down the list to select a choice. The meaning of each choice is described, below:</p> <p>Wake on LAN: This is a Safe Shutdown and Restart option. If this is selected, when an Outlet is turned Off, the KN1000A first sends a message to the computer telling it to prepare for a shutdown; it then waits for the amount time set in the <i>Power Off Delay</i> field to give the OS time to close down before the computer is powered down to standby mode.</p> <p>Likewise, when the Outlet is turned On, the KN1000A waits for the amount time set in the <i>Power On Delay</i> field, then sends an Ethernet message to the computer connected to the Outlet telling the computer to turn itself On.</p> <p>Note: For Safe Shutdown and Restart, the computer must be running Windows (98 or higher), or Linux, and the <i>Safe Shutdown</i> program (available by download from our website), must be installed and running on the computer.</p> <p>System after AC Back: This is a Safe Shutdown and Restart option. If this is selected, when an Outlet is turned Off, the KN1000A first sends a message to the computer telling it to prepare for a shutdown; it then waits for the amount time set in the <i>Power Off Delay</i> field to give the OS time to close down before the computer is powered down.</p> <p>When the Outlet is turned On, the KN1000A waits for the amount time set in the <i>Power On Delay</i> field, then sends power to the server. When the server receives the power, it turns itself on.</p> <p>Note: For Safe Shutdown and Reboot, the computer must be running Windows (98 or higher), or Linux, and the <i>Safe Shutdown</i> program (available by download from our website), must be installed and running on the computer.</p> <p>Kill the Power: If this option is selected, the KN1000A waits for the amount time set in the <i>Power Off Delay</i> field, and then turns the Outlet's power Off. Turning the power off performs a cold (non-safe) shutdown.</p>
MAC	<p>In order to use either of the Safe Shutdown methods the MAC address of the computer connected to the outlet must be filled in here.</p>

Schedule

The *Scheduling* section allows you to configure specific times and dates to initiate power cycles (On/Off/Reboot) for devices connected through the KN1000A.

Schedule

Routine Type	Start Date	End Date	Day	Shutdown Time (HH:MM)	Restart Time (HH:MM)
<div>Add</div>				<div>Delete</div>	

Clicking the **Add** button in the Schedule section opens the Outlet Schedule window which lets you set power schedules for the outlet:

Outlet Schedule

Routine Type:

Once

Weekday

Sunday

Date

1

Start Date

(YYYY-MM-DD)

End Date

(YYYY-MM-DD)

Shutdown Time

08 : 08

☐ Disable

Restart Time

08 : 08

☐ Disable

Every

0

day(s)

Add

Cancel

Note: Since the KN1000A has no RTC (real time clock) circuit, the unit will get time from the NTP server or from the client PC (sync time from client PC after a system reset or losing power).

The meanings of the fields and headings are given in the table, below:

Heading	Meaning
Routine Type	Drop down the list to select whether the scheduled power configuration should take place just Once, or on a Daily, Weekly, or Monthly basis.
Weekday	This field only becomes active if you choose <i>Weekly</i> as the routine type. If you choose Weekly, drop down the list to choose which day of the week you want the power management routine to take place on.
Date	This field only becomes active if you choose <i>Monthly</i> as the routine type. If you choose Monthly, drop down the list to choose which day of the month you want the power management routine to take place on.

Heading	Meaning
Start Date	If you want to limit the power management routine to a particular time period, either click the calendar icon to select the date that the routine will start at, or key in a start date using the YYYY-MM-DD format
End Date	If you want to limit the power management routine to a particular time period, either click the calendar icon to select the date that the routine will end at, or key in an end date using the YYYY-MM-DD format
Shutdown Time	Key in the time of day you want the shutdown to take place using the HH:MM format. If you want to temporarily suspend this function without deleting the entry, click to put a check in the <i>Disable</i> checkbox at the right of this field. You can reinstate the function by unchecking the checkbox.
Restart Time	Key in the time of day you want the restart to take place using the HH:MM format. If you want to temporarily suspend this function without deleting the entry, click to put a check in the <i>Disable</i> checkbox at the right of this field. You can reinstate the function by unchecking the checkbox.
Every	For added flexibility, you can use this field to refine the Daily, Weekly, and Monthly routines. For example, if you chose <i>Daily</i> as your routine type, you could have the routine take place every 3 days (instead of every day), by keying a 3 in this field.

After you have made your schedule settings, click **Add**. The schedule is summarized in the list at the bottom of the panel. To remove the outlet's schedule, select it in the list and click **Delete**.

Routine Type	Start Date	End Date	Day	Shutdown Time (HH:MM)	Restart Time (HH:MM)
Once	2016-11-30	-----	-	08:08	08:08
Every 2 month(s)	2016-11-30	2017-11-01	23	08:08	08:08
Every 2 week(s)	2016-11-15	2017-08-01	Wed	4:08	5:08

Auto Ping

The section allows you to use an ICMP ping command to check if the attached device is functioning properly.

Auto Ping

☐ Enable

Ping Address:

IP Address of device to be test

Interval:

0

(1-255)seconds

Fail Count:

0

1-99

Action:

Send Email

▼

This function is detailed in the following table:

Enable	Put a check in the checkbox to enable this function.
Ping Address	Enter the IP address of the device to be pinged in this field.
Interval	This field sets how often the specified device is pinged, in second intervals. Enter a value between 1 and 255.
Fail Count	This field sets how many times the device is allowed to fail to respond to the ping before an action is taken (see below). Enter a value between 1 and 99.
Action	<div>This field sets what action is taken if the device fails to respond to a specified number of pings. Select one of the following actions from the drop-down menu:</div> <div>Send email: This sends an email using the SMTP server setting. For this function to work, you must also enable reports from the SMTP server. See <i>SMTP Settings</i>, page 37 for details.</div> <div>Outlet Power Off/On: This resets the power at the KN1000A's power outlet.</div> <div>Note: This action must be confirmed before saving.</div> <div>No action: Select this option to do nothing if the specified device fails to respond.</div>

Note: If Auto Ping fails, after power on, the KN1000A waits five minutes before performing the next ping operation.

Serial Console (COM 2)

This section allows you to configure the KN1000A's PON port for connecting a PN9108 (8-port Power Over the NET™) or a 2-wire RS-232 interface.

PON Device

Enable this radio button if you want to connect a PN9108 (8-port Power Over the NET™) to the KN1000's PON port. If a Power over the Net™ module is connected to your installation, click *Download PON Client* to download the KN1000's power management software for the attached PON device.

Enable 2-Wire RS232

Enable this radio button to use the PON port for a serial console. When this option is selected, the page appears for the serial communication parameters, as below:

Outlet Settings **Serial Console (COM2)**

Serial Console Setting

☐ PON Device ☒ Enable 2-Wire RS232

Settings

Port Property Settings:

Baud Rate: 9600 ▼ Data Bits: 8 ▼

Parity: None ▼ Stop Bits: 1 ▼

Flow Control: None ▼

Port Alert Settings

Alert String 1:

Alert String 2:

Note: These settings will be the same as those in the KN1000A's serial console section. See the Serial Console section under *Console Management*, page 60, for further details.

(Continues on next page.)

(Continued from previous page.)

If both RS-232 functions are enabled (PON for 2-wire RS-232 and RS-232 for a serial console), when the Telnet/SSH connection is opened, a menu appears for you to select which serial console is the primary, where Port 1 is the serial console and Port 2 is the 2-wire RS-232, as shown below:



```
10.0.0.49 - PuTTY
Welcome to the ALTUSEN KN1000
ATEN International Co. Ltd. All rights reserved.
Login:administrator
Password:
                Choose Port Menu
-----
    1. Connect to Port 1
    2. Connect to Port 2
    0. Logout

    Select one: █
```

Console Management

This section discusses methods of opening the KN1000A console via OOBBC or serial connection.

OOBC

In case the KN1000A cannot be accessed with the usual LAN-based methods, it can be accessed via the switch's modem port. To enable support for PPP (modem) operation, click to put a checkmark in the *Enable Out of Band Access* checkbox.

PPP Settings

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

Dial Back

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

Dial Back

☐ Enable Dial Back

☒ Enable Fixed Number Dial Back

Phone Number:

☒ Enable Flexible Dial Back

Use dial back phone number for the Username

Password:

- ♦ **Enable Fixed Number Dial Back:** If *Fixed Number Dial Back* is enabled, when there is an incoming call, the KN1000A hangs up the modem and dials back to the modem whose phone number is specified in the Phone Number field.

Key the phone number of the modem that you want the KN1000A to dial back to in the *Phone Number* field.

- ♦ **Enable Flexible Dial Back:** If *Flexible Dial Back* is enabled, the modem that the KN1000A dials back to does not have to be fixed. It can dial back to any modem that is convenient for the user, as follows:
 1. Key the password that the users must specify in the *Password* field.
 2. When connecting to the KN1000A's modem, users specify the phone number of the modem that they want the KN1000A to dial back to as their Username, and specify the password set in the *Password* field for their password.

Dial Out

For the dial out function, you must establish an account with an Internet Service Provider, and use a modem to dial up to your ISP account. An explanation of the Enable Dial Out items is given in the table below:

Dial Out

☒ Enable Dial Out

ISP Settings

Phone Number:

Account Name:

Password:

Dial Out Schedule

☒ Every:

☐ Daily at: :

PPP online time: minute(s)

Emergency Dial Out

☒ PPP stays online until network recovery

☐ PPP online time: minute(s)

Dial Out Mail Configuration

SMTP Server IP Address:

Service Port:

☒ SMTP server requires secure connection (SSL)

☐ SMTP server requires authentication

Account Name:

Password:

Email From:

To:

- ◆ **ISP Settings:** Specify the telephone number, account name (username), and password that you use to connect to your ISP.
- ◆ **Dial Out Schedule:** This entry sets up the times you want the KN1000A to dial out over the ISP connection. *Every* provides a listing of fixed times from every hour to every four hours.
 - ◆ If you select *Every two hours* (for example), the KN1000A will start dialing out every two hours beginning at 00:00.
 - ◆ If you do not want the KN1000A to dial out on a fixed schedule, select **Never** from the list.
- ◆ *Daily at* will dial out once a day at a specified time. Use the hh:mm format to specify the time.

- ♦ *PPP online time* specifies how long you want the ISP connection to last before terminating the session and hanging up the modem. A setting of zero means it is always on line.
- ♦ **Emergency Dial Out:** If the KN1000A gets disconnected from the network, or the network goes down, this function puts the switch on line via the ISP dial up connection.
 - ♦ If you choose *PPP stays online until network recovery*, the PPP connection to the ISP will last until the network comes back up or the switch reconnects to it.
 - ♦ If you choose *PPP online time*, the connection to the ISP will terminate after the amount of time that you specify is up. A setting of zero means it is always on line.
- ♦ **Dial Out Mail Configuration:** This section provides email notification of problems that occur on the devices connected to the KN1000A's ports.

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

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

When you have finished making your settings on this page, click **Save**.

Serial Console

To configure the KN1000A to interact with the connected serial device, you need to set its parameters to match the parameters of the device in the *Port Property Settings*.

The screenshot shows a configuration window titled 'Serial Console (COM1)'. It has a 'Port Property Settings' section with the following values: Baud Rate: 9600, Data Bits: 8, Parity: None, and Flow Control: None. Below this is a 'Port Alert Settings' section with ten empty text input fields labeled 'Alert String 1' through 'Alert String 10'. A 'Save' button is at the bottom right.

Select the values that match the ones used by the connected serial console device. The port property settings that the KN1000A supports are as follows:

- ♦ **Baud Rate:** This sets the port's data transfer speed. Choices are from 300–38400 (drop down the list to see them all). Set this to match the baud rate setting of the serial console device. Default is 9600 (which is a basic setting for many serial console devices).
- ♦ **Data Bits:** This sets the number of bits used to transmit one character of data. Choices are: 7 and 8. Set this to match the data bit setting of the serial console device. Default is 8 (which is the default for the majority of serial console devices).
- ♦ **Parity:** This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even. Set this to match the parity setting of the serial console device. Default is None.
- ♦ **Stop Bits:** This indicates that a character has been transmitted. Set this to match the stop bit setting of the serial console device. Choices are: 1 and 2. Default is 1 (which is the default for the majority of serial console devices).
- ♦ **Flow Control:** This allows you to choose how the data flow will be controlled. Choices are: None, Hardware, and XON/XOFF. Set this to match the flow control setting of the serial console device. Default is None.

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

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

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

Date/Time

The Date/Time dialog page sets the KN1000A time parameters:

Time Zone
(GMT+08:00) Taipei
☐ Daylight Savings Time

Date
November < 2016 >
November 2016

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			

Time
01 : 41 : 38
Set

Network Time
☐ Enable auto adjustment
Preferred time server
AU | ntp1.cs.mu.OZ.AU
☐ Preferred custom server IP
☐ Alternate time server
AU | ntp1.cs.mu.OZ.AU
☐ Alternate custom server IP
Adjust time every 1 days
Adjust Time Now

Set the parameters according to the information below.

Time Zone

- ♦ To establish the time zone that the KN1000A is located in, drop down the **Time Zone** list and choose the city that most closely corresponds to where it is at.
- ♦ If your country or region employs Daylight Saving Time (Summer Time), check the corresponding checkbox.

Date / Time

- ♦ Select the month from the drop-down menu.
- ♦ 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 the *Enable auto adjustment* checkbox.
2. Drop down the time server list to select your preferred time server
– or –
Check the *Preferred custom server IP* checkbox, and key in the IP address of the time server of your choice.
3. If you want to configure an alternate time server, check the *Alternate time server* checkbox, and repeat step 2 for the alternate time server entries.
4. Key in your choice for the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

Customization

Use this section to edit the device settings.

Mode

☐ Force All to Grayscale
☒ Enable Client AP Device List

USB IO Settings

OS:

Win

Language:

US English

Multiuser Mode

Multiuser Mode:

Share

Occupy Timeout:

3

 sec (0-255)

Reset

Reset Default Values

☐ Reset on exit

- ♦ If *Force All to Grayscale* is enabled, the remote displays of all devices connected to the KN1000A are changed to grayscale. This can speed up I/O transfer in low bandwidth situations.
- ♦ If *Enable Client AP Device List* is enabled, the switch appears in the Server List when using the WinClient or Java Client AP (see *The WinClient Viewer*, page 73, and *The JavaClient Viewer*, page 105). If this option is not enabled, the switch can still be connected to, but its name will not appear in the Server List.

♦ OS

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

♦ Language

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

♦ 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 *Message Board*, page 91).
 - ♦ **Occupy Timeout**
- If there is no user input for the amount of time specified here, the control privilege is released and transferred to the next user who moves the mouse or uses the keyboard.
- ♦ **Reset**

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

Click *Reset Default Values* to use the default factory settings of the KN1000A.

Preferences

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

User Preferences

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

The screenshot shows the 'Settings' section of the User Preferences screen. It includes the following elements:

- Language:** A dropdown menu currently set to 'English'.
- OSD Hotkey:** A dropdown menu currently set to '[Scroll Lock] [Scroll Lock]'.
- Logout Timeout:** A text input field containing '30' followed by a 'min' unit label.
- Launch viewer after login:** An unchecked checkbox.
- Viewer:** Two radio buttons; 'Auto Detect' is selected, and 'Java Client' is unselected.
- Buttons:** A 'Save' button is located below the Viewer settings. Below the password fields is a 'Change Password...' button.
- Password Fields:** Three text input fields labeled 'Old Password:', 'New Password:', and 'Confirm Password:'.

Settings

Set device parameters using the following fields:

- ♦ **Language:** Selects the language that the interface displays in. Drop down the list to make your selection.

Selecting **Auto** causes the KN1000A to display the pages in the same language to which the browser is set.

If your browser is set to a non-supported language, the KN1000A looks to what your server's operating system is set to. If the operating system is set to a supported language it will use that language to display its pages. If the operating system is set to a non-supported language, the KN1000A defaults to English. After making your choice, click **Save**.

- ♦ **OSD Hotkey:** Select the keyboard combination to call the OSD function.
- ♦ **Logout Timeout:** Set how many minutes the KN1000A allows a user session to last before terminating the session.
- ♦ **Viewer:** Choose the viewer you would like to use when viewing the remote server's display. This is set to **Auto Detect** by default, which opens the WinClient for Windows systems.

Password

Change your password using the following fields:

- ◆ **Old Password:** Key in the old password.
- ◆ **New Password:** Key in the new password.
- ◆ **Confirm Password:** Key in the exact same characters to verify you have entered the correct new password

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

Log

The KN1000A logs all the events that take place on it. Following a reset, it writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the center left of the page. A screen similar to the one below appears:

Time	Severity	User	Log Information
2012/12/04 15:16:54	Least	System	Log update 1
2012/12/04 15:06:47	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attempting to login via browser.
2012/12/04 15:06:21	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attempting to login via browser.
2012/12/04 15:02:30	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attempting to login via browser.
2012/12/04 15:01:07	Most	System	User administrator from 10.3.41.91 (00-18-6E-4D-DD-81) logged out via browser.
2012/12/04 15:01:06	Most	administrator	End session for user administrator.
2012/12/04 15:01:06	Most	administrator	User administrator (10.3.41.91) logged out. Online time : 00:01:25.
2012/12/04 15:01:03	Most	administrator	User administrator (10.3.41.91) logged out. Online time : 00:00:30.
2012/12/04 15:00:33	Least	administrator	User administrator changes to [01] .
2012/12/04 15:00:33	Most	administrator	User administrator logged in.
2012/12/04 15:00:33	Most	System	User administrator (10.3.41.91) attempting to login.
2012/12/04 15:00:33	Most	System	SYS: Access via windows client 10.3.41.91.
2012/12/04 15:00:33	Most	System	Sys: Connected to 10.3.41.91 (00-18-6E-4D-DD-81).
2012/12/04 15:00:19	Least	System	Get snapshot result....01B70490 9628
2012/12/04 15:00:15	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attempting to login via browser.
2012/12/04 15:00:08	Least	System	Send snapshot request...
2012/12/04 14:59:42	Most	administrator	Start session for user administrator.
2012/12/04 14:59:41	Least	administrator	User administrator changes to [01] .
2012/12/04 14:59:41	Most	administrator	User administrator logged in.


A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded.

Note: To maintain a record of all the events (not just the most recent 512), set up the Log Server AP program. See *The Log Server*, page 121, for details.

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

Remote Console

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

Remote Console Preview


Exit Macro

▼

Telnet Viewer

Telnet Viewer2

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

- ♦ Select the *Exit Macro* you would like to use and click **Save**.
- ♦ Click *Telnet Viewer* to open a remote console session utilizing the RS-232 port. A remote view window appears with options.
- ♦ To configure the PN9108 (a Power Over the NET™ device), click *Telnet Viewer2*. When connection between the devices is established, you can only use the KN1000A's IP address to access the configuration screens of the PN9108. Clicking this button opens the login page of the device.

Note: 1. Connection to the PN9108 or a Power Over the NET™ (PON) device can only be viewed and managed through the browser configuration screens; these screens are not available via the Windows or Java application (AP) programs.

2. Refer to ATEN's PN9108 User Manual (or a compatible PON device's manual) for details on editing the power management configuration screens.

Download

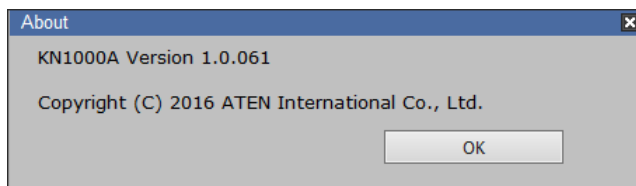
The Download page lets you download the standalone *Windows Client AP*, *Java client AP* and *Log Server AP*.



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 9 on page 129.
 - ◆ For details on the *Log Server AP*, refer to Chapter 8 on page 121.

About

Click *About* to see the current firmware version and copyright information of your KN1000A.



View and Logout

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

Click the Logout icon when you are done configuring the KN1000A's operating environment. This logs you out of the KN1000A GUI.

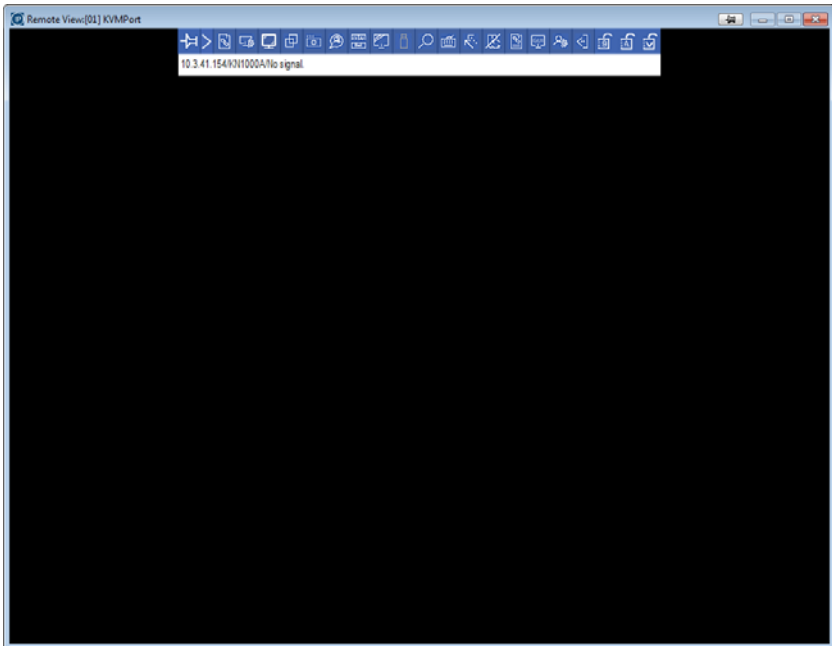
This Page Intentionally Left Blank

Chapter 5

The WinClient Viewer

Starting Up

The WinClient Viewer is available when you log into the KN1000A web GUI using a browser. After you log in (see *Logging In*, page 21), click the **Viewer** icon in the left panel menu. A second or two after, the remote server's display appears as a window on your desktop:



By default, the WinClient version of the viewer is displayed.

If you want to use the JavaClient version, see *User Preferences*, page 68 for details on how to configure this option. To navigate the Java version, refer to Chapter 6, page 105.

Navigation

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

- ♦ You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.
- ♦ You can switch between your local and remote programs with [Alt + Tab].

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

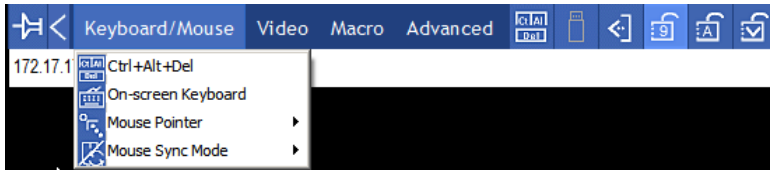
2. Due to net lag, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

The WinClient Control Panel

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



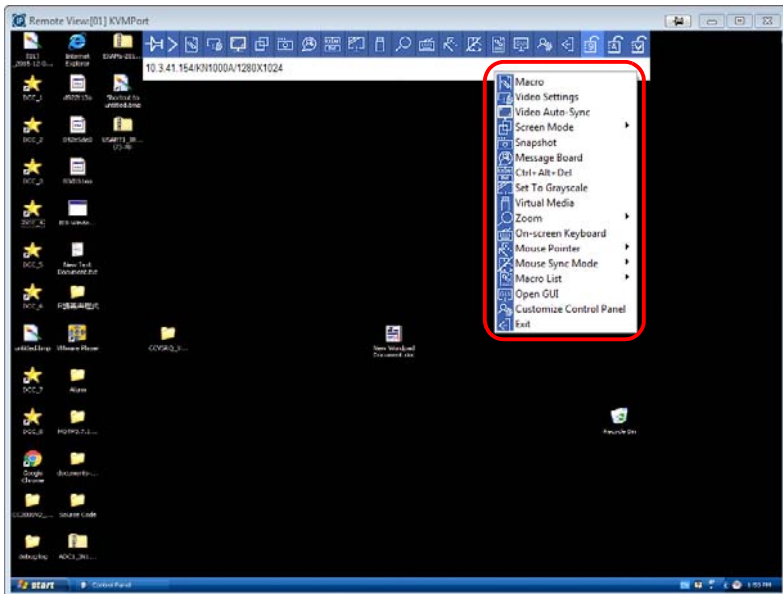
The control panel has two menu styles: at startup, only the icons are displayed. Pressing this icon (▶) changes the menu into a combination of icon + text mode as show below:



Note: 1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Customize Control Panel*, page 103, for details.

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



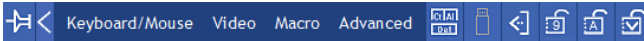





- ♦ By default, the left of the top text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, however, the information in the top text row changes to describe the icon's function. In addition, if a message from another user is entered in the message board, and you have not opened the message board in your session, the message will appear in the top row.
- ♦ If the *User Info* function has been enabled under *Customize Control Panel* (see *User Info*, page 104), the total number of users currently logged into the KN1000A displays in the center of the upper text row.
- ♦ Right clicking in the text row area brings up a menu that allows you to select options for the *Screen Mode*, *Zoom*, *Mouse Pointer type*, *Mouse Sync Mode* and *Macro List*. These functions are discussed in the sections that follow.
















Control Panel Functions

The Control Panel functions are described in the table below.

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

Icon	Function
 <p>Always on Top</p>	<p>This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.</p>
 <p>Show Menu</p>	<p>When you click this, the Control Panel format changes and you get 4 categories: Keyboard/Mouse, Video, Macro and Advanced. Hover your mouse over these categories to see the rest of the menu items:</p>  <p>Click the icon again to revert to the original Control Panel format.</p>
 <p>Macros</p>	<p>Click to bring up the Macros dialog box (see page 79 for details).</p>
 <p>Video Settings</p>	<p>Click to bring up the Video Options dialog box. Right-click to perform a quick Auto Sync (see <i>Video Settings</i>, page 88, for details).</p>
 <p>Screen Mode</p>	<p>Click to perform a video and mouse auto-sync operation. It is the same as clicking the Auto-sync button in the Video Options dialog box (see Video Settings, page 86, for details).</p>
 <p>Screen Mode</p>	<p>Toggles the display between <i>Full Screen Mode</i> and <i>Windowed Mode</i>.</p>
 <p>Snap Shot</p>	<p>Click to take a snapshot (screen capture) of the remote display. See <i>Snapshot</i>, page 104, for details on configuring the Snapshot parameters.</p>

Icon	Function
 Message Board	Click to bring up the Message Board (see <i>Message Board</i> , page 91).
 Ctrl+Alt+Del	Click to send a <i>Ctrl+Alt+Del</i> signal to the remote system.
 Set to Grayscale	Click to toggle the remote display between color and grayscale.
 Virtual Media	Click to bring up the <i>Virtual Media</i> dialog box. The icon changes when a virtual media device is started on the port. See <i>Virtual Media</i> , page 93, for specific details. Note: This icon displays in gray when the function is disabled or not available to the user.
 Zoom	Click to zoom the remote display window. Note: This feature is only available in windowed mode (Full Screen Mode is off). See <i>Zoom</i> , page 97 for details.
 On-Screen Keyboard	Click to bring up the on-screen keyboard (see <i>The On-Screen Keyboard</i> , page 98).
 Mouse Pointer	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 100).
 Mouse Sync Mode	Click to toggle Automatic or Manual mouse sync. ♦ When the selection is <i>Automatic</i> , a green ✓ appears on the icon. ♦ When the selection is <i>Manual</i> , a red X appears on the icon. See <i>Mouse DynaSync Mode</i> , page 100 for a complete explanation of this feature.
 Macro List	Click to display a drop-down Macro List of <i>User</i> macros. Access and run macros more conveniently rather than using the Macros dialog box (see the <i>Macros</i> icon in the table above, and the <i>Macros</i> section on page 79).

Icon	Function
 Open GUI	Click this icon to open a Viewer based GUI with the web browser administrative functionalities. See Admin Utility, page 103, for details.
 Customize Control Panel	Click to bring up the Control Panel Configuration dialog box. See <i>Customize Control Panel</i> , page 103, for details on configuring the Control Panel.
 Exit	Click to exit the remote view and go back to the web browser Main Page.
	<p>These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer.</p> <ul style="list-style-type: none"> ◆ When the lock state is <i>On</i>, the LED is bright green and the lock hasp is closed. ◆ When the lock state is <i>Off</i>, the LED is dull green and the lock hasp is open. <p>Click on the icon to toggle the status.</p> <p>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.</p>

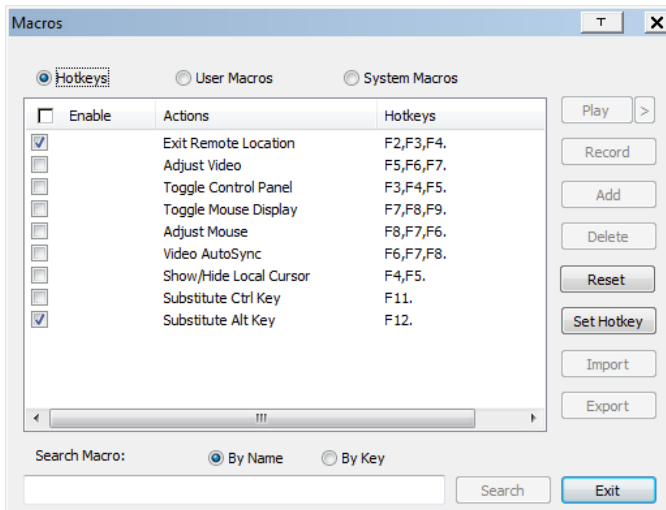


Macros

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**.

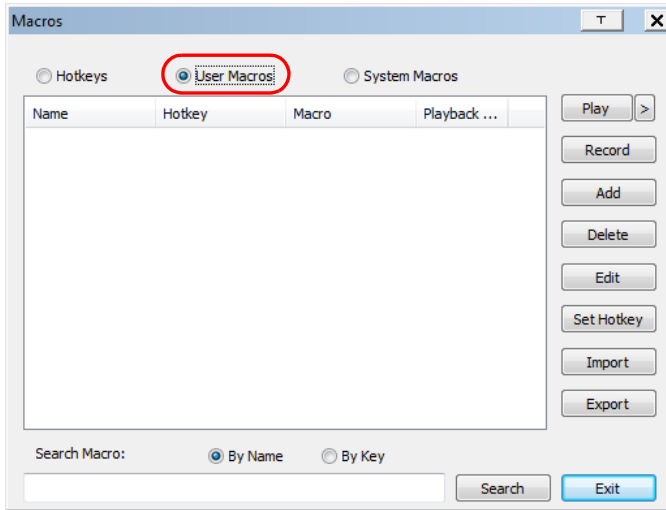
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit Remote Location	Exits the remote view and goes back to the web browser Main Page. 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	<p>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.</p> <p>Note: The Java Control Panel does not have this feature.</p>
Adjust Mouse	This synchronizes the local and remote mouse movements. The default keys are F7, F8, F9.
Video AutoSync	This combination performs an auto-sync operation. It is equivalent to clicking the <i>Video Autosync</i> icon on the Control Panel. The default keys are F6, F7, F8.
Show/Hide Local Cursor	Toggles the display of your local mouse pointer off and on. This is equivalent to selecting the <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	<p>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.</p> <p>Note: When Keyboard Pass Through is enabled, [Alt + Tab] can be sent directly to the remote system (see <i>Customize Control Panel</i>, page 103 for details).</p>
Substitute Alt key	<p>Although all other keyboard input is captured and sent to the remote system, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F11.</p> <p>Note: When Keyboard Pass Through is enabled, [Alt + Tab] can be sent directly to the remote system (see <i>Customize Control Panel</i>, page 103 for details).</p>

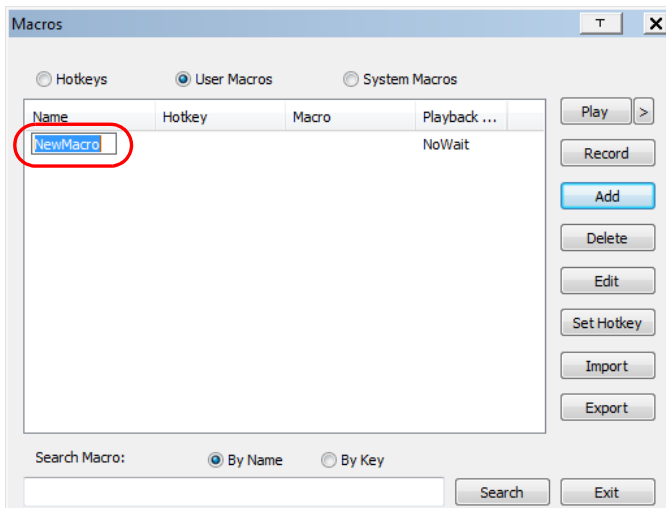
User Macros

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

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

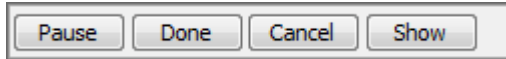


2. In the dialog box that comes up, replace “NewMacro” with a name of your choice for the macro:



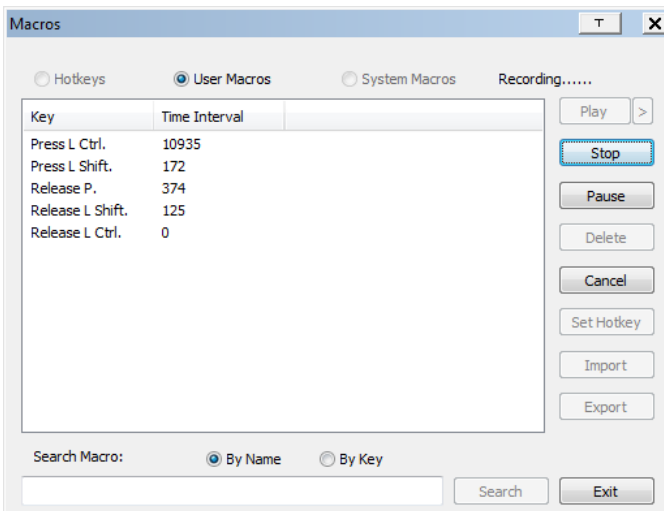
3. Click **Record**.

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



4. Press the keys for the macro.

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

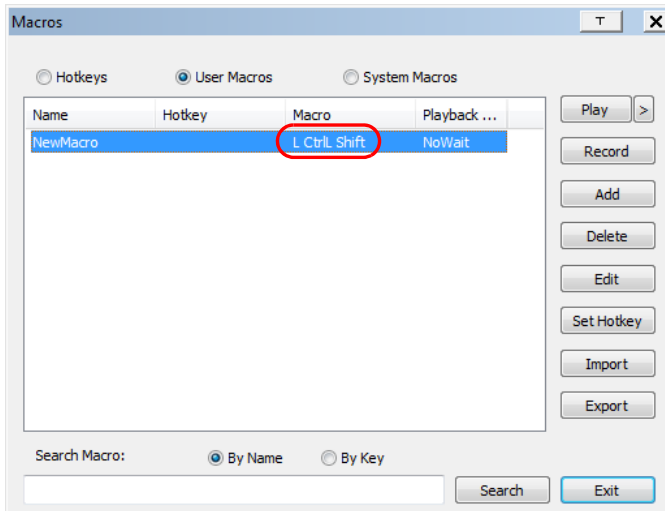


- ◆ Clicking **Cancel** cancels all keystrokes.
- ◆ When you have finished, click **Stop**. This is the equivalent of clicking *Done* in Step 5.

Note: 1. Case is not considered – typing **A** or **a** has the same effect.

2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.
 3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.
-

5. If you have not brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with the macro keys that you pressed displayed in the Macro column:

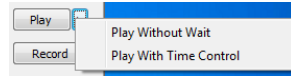


6. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.
7. Repeat the procedure for any other macros you wish to create.

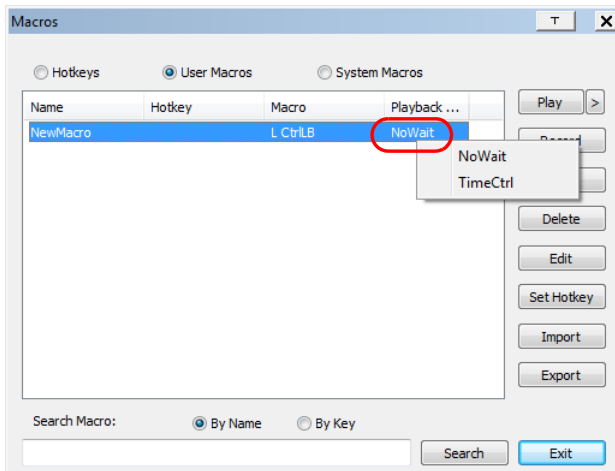
After creating your macros, you can run them in any of three ways:

1. By using the hotkey (if one was assigned).
2. By opening the Macro List on the Control Panel and clicking the one you want (see *Macro List*, page 77).
3. By opening this dialog box and clicking **Play**.

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



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



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

Note: 1. Information about the Search function is given on page 85.

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

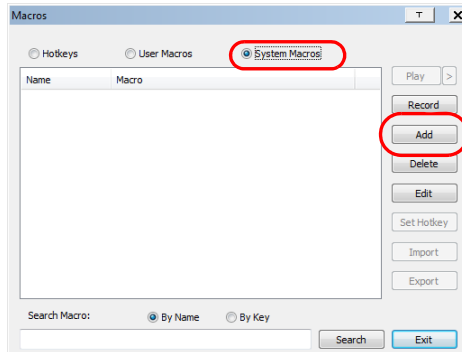
Search

Search, at the bottom of the dialog box, lets you filter the list of macros that appear in the large upper panel for you to play or edit. Click a radio button to choose whether you want to search by name or by key; key in a string for the search; then click **Search**. All instances that match your search string appear in the upper panel.

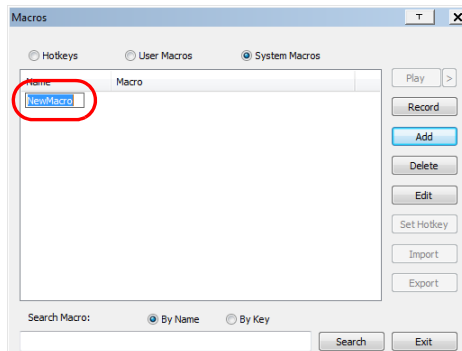
System Macros

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

1. Select *System Macros*, then click **Add**.

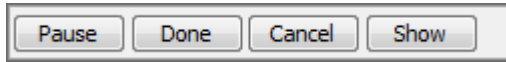


2. In the dialog box that comes up, replace the “NewMacro” text with a name of your choice for the macro:



3. Click **Record**.

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



4. Press the keys for the macro.

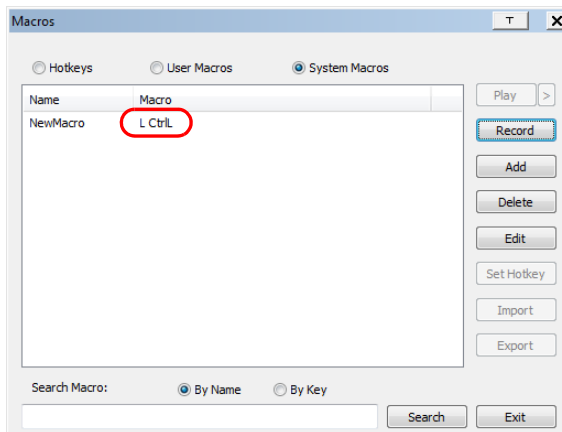
- ♦ To pause macro recording, click **Pause**. To resume, click **Record** again.
- ♦ Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 82).

Note: 1. Case is not considered – typing **A** or **a** has the same effect.

2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.

5. If you have not 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 KN1000A. System macros will only execute when the last user has logged out of the viewer (see *System Macros*, page 85 for details).

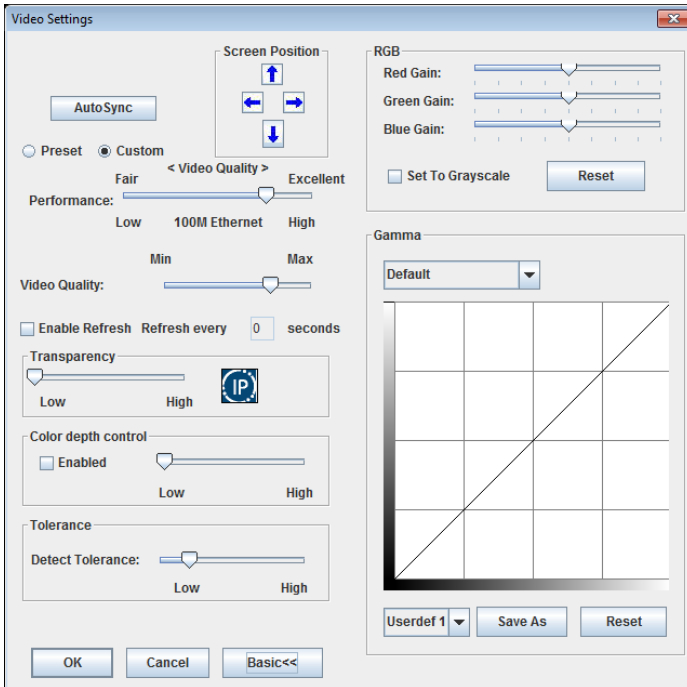
Note: 1. Information about the Search function is given on page 85.

2. Systems macros are stored on the KN1000A; therefore macro names may not exceed 64 Bytes (1 byte = 1 English alphanumeric character), and hotkey combinations may not exceed 256 Bytes (each key usually takes 3–5 bytes).
-



Video Settings

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



Descriptions of the adjustment options are given in the table below:

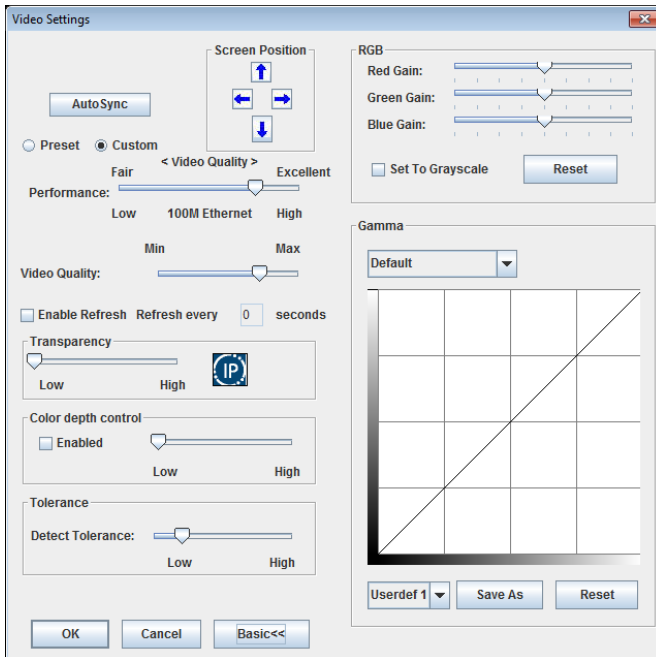
Option	Usage
Screen Position	Adjust the horizontal and vertical position of the remote computer window by clicking the Arrow buttons.
Auto Sync	<p>Click Auto Sync to have the vertical and horizontal offset values of the remote screen detected and automatically synchronized with the local screen.</p>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

Option	Usage
RGB	<p>Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When an RGB value is increased, the RGB component of the image is correspondingly increased.</p> <p>If you enable <i>Set to Grayscale</i>, the remote video display is changed to grayscale.</p>
Gamma	<p>This section allows you to adjust the video display's gamma level. This function is discussed in detail in the next section, <i>Gamma Adjustment</i>.</p>
Performance	<p>Select the type of Internet connection that exists between the Local Client computer and the KN1000A. The KN1000A 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.</p> <p>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.</p>
Video Quality	<p>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 effect response time.</p>
Enable Refresh	<p>The KN1000A 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 KN1000A 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.</p> <p>Note:</p> <ol style="list-style-type: none"> 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	<p>Drag the slider bars to adjust the transparency of the remote display.</p>
Color Depth Control	<p>This setting determines the richness of the video display by adjusting the amount of color information.</p>
Tolerance	<p>This setting also relates to video quality. It governs detecting or ignoring pixel changes. A high setting can result in a lower quality display due to less data transfer. A lower setting will result in better video quality, but setting the threshold too low may allow too much data to be transferred, negatively impacting network performance.</p>

Gamma Adjustment

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

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



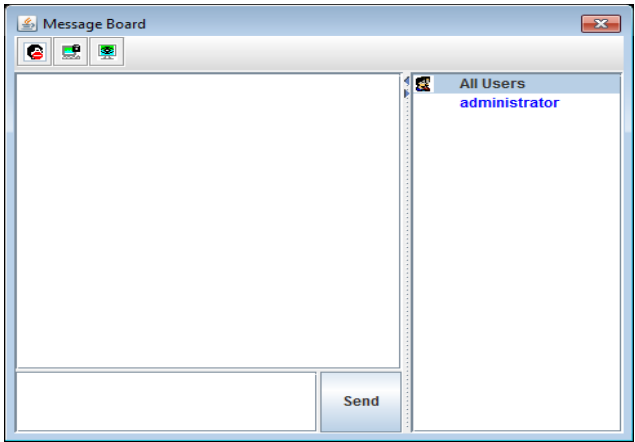
- There are ten preset and four user-defined levels to choose from. Drop down the list box and choose the most suitable one.
- Click and drag the diagonal line at as many points as you wish to achieve the display output you desire.
- Click **Save As** to save up to four user-defined configurations derived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

Note: For best results, change the gamma while viewing a remote computer.



Message Board

To alleviate the possibility of access conflicts resulting from multiple user logins, the KN1000A 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. When a port is set to <i>Occupy</i> mode (see <i>Multuser Mode</i> , page 66), 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>Occupy</i> mode (see <i>Multuser Mode</i> , page 66), you can use this button to occupy the KM. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed when the KM is occupied. The icon displays next to the user's name in the User List panel when the user has occupied the KM.
	Show/Hide User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.

Message Display Panel

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

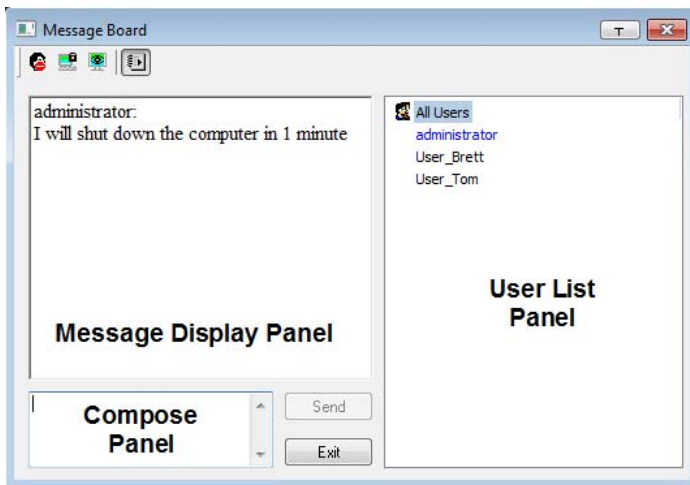
Compose Panel

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

User List Panel

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

- ♦ Your name appears in blue; other users' names appear in black.
- ♦ By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- ♦ If a user's name is selected, and you want to post a message to all users, select All Users before sending your message.
- ♦ If a user has disabled Chat, its icon displays before the user's name to indicate so.
- ♦ If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.







Virtual Media

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

Virtual Media Icons

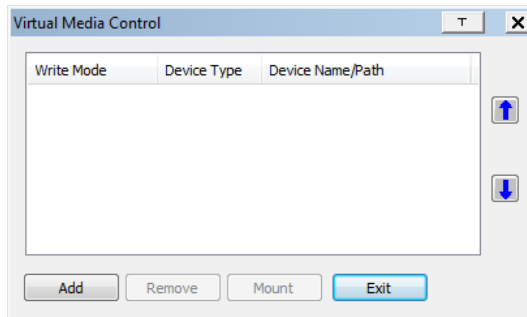
The Virtual Media icon on the WinClient Control Panel changes, to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

Icon	Function
	The icon displays in blue to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.
	The icon displays in blue with a <i>/</i> to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.

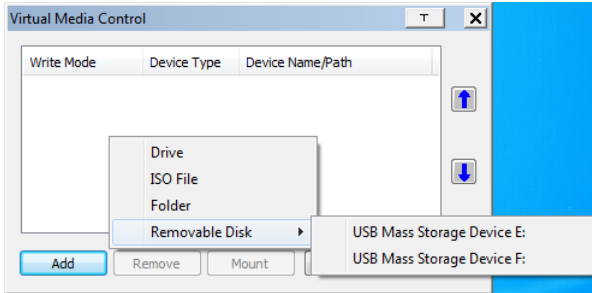
Virtual Media Redirection

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**; then select the media source.

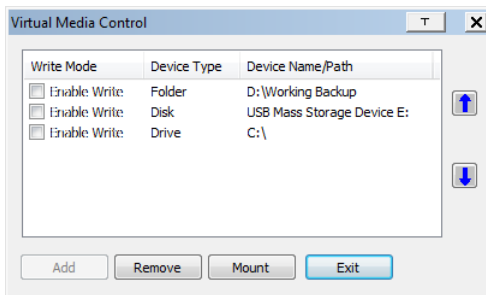


Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 170 for details about mounting these media types.

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

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

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

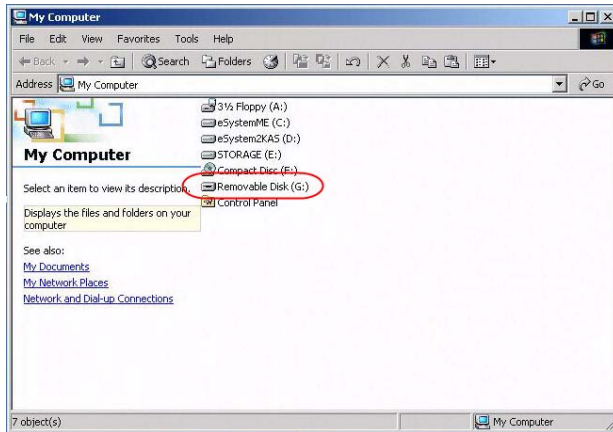


Note:

- ♦ 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.

- ♦ See *Virtual Media Support*, page 170, for a list of supported virtual media types.

5. To remove an entry from the list, select 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 file system.



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

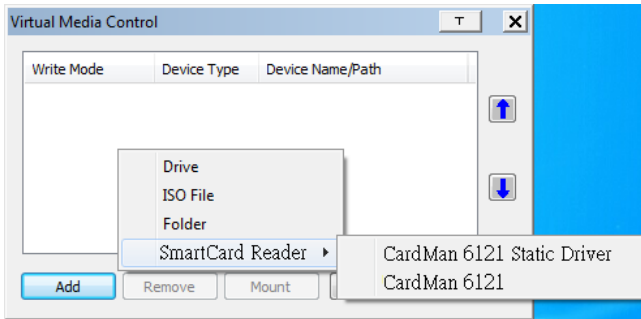
Files that you save to the redirected media, will actually be saved on your local system. Files that you drag from the redirected media will actually come from your local system.

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

Smart Card Reader

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

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



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

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



Zoom

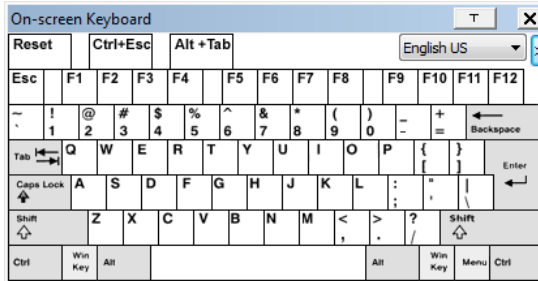
The Zoom icon controls the zoom factor for the remote view window. Settings are as follows:

Setting	Description
100%	Sizes and displays the remote view window at 100%.
75%	Sizes and displays the remote view window at 75%.
50%	Sizes and displays the remote view window at 50%.
25%	Sizes and displays the remote view window at 25%.
1:1	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents do not resize – they remain at the size they were. To see any objects that are outside of the viewing area, move the mouse to the window edge, to have the screen scroll.



The On-Screen Keyboard

The KN1000A 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:

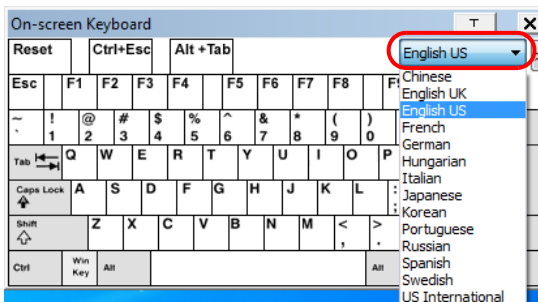


One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems aren't the same, you do not have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer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

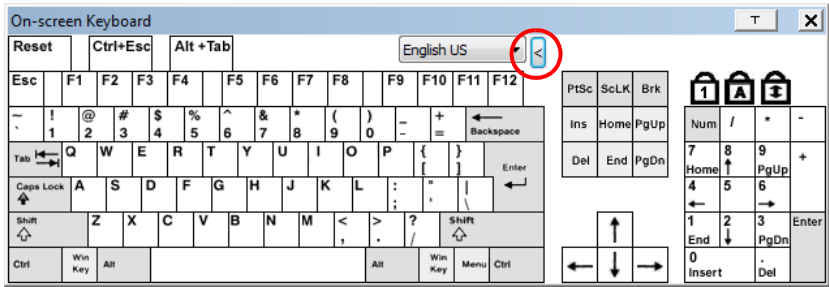
To change languages, do the following:

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 KN1000A offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:



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



Mouse DynaSync Mode

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

Automatic Mouse Synchronization (DynaSync)

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

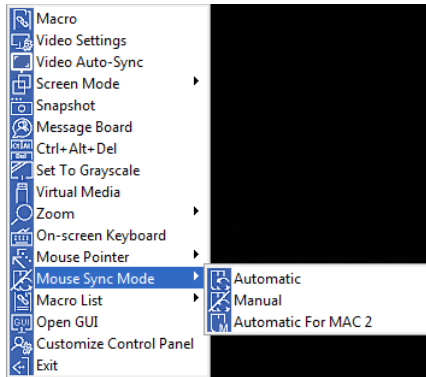
The icon on the toolbar indicates the synchronization mode status as follows:

Icon	Function
	This icon indicates that Mouse DynaSync is available and is enabled . This is the default setting when Mouse DynaSync is available.
	The / over this icon indicates that Mouse DynaSync is available but is not enabled .

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

Mac Considerations

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



Manual Mouse Synchronization

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

1. Perform a video and mouse auto sync by clicking the *Video Settings* icon on the Control Panel (see page 88).
2. Perform an *Auto Sync* with the Video Adjustment function (see *Video Settings*, page 88, for details).
3. Invoke the *Adjust Mouse* function with the *Adjust Mouse* hotkeys (see *Adjust Mouse*, page 80, for details).
4. Move the pointer into all 4 corners of the screen (in any order).
5. Drag the Control Panel to a different position on the screen.
6. Set the mouse speed and acceleration for each problematic computer attached to the switch. See *Additional Mouse Synchronization Procedures*, page 168, for instructions.



Open GUI

Clicking the *Open GUI* icon brings up a window that allows you to configure the KN1000A via Viewer based GUI with the web browser administrative functionalities:

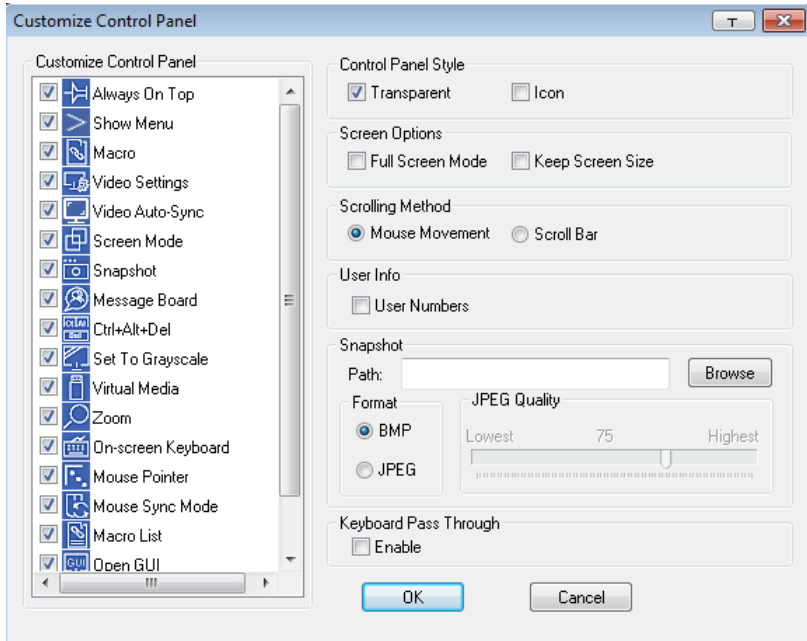


The sidebar menu items available on this page are based upon the user's permissions. For information on how to use these functions, see *Configuration*, page 23 for details.



Customize Control Panel

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



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

Item	Description
Customize Control Panel	Allows you to select which icons display in the Control Panel
Control Panel Style	<ul style="list-style-type: none"> Enabling <i>Transparent</i> makes the Control Panel semi-transparent, so that you can see through it to the display underneath. Enabling <i>Icon</i> causes the Control Panel to disappear and display as an icon (shown left) on the screen until you mouse over it. When you mouse over the icon, the full panel comes up. This function only works when the Control Panel is dragged out of its default position (top center or bottom center of the screen).



Item	Description
Screen Options	<ul style="list-style-type: none"> ◆ If <i>Full Screen Mode</i> is enabled, the remote display fills the entire screen. ◆ If <i>Full Screen Mode</i> is not enabled, the remote display appears as a window on the local desktop. If the remote screen is larger than what is able to fit in the window, scrollbars will appear. ◆ If <i>Keep Screen Size</i> is enabled, the remote screen is not resized. <ul style="list-style-type: none"> ◆ If the remote resolution is smaller than that of the local monitor, its display appears like a window centered on the screen. ◆ If the remote resolution is larger than that of the local monitor, its display is scaled to the local size. ◆ If <i>Keep Screen Size</i> is not enabled, the remote screen is resized to fit the local monitor's resolution.
Scrolling Method	<ul style="list-style-type: none"> ◆ If <i>Mouse Movement</i> is selected when the remote view window is larger than can fit the local desktop, moving the mouse to the edges of the screen will automatically scroll the window up or down. ◆ If <i>Scroll Bar</i> is selected a scroll bar will appear when the remote view window is larger than can fit the local desktop, allowing you to adjust the viewing position with the scroll bar.
User Info	<p>If <i>Show User Numbers</i> is enabled, the total number of users logged into the KN1000A displays in the text row of the Control Panel (See the Control Panel diagram on page 74 for an example.)</p>
Snapshot	<p>These settings let the user configure the KN1000A's screen capture parameters (see the <i>Snapshot</i> description under <i>Control Panel Functions</i>, page 76):</p> <ul style="list-style-type: none"> ◆ 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 do not specify a directory here, the snapshot is saved to your desktop. ◆ Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file. ◆ If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.
Keyboard Pass Through	<p>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.</p>

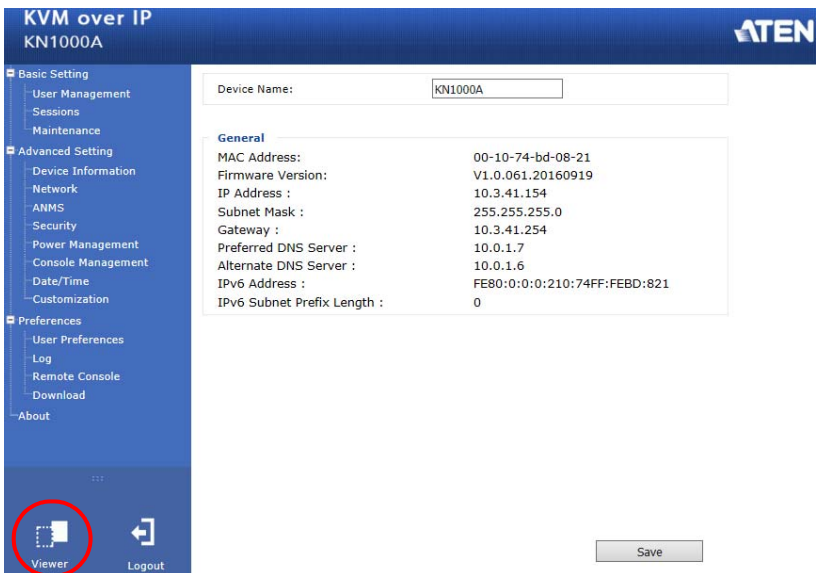
Chapter 6

The JavaClient Viewer

Introduction

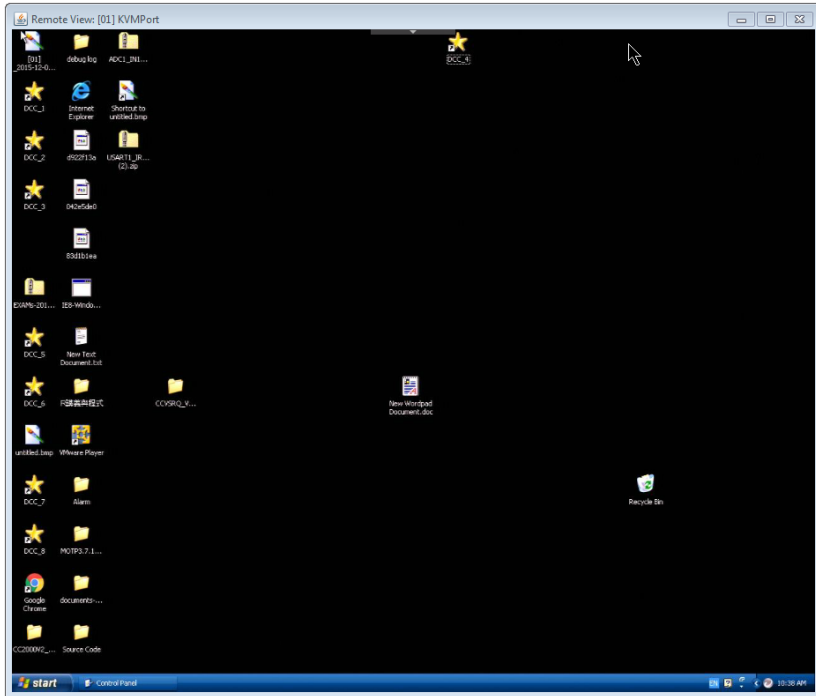
The JavaClient Viewer makes the KN1000A accessible to all platforms that have the Java Runtime Environment (JRE) installed. (See *System Requirements*, page 7, for the required JRE version.) The JRE is available for free download from the Java web site (<http://java.com>).

To run the JavaClient Viewer, after you log in (see *Logging In*, page 21), Click the *Viewer* link on the lower *Sidebar* panel, shown below.



Note: For the JavaClient Viewer to launch, it must be set as the default viewer. See *User Preferences*, page 68, for details.

A second or two after you click the *Viewer* link, the remote server's display appears as a window on your desktop:



Navigation

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

- ♦ You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.
- ♦ You can switch between your local and remote programs with [Alt + Tab].

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

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

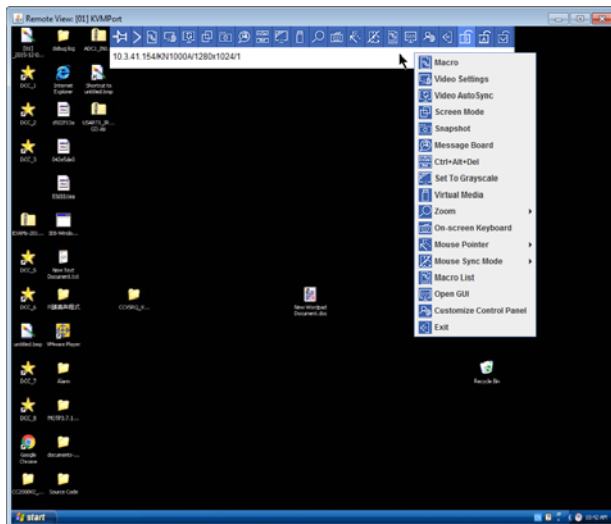
The JavaClient Control Panel

The JavaClient control panel is hidden at the top center of the screen. It becomes visible when you move the mouse pointer into that area:





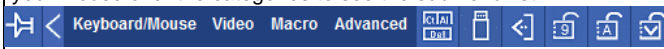









- Note:**
1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Control Panel Configuration*, page 118, for details.
 2. To place the control panel anywhere on the screen, move the mouse pointer over the text bar area and drag the panel to the new position.










- ♦ By default, the text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, information will be displayed that describes the icon's function.
- ♦ If the *Show User Numbers* function has been enabled under *Control Panel Configuration* (see *User Info*, page 104), the total number of users currently logged into the KN1000A displays next to the text row on the right.
- ♦ Right clicking in the text row area brings up a menu that allows you to select and use the Control Panel options. All Control Panel functions are discussed in the sections that follow.



Control Panel Functions

The Control Panel functions are described in the table below:

Icon	Function
	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
	<p>When you click this icon, the Control Panel collapses into 4 categories: Keyboard/Mouse, Video, Macro and Advanced. Hover your mouse over the categories to see the submenu list.</p>  <p>Click the icon again to revert to the original Control Panel format.</p>
	Click to bring up the Macros dialog box (see <i>Macros</i> , page 110 for details).
	Click to bring up the <i>Video settings</i> dialog box. Right-click to perform a quick Auto Sync (see <i>Video Settings</i> , page 112, for details).
	Click to perform a video and mouse autosync operation. It is the same as clicking the Auto-sync button in the <i>Video Options</i> dialog box (see <i>Video Settings</i> , page 112).
	Toggles the display between <i>Full Screen Mode</i> and <i>Windowed Mode</i> .
	Click to take a snapshot (screen capture) of the remote display. See <i>Snapshot</i> , page 104, for details on configuring the Snapshot parameters.
	Click to bring up the <i>Message board</i> (see page 113).
	Click to send a <i>Ctrl+Alt+Del</i> signal to the remote system.
	Click to toggle the remote display between grayscale and color.
	Click to bring up the <i>Virtual Media</i> dialog box. The <i>/</i> over the icon will indicate that a media device has been mounted. The icon changes back when the virtual media icon is clicked again and the device is unmounted. See <i>Virtual Media</i> , page 115, for specific details.

Icon	Function
	Click to zoom the remote display window. Note: This feature is only available in windowed mode (Full Screen Mode is off). See <i>Zoom</i> , page 115, for details.
	Click to bring up the on-screen keyboard (see <i>The On-Screen Keyboard</i> , page 117).
	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 117).
	Click to toggle Automatic or Manual mouse sync. <ul style="list-style-type: none"> When the selection is <i>Automatic</i>, the icon to the right appears. When the selection is <i>Manual</i>, a <i>/</i> appears over the icon. (See <i>Mouse DynaSync Mode</i> , page 100 for a complete explanation of this feature.)
	Click to display a drop-down list of <i>User</i> macros. Access and run macros more conveniently rather than using the Macros dialog box (see the <i>Macros</i> icon in the table above, and the <i>Macros</i> section on page 110).
	Click this icon to open a Viewer based GUI with the web browsers administrative functionalities.
	Click to bring up the Control Panel Configuration dialog box. See <i>Control Panel Configuration</i> , page 118, for details on configuring the Control Panel.
	Click to exit the remote view.
	<p>These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer.</p> <ul style="list-style-type: none"> When the lock state is <i>On</i>, the LED is bright green and the lock hasp is closed. When the lock state is <i>Off</i>, the LED is dull green and the lock hasp is open. <p>Click on the icon to toggle the status.</p> <p>Note: When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.</p>

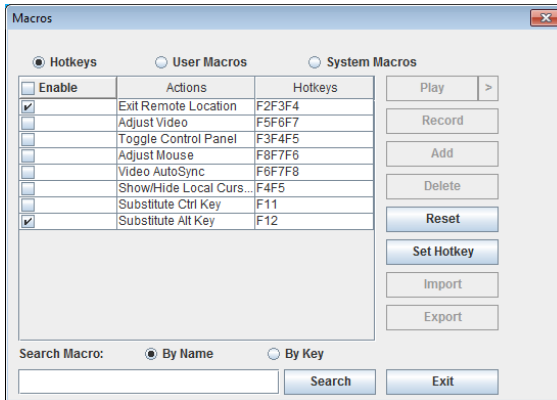


Macros

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

Hotkeys

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



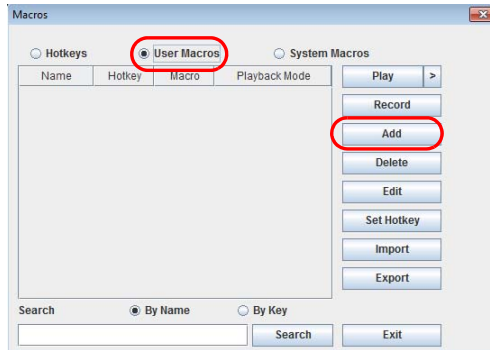
Hotkey operation is the same under the JavaClient as it is under the WinClient. See *Hotkeys*, page 79, for details.

Note: *Toggle Mouse Display* is not available in the JavaViewer version.

User Macros

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

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

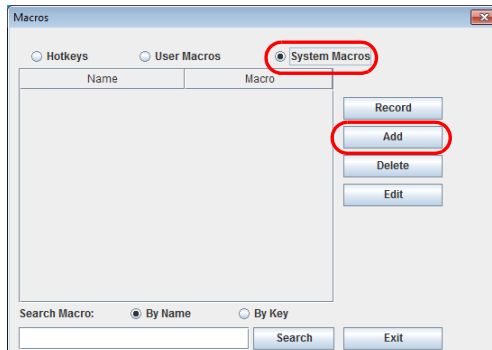


User Macro operation is the same under the JavaClient as it is under the WinClient. See *User Macros*, page 81, for details.

System Macros

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

1. Select *System Macros*, then click **Add**.



System Macro operation is the same under the JavaClient as it is under the WinClient. See *System Macros*, page 85, for details.

Search

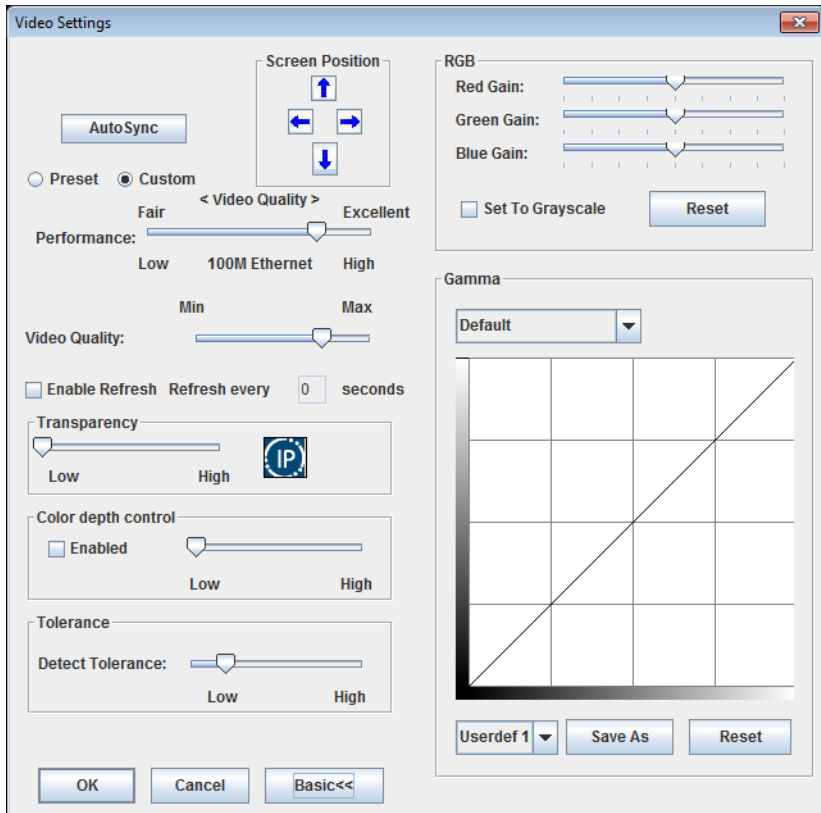
Search allows you to find previously created macros and have them listed in the large upper panel for you to play or edit.

The Search operation is the same under the JavaClient as it is under the WinClient. See *Search*, page 85, for details.



Video Settings

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

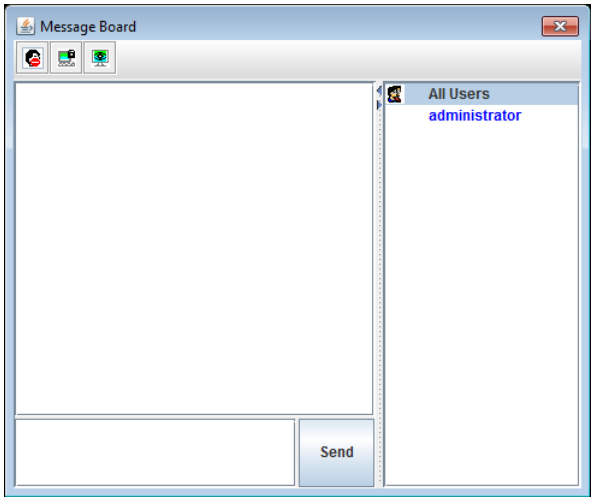


Video Settings operation is the same under the JavaClient as it is under the WinClient. See *Video Settings*, page 88, for details.



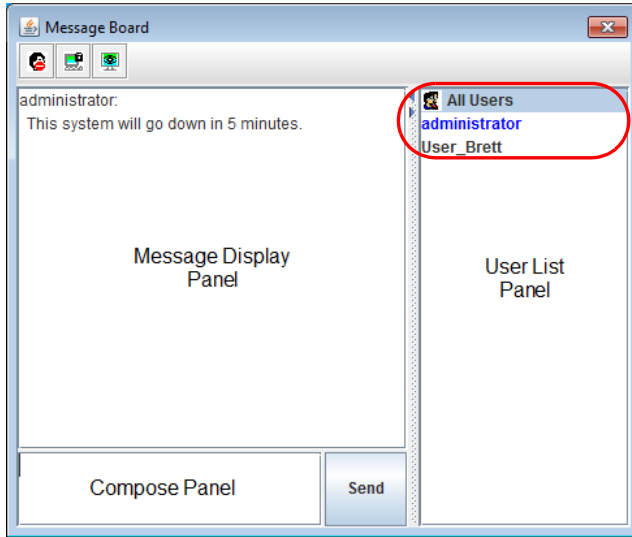
Message Board

The KN1000A supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature, similar to an Internet chat program, allows users to communicate with each other:



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

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



- ◆ The names of all the logged in users appear in the *User List* panel.
 - ◆ Select the users that you want to post to before sending your message. Users that aren't selected will not see the message.
 - ◆ To Hide/Unhide the User List panel, click on the arrows in the panel separator.
 - ◆ If a user has disabled Chat, the *Disabled Chat* icon displays before the user's name to indicate so.
 - ◆ If a user has occupied the KVM or the KM, the corresponding icon displays before the user's name to indicate so.
- ◆ Key in the messages that you want to post to the board in the *Compose* panel. Click **Send**, to post the message to the board.
 - ◆ Messages that users post to the board – as well as system messages – display in the *Message Display* panel. If you disable Chat, however, messages that get posted to the board do not appear.
 - ◆ If another user sends a message to the message board and your message board is not open, a window showing the message pops up on your screen.

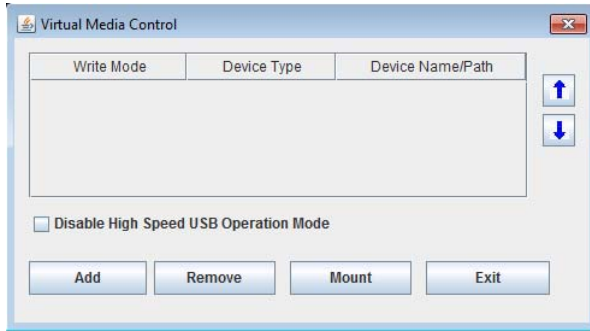


Virtual Media

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

To implement this redirection feature, do the following:

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



Virtual Media operation is the same under the JavaClient as it is under the WinClient. See *Virtual Media*, page 93, for details.

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



Zoom

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

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

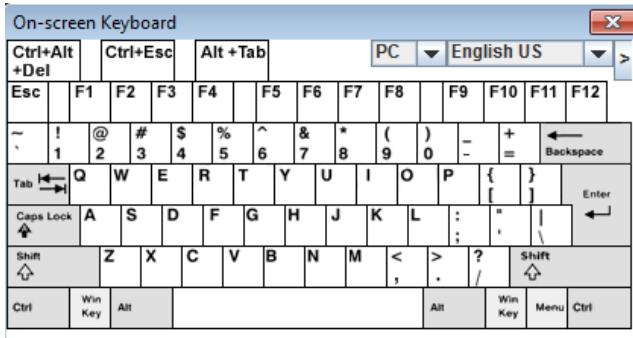
Setting	Description
1:1	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents do not resize – they remain at the size they were. To see any objects that are outside of the viewing area, move the mouse to the window edge, to have the screen scroll.



The On-Screen Keyboard

The KN1000A supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language.

Click this icon to pop up the on-screen keyboard:



On-Screen Keyboard operation is the same under the JavaClient as it is under the WinClient. See *The On-Screen Keyboard*, page 98, for details.



Mouse Pointer Type

The KN1000A offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:



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



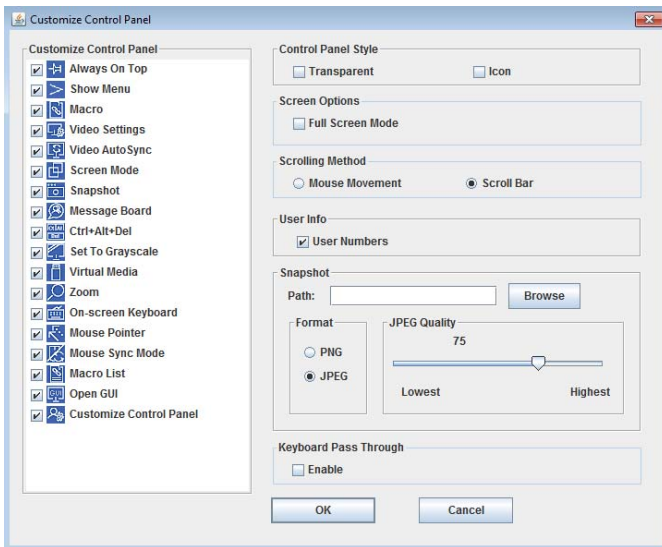
Mouse DynaSync Mode

Clicking this icon selects whether synchronization of the local and remote mouse pointers is accomplished either automatically or manually. DynaSync operation is the same under the JavaClient as it is under the WinClient. See *Mouse DynaSync Mode*, page 100, for details.



Control Panel Configuration

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



Control Panel Configuration is almost the same under the JavaClient as it is under the WinClient. See *Customize Control Panel*, page 103, for details.

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

Chapter 7

Local Console

Introduction

The KN1000A can be accessed directly from a local console's keyboard/mouse/monitor or via a laptop application (AP) program at the local site. With the laptop, you can then access and edit the KN1000A application.

Laptop USB Console

Use the instructions below to use the mini USB port for Laptop USB Console (LUC) operations.

Note: The LUC function only works for Windows systems.

The laptop application (AP) program for operating the LUC is built into the KN1000A's firmware and does not require a download. To access the switch, do the following:

1. Use the Mini USB to Type A USB cable included in the package to connect your laptop to the KN1000A's mini USB port, located on the unit's front panel (see *Installation*, page 18).
2. The KN1000A appears as a virtual drive in the laptop's file system. Locate the Laptop AP on the virtual CD ROM and double-click the icon. The login screen appears.



3. At the login screen, key in your valid Username and Password, then click **Login**. Once you have logged in successfully, the **Remote View** button becomes active.

4. Click **Remote View** to bring up the Laptop Console Main Page.

Laptop USB Console Main Page

After connecting a laptop to the KN1000A's Laptop port, logging in, and opening the AP, the Laptop Console main page appears.



The Laptop Console Main Page is similar to the Web Browser, WinClient and Java Client Main Pages. See *AP Operation*, page 129, for further details, and reference the AP GUI sections throughout the rest of the manual regarding operations.

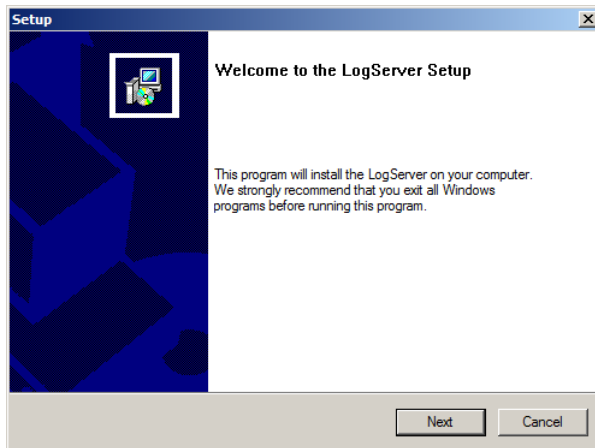
Chapter 8

The Log Server

The Log Server is a Windows-based administrative utility that records all the events that take place on selected KN1000A units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

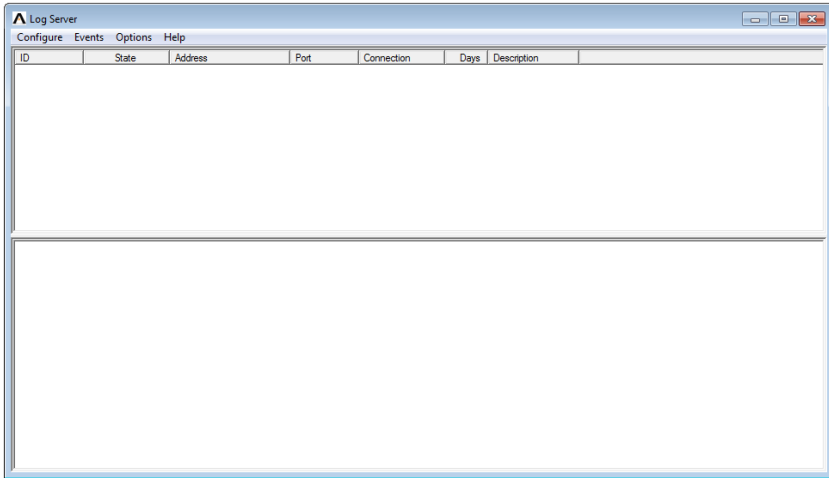
1. On the KN1000A product page of our website, download the LogServer software to your computer.
2. Unzip the installation files and click the *kn1000a_logserver_vxx.exe* file to execute the Log Server setup and start the installation.



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

Starting Up

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



Note: 1. The MAC address of the Log Server computer must be specified in the ANMS settings – see *Log Server*, page 38 for details.

2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server program does not run.*, page 167 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 KN1000A units in the middle (see *The Log Server Main Screen*, page 127, 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.

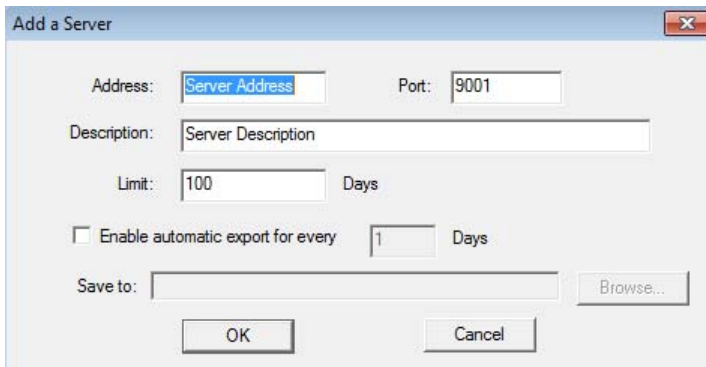
Note: If the Menu Bar appears to be disabled, click in the KN1000A List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new KN1000A units to the KN1000A List, edit the information for units already on the list, or delete KN1000A units from the list.

- ♦ To add a KN1000A to the KN1000A List, click **Add**.
- ♦ To edit or delete a listed KN1000A, first select the one you want in the KN1000A 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 image shows a Windows-style dialog box titled "Add a Server". It contains several input fields and controls:

- Address:** A text box containing "Server Address".
- Port:** A text box containing "9001".
- Description:** A larger text box containing "Server Description".
- Limit:** A text box containing "100", followed by the word "Days".
- Enable automatic export:** A checkbox that is currently unchecked, followed by the text "Enable automatic export for every".
- Frequency:** A text box containing "1", followed by the word "Days".
- Save to:** A text box that is empty, followed by a "Browse..." button.
- Buttons:** "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 KN1000A or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the KN1000A in the <i>ANMS</i> settings (see <i>ANMS</i> , page 36).
Port	Key in the port number that was specified for the Log Server's <i>Service Port</i> in the <i>ANMS</i> settings (see <i>Log Server</i> , page 38).
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	Check this box to automatically save an exported log file to your computer. Input how often you want the log file to be exported in the Days box.
Save to	Click Browse to select a location to save exported log files when the automatic feature described above is enabled.

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

Server List:

Priority List:

Least
Less
Most

Start date: 11/ 2/2016 Start time: 4:33:09 PM End date: 11/ 3/2016 End time: 4:33:09 PM Pattern:

Result:

Search Print Export Exit

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

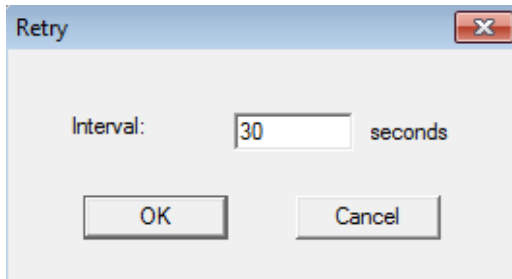
Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected KN1000A.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected KN1000A <i>excluding</i> the events that resulted from the last search.
Server List	KN1000A 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 124).

Options

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



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

Help

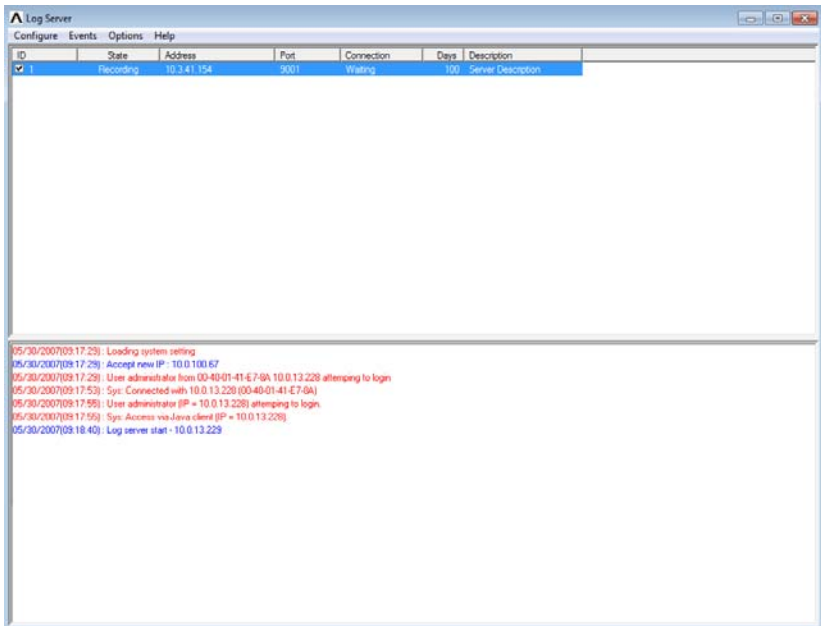
From the Help Menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

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

- The upper (List) panel lists the KN1000A units that have been selected for the Log Server to track (see *Configure*, page 123).
- The lower (Event) panel displays the log events for the currently selected KN1000A (the highlighted one - if there are more than one). To select a KN1000A unit in the list, simply click on it.



The List Panel

The List panel contains six fields:

Field	Explanation
Recording	Determines whether the Log Server records log events for this KN1000A or not. If the Recording check box is checked, the field displays <i>Recording</i> , and log events are recorded. If the Recording check box is not checked, the field displays <i>Paused</i> , and log events are not recorded. Note: Even though a KN1000A is not the currently selected one, if its Recording check box is checked, the Log Server will still record its log events.
Address	This is the IP Address or DNS name that was given to the KN1000A when it was added to the Log Server (see <i>Configure</i> , page 123).
Port	This is the port number that was assigned to the KN1000A when it was added to the Log Server (see <i>Configure</i> , page 123).
Connection	If the Log Server is connected to the KN1000A, 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 38) and specified in the <i>Configure</i> dialog box (see <i>Configure</i> , page 123).
Days	This field displays the number of days that the KN1000A's log events are to be kept in the Log Server's database before expiration (see <i>Configure</i> , page 123).
Description	This field displays the descriptive information given for the KN1000A when it was added to the Log Server (see <i>Configure</i> , page 123).

The Tick Panel

The lower panel displays tick information for the currently selected KN1000A. Note that if the installation contains more than one switch, even though a switch is not currently selected, if its *Recording* check box is checked, the Log Server records its tick information and keeps it in its database.

Chapter 9

AP Operation

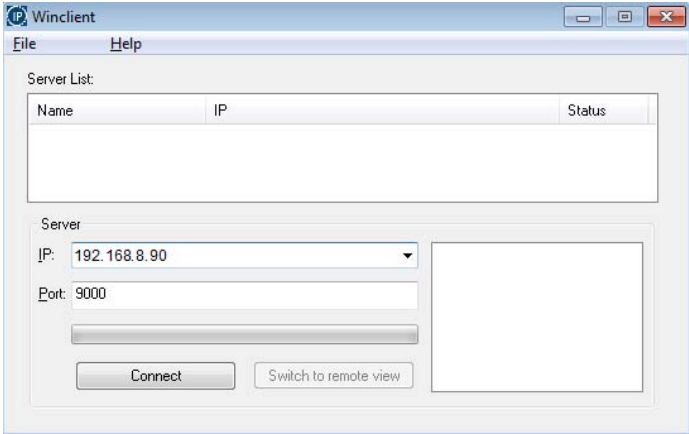
Introduction

In addition to the browser-based client viewers, the KN1000A also provides stand-alone Windows and Java applications that can be used without a browser. This allows users to access the computer connected to the KN1000A without having to log in to its Web GUI. For Java Client AP instructions, see *The Java Client AP*, page 133, for details. The Windows Client AP and Java Client AP can be downloaded from the Download page of the KN1000A Web GUI by clicking the *Download Windows Client AP* and *Download Java Client AP* button (see *Download*, page 71), as shown below.



The WinClient AP

Download the **WinClient.exe** file from the Download page in the KN1000A Web GUI (see *Download*, page 71). When you run the *WinClient.exe* file, the Connection screen appears:

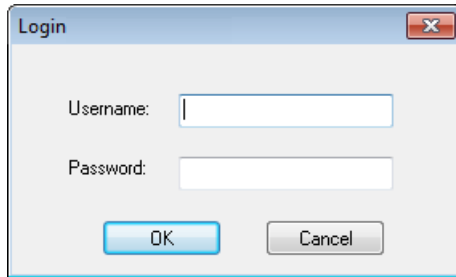


A description of the Connection Screen is given in the following table:

Item	Description
Server List	Each time the WinClient.exe program is run, it searches the local LAN segment for KN1000A units, and lists whichever ones it finds in this box. If you want to connect to one of these units, select it, then click Connect . When you have finished with your session, Click Disconnect to end the connection.
Server	This area is used when you want to connect to a KN1000A at a remote location. If the IP address that appears is not the one you want, or if there is no entry at all, key in the IP address you want. Next, key in the Port number in the <i>Port</i> field. If you do not 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. When you have finished with your session, Click Disconnect to end the connection.
Connect	Starts the connection to the KN1000A.
Disconnect	These buttons become active once you log into the KN1000A. See <i>Switch to remote view</i> , page 132, for details for details.
Switch to remote view	

Logging In

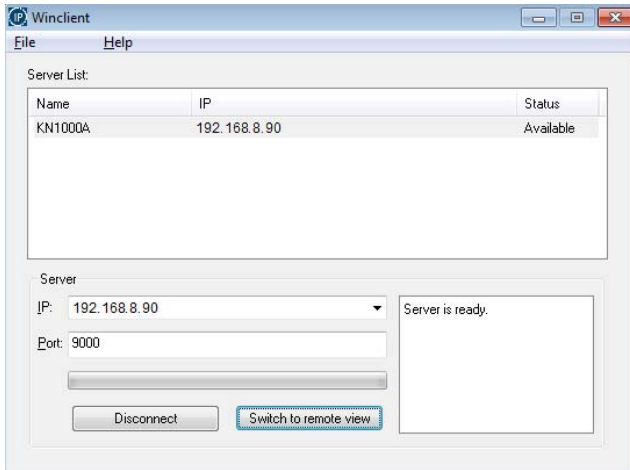
Once the KN1000A connects to the unit you specified, a login window appears:



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

Note: The default Username is *administrator*; the default Password is *password*. For security, we strongly recommend that you change these to something unique (see *User Management*, page 24, for details).

After you have successfully logged in new buttons are available:



At this time there are two active buttons, as described below:

Button	Action
Disconnect	Breaks the connection to the KN1000A.

Button	Action
Switch to remote view	In some cases, administrator's do not wish to have users connect to the KN1000A with a browser. <i>Switch to remote view</i> solves this problem. It opens a window on the user's desktop containing the remote server's display that is the same as the one that appears with the browser-based Windows client. Refer to Chapter 5, <i>The WinClient Viewer</i> , for operation details.

The File Menu

The File Menu allows the operator to Create, Save, and Open user created Work files. A Work File consists of all the information specified in a Client session. This includes the Server List and Server IP list items, as well as the Hotkey settings.

Whenever a user runs the Client program, it opens with the values contained in the current work file. The current work file consists of the values that were in effect the last time the program was closed.

The File menu consists of the following items:

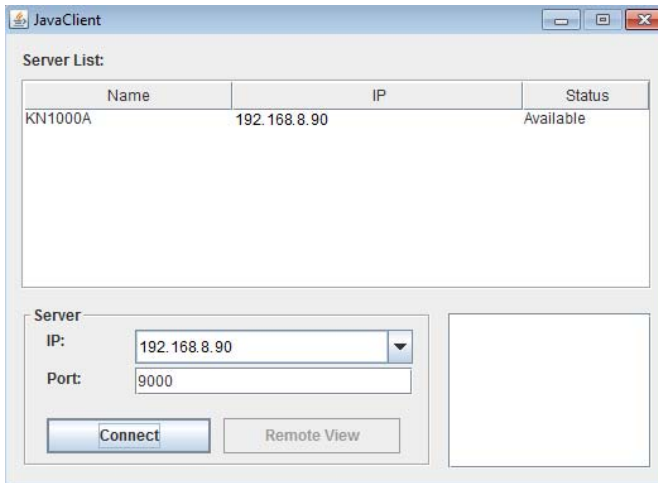
Button	Action
New	Allows the user to create a named work file so its values will not be lost, and it will be available for future recall.
Open	Allows the user to open a previously saved work file and use the values contained in it.
Save	Allows the user to save the values presently in effect as the current work file.
Exit	Exits the WinClient AP.
Help	About opens a window that displays the WinClient's current version and copyright information.

The Java Client AP

The Java Client AP is provided to make the KN1000A accessible to all platforms. Systems that have JRE 6 Update 3 or higher installed can connect. If you do not already have Java, it is available for free download from Sun's Java web site (<http://java.sun.com>).

Starting Up

The Java Client AP can be downloaded from the Download page of the KN1000A Web GUI by clicking the *Download Java Client AP* button (see *Download*, page 71). After downloading the Java Client AP use the instructions below to access the computer. When you run the Java Client AP the Connection screen appears:



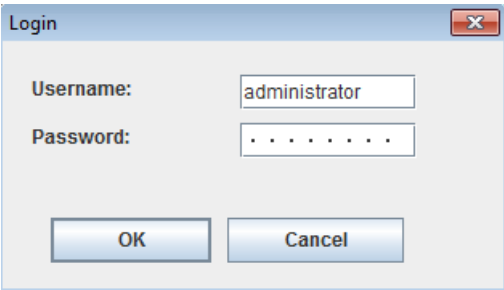
A description of the Connection Screen is given in the following table:

Item	Description
Server List	Each time the Javaclient.jar program is run, it searches the local LAN segment for KN1000A units, and lists whichever ones it finds in this box. If you want to connect to one of these units, select it, then click Connect . When you have finished with your session, Click Disconnect to end the connection.

Server	<p>This area is used when you want to connect to a KN1000A at a remote location. If the IP address that appears is not the one you want, or if there is no entry at all, key in the IP address you want.</p> <p>Next, key in the Port number in the <i>Port</i> field. If you do not know the Port number, contact the Administrator.</p> <p>When the IP address and Port number for the unit you wish to connect to have been specified, click Connect to start the connection. When you have finished with your session, Click Disconnect to end the connection.</p>
Connect	Starts the connection to the KN1000A.
Disconnect	These buttons become active once you log into the KN1000A. See <i>Remote View</i> , page 136, for details for details.
Remote view	

Logging In

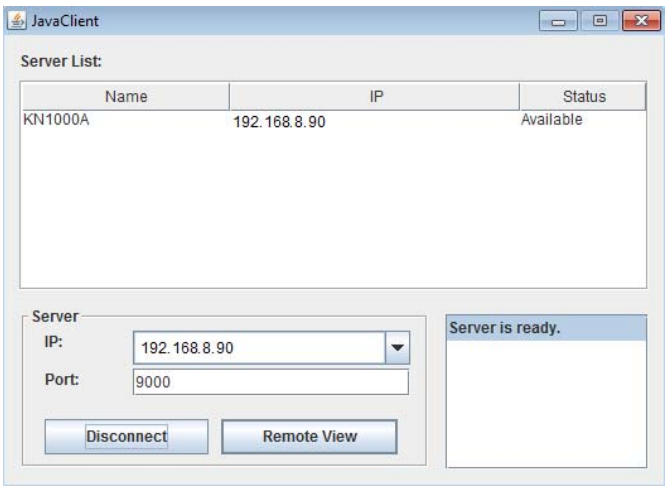
Once the KN1000A connects to the unit you specified, a login window appears:



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

Note: The default Username is *administrator*; the default Password is *password*. For security, we strongly recommend that you change these to something unique (see *User Management*, page 24, for details).

After you have successfully logged in new two new buttons are available:



Button	Action
Disconnect	Breaks the connection to the KN1000A.

Button	Action
Remote View	In some cases, administrator's do not wish to have users connect to the KN1000A with a browser - <i>Remote View</i> solves this problem. It opens a window on the user's desktop containing the remote server's display that is the same as the one that appears with the browser-based Java client. Refer to Chapter 6, <i>The JavaClient Viewer</i> , for operation details.

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.
- ♦ Avoid circuit overloads. Before connecting equipment to a circuit, know the power supply's limit and never exceed it. Always review the electrical specifications of a circuit to ensure that you are not creating a dangerous condition or that one does not already exist. Circuit overloads can cause a fire and destroy equipment.
- ♦ The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- ♦ To prevent damage to your installation it is important that all devices are properly grounded.
- ♦ The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the

purpose of the grounding-type plug. Always follow your local/national wiring codes.

- ♦ Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- ♦ If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- ♦ To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or un-interruptible power supply (UPS).
- ♦ Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- ♦ When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
 - ♦ Install the power supply before connecting the power cable to the power supply.
 - ♦ Unplug the power cable before removing the power supply.
 - ♦ If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- ♦ Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- ♦ Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- ♦ If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
 - ♦ The power cord or plug has become damaged or frayed.
 - ♦ Liquid has been spilled into the device.
 - ♦ The device has been exposed to rain or water.
 - ♦ The device has been dropped, or the cabinet has been damaged.
 - ♦ The device exhibits a distinct change in performance, indicating a need for service.
 - ♦ The device does not operate normally when the operating instructions are followed.
- ♦ Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.

- ♦ The socket-outlet shall be installed near the equipment and shall be easily accessible.
- ♦ Inlet power cord selection: Detachable, maximum 2.0 m long, 18 AWG, flexible cord (125V, 10A, 3C, NEMA 5-15P). Or, 0.75mm², 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.

Consignes de sécurité

Général

- ♦ Ce produit est destiné exclusivement à une utilisation à l'intérieur.
- ♦ Veuillez lire la totalité de ces instructions. Conservez-les afin de pouvoir vous y référer ultérieurement.
- ♦ Respectez l'ensemble des avertissements et instructions inscrits sur l'appareil.
- ♦ Ne placez jamais l'unité sur une surface instable (chariot, pied, table, etc.). Si l'unité venait à tomber, elle serait gravement endommagée.
- ♦ N'utilisez pas l'unité à proximité de l'eau.
- ♦ Ne placez pas l'unité à proximité de ou sur des radiateurs ou bouches de chaleur.
- ♦ Le boîtier de l'unité est doté de fentes et d'ouvertures destinées à assurer une ventilation adéquate. Pour garantir un fonctionnement fiable et protéger l'unité contre les surchauffes, ces ouvertures ne doivent jamais être bloquées ou couvertes.
- ♦ L'unité ne doit jamais être placée sur une surface molle (lit, canapé, tapis, etc.) car ses ouvertures de ventilation se trouveraient bloquées. De même, l'unité ne doit pas être placée dans un meuble fermé à moins qu'une ventilation adaptée ne soit assurée.
- ♦ Ne renversez jamais de liquides de quelque sorte que ce soit sur l'unité.
- ♦ Débranchez l'unité de la prise murale avant de la nettoyer. N'utilisez pas de produits de nettoyage liquide ou sous forme d'aérosol. Utilisez un chiffon humide pour le nettoyage de l'unité.
- ♦ Evitez toute surcharge du circuit. Avant de connecter l'équipement à un circuit, vérifiez la limite de l'alimentation et ne la dépassez pas. Contrôlez toujours les caractéristiques électriques d'un circuit pour vous assurer de ne pas créer de situation dangereuse ou qu'il n'y en a pas déjà. Les surcharges du circuit peuvent provoquer un incendie et détruire l'équipement.
- ♦ L'appareil doit être alimenté par le type de source indiqué sur l'étiquette. Si vous n'êtes pas sûr du type d'alimentation disponible, consultez votre revendeur ou le fournisseur local d'électricité.
- ♦ Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.

- ♦ L'unité est équipée d'une fiche de terre à trois fils. Il s'agit d'une fonction de sécurité. Si vous ne parvenez pas à insérer la fiche dans la prise murale, contactez votre électricité afin qu'il remplace cette dernière qui doit être obsolète. N'essayez pas d'aller à l'encontre de l'objectif de la fiche de terre. Respectez toujours les codes de câblage en vigueur dans votre région/pays.
- ♦ L'équipement doit être installé à proximité de la prise murale et le dispositif de déconnexion (prise de courant femelle) doit être facile d'accès.
- ♦ La prise murale doit être installée à proximité de l'équipement et doit être facile d'accès.
- ♦ Veillez à ce que rien ne repose sur le cordon d'alimentation ou les câbles. Acheminez le cordon d'alimentation et les câbles de sorte que personne ne puisse marcher ou trébucher dessus.
- ♦ En cas d'utilisation d'une rallonge avec cette unité, assurez-vous que le total des ampérages de tous les produits utilisés sur cette rallonge ne dépasse pas l'ampérage nominal de cette dernière. Assurez-vous que le total des ampérages de tous les produits branchés sur la prise murale ne dépasse pas 15 ampères.
- ♦ Pour contribuer à protéger votre système contre les augmentations et diminutions soudaines et transitoires de puissance électrique, utilisez un parasurtenseur, un filtre de ligne ou un système d'alimentation sans coupure (UPS).
- ♦ Placez les câbles du système et les câbles d'alimentation avec précaution ; veillez à ce que rien ne repose sur aucun des câbles.
- ♦ Lors du branchement ou du débranchement à des blocs d'alimentation permettant la connexion à chaud, veuillez respecter les lignes directrices suivantes:
- ♦ Installez le bloc d'alimentation avant de brancher le câble d'alimentation à celui-ci.
- ♦ Débranchez le câble d'alimentation avant de retirer le bloc d'alimentation.
- ♦ Si le système présente plusieurs sources d'alimentation, déconnectez le système de l'alimentation en débranchant tous les câbles d'alimentation des blocs d'alimentation.
- ♦ N'insérez jamais d'objets de quelque sorte que ce soit dans ou à travers les fentes du boîtier. Ils pourraient entrer en contact avec des points de tension dangereuse ou court-circuiter des pièces, entraînant ainsi un risque d'incendie ou de choc électrique.

- ♦ N'essayez pas de réparer l'unité vous-même. Confiez toute opération de réparation à du personnel qualifié.
- ♦ Si les conditions suivantes se produisent, débranchez l'unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
 - ♦ Le cordon d'alimentation ou la fiche ont été endommagés ou éraillés.
 - ♦ Du liquide a été renversé dans l'unité.
 - ♦ L'unité a été exposée à la pluie ou à l'eau.
 - ♦ L'unité est tombée ou le boîtier a été endommagé.
 - ♦ Les performances de l'unité sont visiblement altérées, ce qui indique la nécessité d'une réparation.
 - ♦ L'unité ne fonctionne pas normalement bien que les instructions d'utilisation soient respectées.
- ♦ N'utilisez que les commandes qui sont abordées dans le mode d'emploi. Le réglage incorrect d'autres commandes peut être à l'origine de dommages qui nécessiteront beaucoup de travail pour qu'un technicien qualifié puisse réparer l'unité.

Montage sur bâti

- ♦ Avant de travailler sur le bâti, assurez-vous que les stabilisateurs sont bien fixés sur le bâti, qu'ils sont étendus au sol et que tout le poids du bâti repose sur le sol. Installez les stabilisateurs avant et latéraux sur un même bâti ou bien les stabilisateurs avant si plusieurs bâtis sont réunis, avant de travailler sur le bâti.
- ♦ Chargez toujours le bâti de bas en haut et chargez l'élément le plus lourd en premier.
- ♦ Assurez-vous que le bâti est à niveau et qu'il est stable avant de sortir une unité du bâti.
- ♦ Agissez avec précaution lorsque vous appuyez sur les loquets de libération du rail d'unité et lorsque vous faites coulisser une unité dans et hors d'un bâti ; vous pourriez vous pincer les doigts dans les rails.
- ♦ Une fois qu'une unité a été insérée dans le bâti, étendez avec précaution le rail dans une position de verrouillage puis faites glisser l'unité dans le bâti.
- ♦ Ne surchargez pas le circuit de l'alimentation CA qui alimente le bâti. La charge totale du bâti ne doit pas dépasser 80 % de la capacité du circuit.
- ♦ Assurez-vous que tous les équipements utilisés sur le bâti, y-compris les multiprises et autres connecteurs électriques, sont correctement mis à la terre.
- ♦ Assurez-vous que les unités présentes dans le bâti bénéficie d'une circulation d'air suffisante.
- ♦ Assurez-vous que la température ambiante de fonctionnement de l'environnement du bâti ne dépasse pas la température ambiante maximale spécifiée pour l'équipement par le fabricant.
- ♦ Ne marchez sur aucun appareil lors de la maintenance d'autres appareils d'un bâti.

Technical Support

International

- ♦ For online technical support – including troubleshooting, documentation, and software updates: **<http://eservice.aten.com>**
- ♦ For telephone support, see *Telephone Support*, page 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 KN1000A in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your computer must be on the same network segment as the KN1000A. After you have connected and logged in

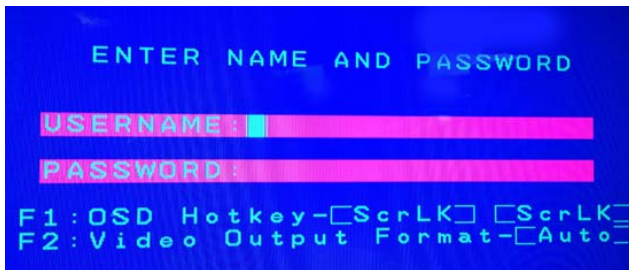
Local IP Setup

Use the local console to set the IP address. All procedures start from the OSD Main Screen.

1. To display the Main Screen, tap [Scroll Lock] twice.

Note: [Scroll Lock] is the default OSD hotkey. You can optionally change the Hotkey to the Ctrl key.

The login screen appears:



From this screen, you can select the following options:

- ♦ Press **F1** to change the hotkey for invoking the OSD screen. You can change the Hotkey to the Ctrl key instead of the Scroll lock key (shown as *ScrLK* in the screen).
- ♦ Press **F2** to select the video output format for the remote display, which includes AUTO, DVI and HDMI.

2. Enter a valid **Username** and **Password** to continue.

The default username is *administrator*; the default password is *password*. The first time you log in, you must use these defaults. For security purposes, we strongly recommend that you change the default password to something unique.

3. In the screen that appears, press **F1** to set the IP address. Proceed to step 4.



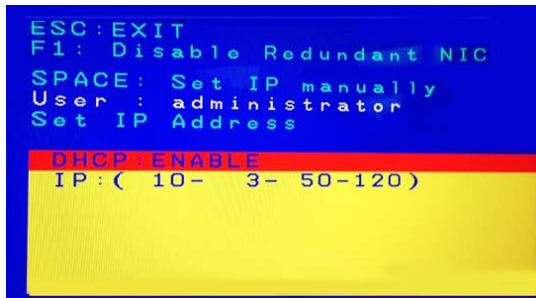
Press **F2** to enable the KN1000A to authenticate users. The KN1000A allows authentication and authorization through external programs. If the external programs fail to authenticate and you cannot log on to the device, use the local console to transfer authentication to the KN1000A. The following message displays when the operation is successful.



See *ANMS*, page 36 for details.

Press the **Esc** key to exit the local console.

4. When you invoke the OSD, a screen similar to the one below appears:



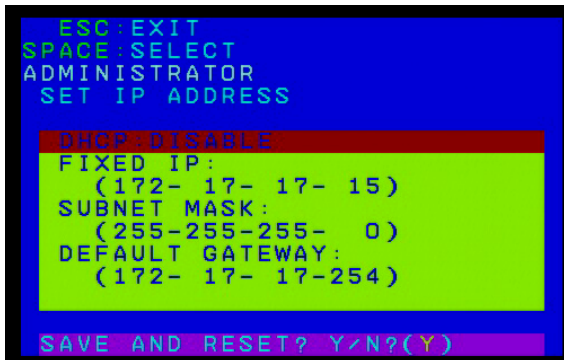
- ♦ To move up or down through the list one screen at a time, Click the Up and Down Arrow symbols (↑↓), or use the [Pg Up] and [Pg Dn] keys.
- ♦ To select or confirm a value, press the space bar [Space].
- ♦ To dismiss the menu, and deactivate OSD, press [Esc].

(Continues on next page.)

5. From the list, select **DHCP: Enable** and hit the space bar to toggle enabling or disabling the DHCP server. It should change to **DHCP: Disable** with additional fields, as follows:



6. For the fields **Fixed IP**, **Subnet Mask**, and **Default Gateway**, select each choice and enter the numerical address (dotted quad address).

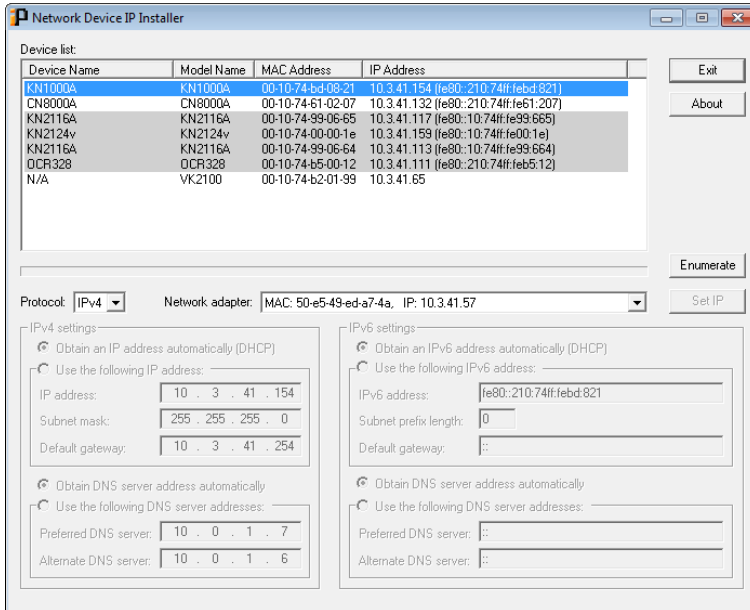


7. Go to **Save and Reset** and enter **Y** to confirm the new IP address.

IP Installer

For client computers running Windows, an IP address can be assigned with the *IP Installer* utility. The utility can be obtained from the *Support & Download* area of our website. Look under *Driver/SW*, and the model of your device. After downloading the utility to your client computer, do the following:

1. Unzip the contents of *IPInstaller.zip* to a directory on your hard drive.
2. Go to the directory that you unzipped the IPInstaller program to and run *IPInstaller.exe*. A dialog box similar to the one below appears:



(Continues on next page.)

3. Select the KN1000A in the *Device List*.

Note: 1. If the list is empty, or your device does not 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 KVM over IP switch's MAC address is located on its bottom panel.
-

4. Select the *Protocol* and *Network adapter*.
5. Select either *Obtain an IP address automatically (DHCP)*, or *Use the following IP address*. If you chose the latter, fill the IP Address, Subnet Mask, and Default Gateway fields with the information appropriate to your network.
6. Click **Set IP**.
7. After the IP address shows up in the Device List, click **Exit**. See *IP Installer*, page 149 for more information.

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 KN1000A.)
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 KN1000A 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 KN1000A's IP address can be determined with the Windows AP program (see *The WinClient AP*, page 130). When you run the program it searches the network segment for KN1000A devices, and displays the results in a dialog box similar to the one below:

You can now use this network address, or you can change it by clicking **Login**, logging in, clicking **Open GUI**, and clicking the *Network* tab. See *Network*, page 32, for details.

IPv6

At present, the KN1000A supports two IPv6 address protocols: *Link Local IPv6 Address*, and *IPv6 Stateless Autoconfiguration*

Link Local IPv6 Address

At power on, the KN1000A 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 KN1000A's IPv4 address and click the *Device Information* icon. The address is displayed at the bottom of the *Device Information* page (see page 24).

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

For example:

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

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

for the URL bar.

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

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

for the *IP* field of the *Server* panel (see *The WinClient AP*, page 130).

-
- Note:**
1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the KN1000A
 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 KN1000A's network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the KN1000A 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 (see *Device Information*, page 31).

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 WinClient AP*, page 130).

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 KN1000A connected to a particular router has an IP address of 192.168.1.180, you would log into your router's setup program and access the Port Forwarding (sometimes referred to as *Virtual Server*) configuration page. You would then specify 192.168.1.180 for the IP address and the port number you want opened for it (9000 for Internet access, for example).

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

Keyboard Emulation

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

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

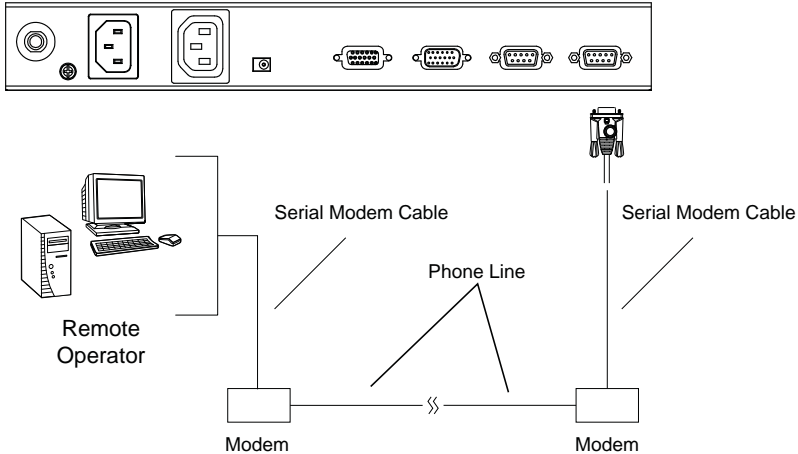
Note: When using key combinations, press and release the first key (Ctrl), then press and release the activation key.

PPP Modem Operation

Basic Setup

In addition to the browser and AP methods, the KN1000A can also be accessed through its RS-232 port using a PPP dial-in connection, as follows:

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



2. From your computer, use your modem terminal program to dial into the KN1000A's modem.

Note: 1. If you do not know the KN1000A modem's serial parameters, get them from the KN1000A administrator.

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

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

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

Connection Setup Example (Windows XP)

To set up a dial-in connection to the KN1000A under Windows XP, do the following:

1. From the *Start* menu, select Control Panel → Network Connections → Create a New Connection.
2. When the *Welcome to the New Connection Wizard* dialog box appears, click **Next** to move on.
3. In the *Network Connection Type* dialog box, select *Connect to the network at my workplace*, then click **Next**.
4. In the *Network Connection* dialog box, select *Dial-up connection*, then click **Next**.
5. In the *Connection Name* dialog box, key in a name for the connection (for example, TPE-KN1000-01), then click **Next**.
6. In the *Connection Availability* dialog box, you can select either *Anyone's use* or *My use only*, depending on your preferences, then click **Next**.

Note: If you are the only user on this computer, this dialog box will not appear.

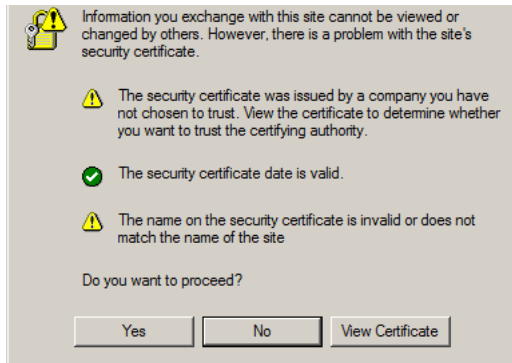
7. In the *Phone Number to dial* dialog box, key in the phone number of the modem connected to the KN1000A (be sure to include country and area codes, if necessary), then click **Next**.
8. In the *Completing the New Connection Wizard* dialog box, check **Add a shortcut to this connection on my desktop**, then click **Finish**.

This completes the connection setup. Double click the desktop shortcut icon to make a PPP connection to the KN1000A.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.



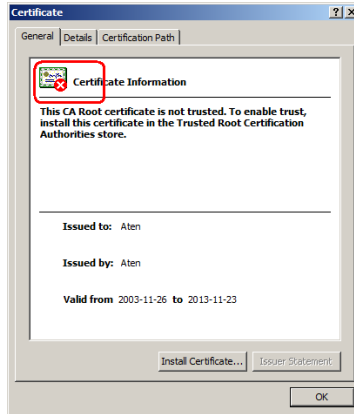
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- ♦ If you are working on a computer at another location, accept the certificate for just this session by clicking **Yes**.
- ♦ If you are working at your own computer, install the certificate on your computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Installing the Certificate

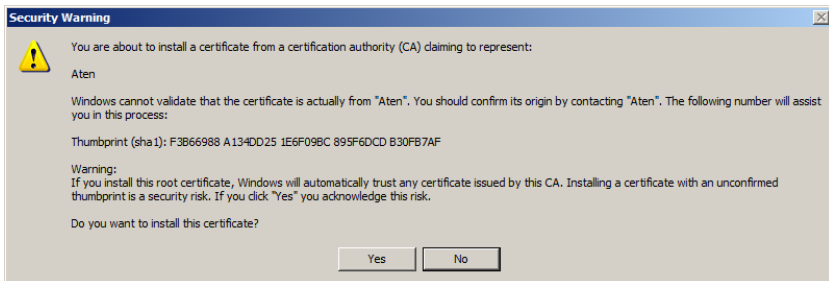
To install the certificate, do the following:

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



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

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

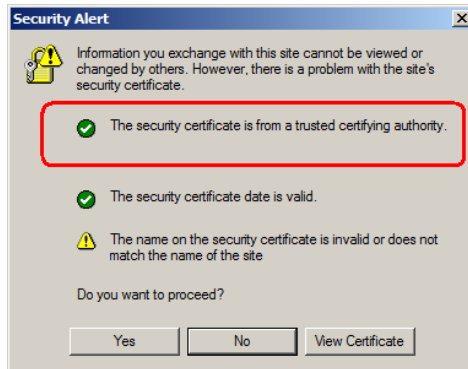


Click **Yes**.

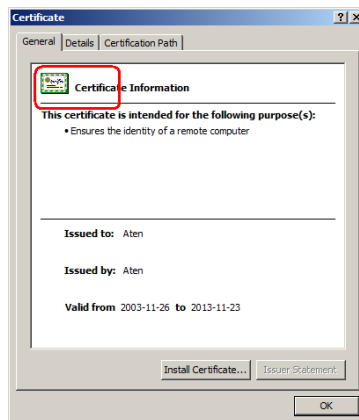
13. Next, click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:

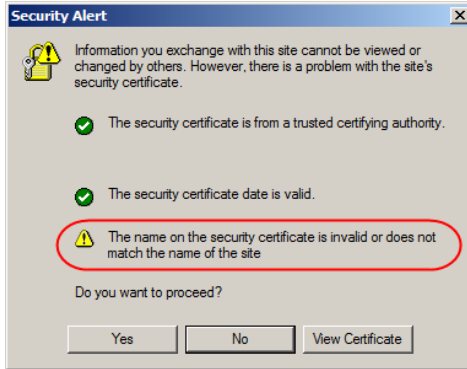


When you click *View Certificate*, you can see that the red and white X logo is no longer present – further indication that the certificate is trusted:



Mismatch Considerations

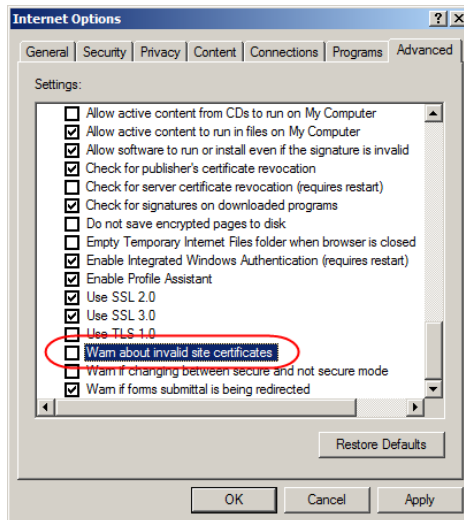
If the site name or IP address used for generating the certificate no longer matches the current address of the KN1000A a mismatch warning occurs:



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 49).

Troubleshooting

General Operation

Problem	Resolution
Erratic operation	<p>The KN1000A needs to be started before the KVM switch</p> <ol style="list-style-type: none"> 1. If the KN1000A 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 KN1000A, reset or restart the KVM switch. <p>The KN1000A needs to be reset (see <i>Firmware Upgrade / Reset Switch</i>, page 11).</p>
I cannot access the KN1000A, even though I have specified the IP address and port number correctly.	If the KN1000A 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 153, 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 80 for details.
Mouse movement extremely slow	There is too much data being transferred for your connection to keep up with. Lower the video quality (see <i>Video Settings</i> , page 88) so that less video data is transmitted.
Changing Mouse Sync Mode to Manual makes the KN1000A crash.	The KN1000A hasn't crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the KN1000A to get it going right away (see <i>Firmware Upgrade / Reset Switch</i> , page 11).
I cannot access my PN9108 when I click the <i>Power Management</i> icon.	Since the PN9108 already has over IP functionality, there is no need for the KN1000A to provide it. Therefore, only PON devices that do not have their own over IP functionality (such as the PN0108) are supported.
When I am in a web browser session, and making configuration changes, and I am timed out, the settings changes I have made are lost.	If you do not click Apply , the KN1000A 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 KN1000A and reset the timeout counter.
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.

Problem	Resolution
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 KN1000A with a browser; open a viewer; on the control panel set <i>Mouse DynaSync</i> to Manual . See page 100 for details.

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.	<ol style="list-style-type: none"> 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 157, 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 49).
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 160 for a complete explanation of this topic.
Remote mouse pointer is out of step.	<ol style="list-style-type: none"> 1. Check the status of the <i>Mouse DynaSync Mode</i> setting (see <i>Mouse DynaSync Mode</i>, page 100). 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 88), 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 80) 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 168, 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 88), to sync the local and remote monitors.
Virtual Media does not work.	This problem sometimes arises on older computers. Get the latest firmware version for your mainboard from the manufacturer and upgrade your mainboard firmware.
Under Virtual Media, I can mount an ISO file, but I cannot access it.	Virtual Media under the WindowsClient only supports ISO files less than 4G.Bytes. If the ISO file is 4GBytes or greater it cannot be accessed.
My antivirus program reports that there is a trojan after I access the KN1000A 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 110, *Mouse DynaSync Mode*, page 118, and *Sun / Linux*, page 169. For other problems, see the table below:

Problem	Resolution
Java Applet will not connect to the KN1000A	<ol style="list-style-type: none"> 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 KN1000A'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 do not appear.	Use the KN1000A'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 117.)
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 157, for details.
There is no Virtual Media icon on my Control Panel.	The virtual media function only supports the Windows Client programs.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g., Sun Blade 1000 servers). ¹	<p>The display resolution should be set to 1024 x 768:</p> <p>Under Text Mode:</p> <ol style="list-style-type: none">1. Go to OK mode and issue the following commands: <pre>setenv output-device screen:r1024x768x60 reset-all</pre> <p>Under XWindow:</p> <ol style="list-style-type: none">1. Open a console and issue the following command: <pre>m64config -res 1024x768x60</pre> <ol style="list-style-type: none">2. Log out3. Log in
Video display problems with 13W3 interface systems (e.g., Sun Ultra servers).*	<p>The display resolution should be set to 1024 x 768:</p> <p>Under Text Mode:</p> <ol style="list-style-type: none">1. Go to OK mode and issue the following commands: <pre>setenv output-device screen:r1024x768x60 reset-all</pre> <p>Under XWindow:</p> <ol style="list-style-type: none">1. Open a console and issue the following command: <pre>m64config -res 1024x768x60</pre> <ol style="list-style-type: none">2. Log out3. Log in
The local and remote mouse pointers do not sync	<p>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 100 for further details.</p>

* 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 66). 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. Do not use the Snapshot feature in the future.
	To use the Snapshot feature with Safari, upgrade to Mac OS 10.4.11.

The Log Server

Problem	Resolution
The Log Server program does not run.	<p>The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database.</p> <p>This driver is automatically installed with Windows ME, 2000 and XP.</p> <p>For Windows 98 or NT, you will have to go to the Microsoft download site:</p> <p>http://www.microsoft.com/data/download.htm</p> <p>to retrieve the driver file:</p> <p>MDAC 2.7 RTM Refresh (2.70.9001.0)</p> <p>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.</p>

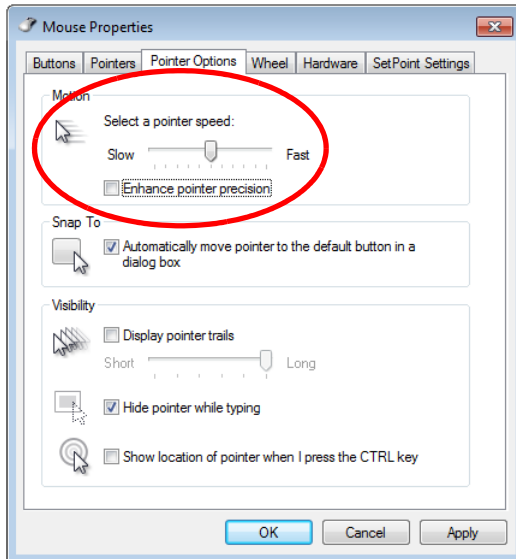
Additional Mouse Synchronization Procedures

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

Windows:

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

1. Windows 7 / Windows XP / Windows Server 2003:
 - a) Open the Mouse Properties dialog box (Control Panel → Mouse).
 - b) Click the *Pointer Options* tab.
 - c) Set the mouse speed to the middle position (5 units in from the left).
 - d) Disable *Enhance Pointer Precision*.



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.)

Supported KVM Switches

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

ACS1208A	CS1758
ACS1216A	CS9134
CS1308	CS9138
CS1316	KH1508A
CS1708A	KH1516A
CS1716A	KH2508A
CS1754	KH2516A

- Note:** 1. Some of the KN1000A's features may not be supported, depending on the functionality of the cascaded KVM switch. (For example, some switches do not support virtual media.)
2. Some features found on the cascaded KVM switches may not be supported on the KN1000A. (For example, the CS1754's audio, and the CS1708A/CS1716A must use PS/2 connectors when cascading.)
-

Virtual Media Support

WinClient ActiveX Viewer / WinClient AP

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

* These drives can be mounted either as Drives or Removable Disks (see *Virtual Media*, page 93). 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

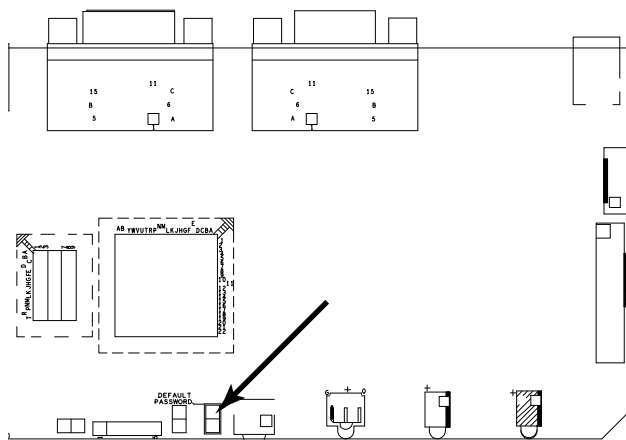
- ♦ Smart Card Readers

Java Applet Viewer / Java Client AP

- ♦ ISO Files – Read Only
- ♦ Folders – Read/Write

To clear the login information do the following:

1. Power off the KN1000A, disconnect the power cord from its inlet, and remove its housing.
2. Use a jumper cap to short the jumper on the mainboard labeled J10.



3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from J10.
6. Close the housing and power on the KN1000A.

After you start back up, you can use the default Username and Password (see page 22, and page 131) to log in.

Specifications

Function		Specification
Connectors	Console	1 x SPHD-18 Male (Yellow)
	KVM (Computer)	1 x SPHD-18 Female (Yellow)
	PON ¹	1 x DB-9 Male (Black)
	Modem	1 x DB-9 Male (Black)
	LAN	1 x RJ-45 Female
	Power Inlet	1 x IEC320 C14
	Power Outlet	1 x IEC320 C13
	Power	1 x DC Jack
	Virtual Media	1 x USB Mini-B Female (Black)
Switches	Reset	1 x Semi-recessed pushbutton
LEDs	Power	1 (Orange)
	Power Outlet	1 (Orange)
	Link	1 (Green)
	10/100/1000 Mbps	1 (10 Mbps: Orange / 100 Mbps: Orange + Green / 1000 Mbps: Green)
Emulation	Keyboard/Mouse	USB; PS/2
Video		1920 x 1200 @ 60 Hz; DDC2B
Input		100–240 V~; 50/60 Hz, 10A
Output		100–240 V~; 50/60 Hz; 9A
Power Consumption		DC5.3 V; 4.48 W
Environment	Operating Temp.	0–40° C
	Storage Temp.	-20–60° C
	Humidity	0–80% RH Non-condensing
Physical Properties	Housing	Metal
	Weight	0.88 kg
	Dimensions (L x W x H)	31.00 x 8.39 x 4.20 cm

¹ Power Over the NET™

About SPHD Connectors



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

Limited Warranty

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

What is covered by the Limited Hardware Warranty

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

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

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